

4th Annual HBCU Tech Law Summit
&
19th Annual IP and Social Justice CLE Seminar

IP Law Year In Review



THOMAS IRVING



DOUGLAS RETTEU



IAN BALLON



Douglas Rettew

Douglas (Chip) Rettew is a partner in Finnegan's Washington, DC office. He has been recognized in World Trademark Review WTR 1000 as "[o]ne of the best litigators in the country with an unbelievable success rate," and "a go-to litigation lead for world-famous consumer brands." He focuses his practice on trademark, false advertising, and unfair competition litigation and disputes. Doug litigates cases involving a broad range of issues, including traditional trademarks, false advertising, product disparagement, rights of publicity, unfair competition, trade dress, design patents, and domain names. Doug is also involved in advertising issues and counseling, right-of-publicity matters, and trademark and copyright prosecution and licensing. Doug has first-chair jury and bench trial and appellate experience and has successfully argued appeals before the U.S. Courts of Appeals for the Federal, Fourth, Eighth, and Eleventh Circuits. He also litigates oppositions, cancellations, and ex parte appeals before the Trademark Trial and Appeal Board. Doug has significant experience in obtaining (and defeating) temporary restraining orders (TROs) and preliminary injunctions, including those involving counterfeiting and ex parte seizures. He has testified before Congress on trademark issues, served as leader of the firm's trademark/copyright/advertising practice, and is currently on the firm's management committee.

Ian Ballon

Ian C. Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and TCPA class action suits.

Ian is also the author of the leading treatise on internet and mobile law, E-Commerce and Internet Law: Treatise with Forms 2d edition, the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of intellectual property law issues. In addition, he serves as Executive Director of Stanford University Law School's Center for the Digital Economy. He also chairs PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian was named the Lawyer of the Year for Information Technology Law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of Best Lawyers in America (including lawyer of the year for 2022). In 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by World Trademark Review. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the Los Angeles and San Francisco Daily Journal. He received the "Trailblazer" Award, Intellectual Property, 2017 from The National Law Journal and he has been recognized as a "Groundbreaker" in The Recorder's 2017 Litigation Departments of the Year Awards. He was also recognized as the 2012 New Media Lawyer of the Year by the Century City Bar Association. In 2010, he was the recipient of the California State Bar Intellectual Property Law section's Vanguard Award for significant contributions to the development of intellectual property law. Ian was listed in Variety's "Legal Impact Report: 50 Game-Changing Attorneys" and has been named by the LA and San Francisco Daily Journal as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2021), and has been listed as a Northern California Super Lawyer every year from 2004 through 2021 and as one of the top 100 lawyers in California. He is also listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology.

Ian holds JD and LLM degrees and the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

19th Annual IP & Social Justice CLE Program

YEAR IN REVIEW: PATENT LAW

BY

TOM IRVING AND STACY LEWIS

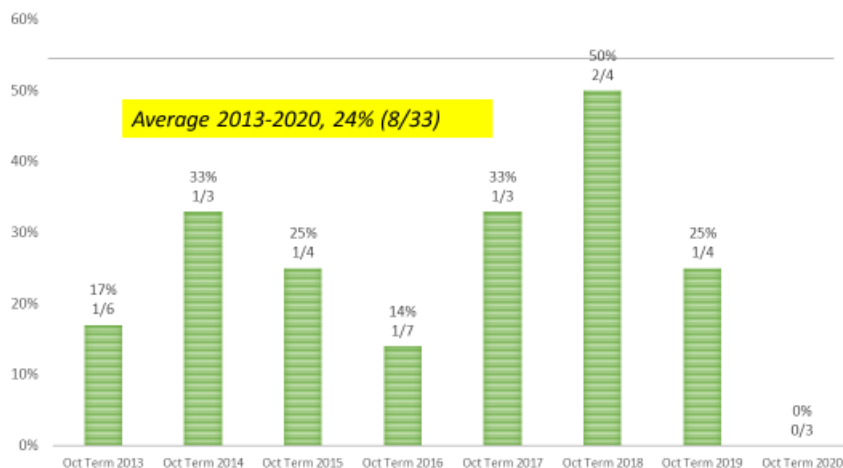


March 4, 2022

Disclaimer

These materials have been prepared solely for educational and entertainment purposes to contribute to the understanding of U.S. intellectual property law. These materials reflect only the personal views of the authors and are not individualized legal advice. It is understood that each case is fact specific, and that the appropriate solution in any case will vary. Therefore, these materials may or may not be relevant to any particular situation. Thus, the authors and Finnegan, Henderson, Farabow, Garrett & Dunner, LLP (including Finnegan Europe LLP, and Fei Han Foreign Legal Affairs Law Firm), cannot be bound either philosophically or as representatives of their various present and future clients to the comments expressed in these materials. The presentation of these materials does not establish any form of attorney-client relationship with these authors. While every attempt was made to ensure that these materials are accurate, errors or omissions may be contained therein, for which any liability is disclaimed.

U.S. Supreme Court Affirmance Rate of CAFC Decisions



Source: <https://www.scotusblog.com/reference/stat-pack/>

FINNEGAN

3

The Supreme Court and “A”

Niz-Chavez v. Garland, 593 U.S. ____ (2021)

- 5-3 decision, “a” means “one.”
- A federal law requires the government to serve “a notice to appear.”
- According to the majority: “a” notice would seem to suggest just that: “a” single document containing the required information, not a mishmash of pieces with some assembly required.
- Dissent: “The statute nowhere says that written notice must be provided in a single document.” “As a matter of ordinary parlance, however, the word ‘a’ is not a one-size-fits-all word.” *Id.* The dissent would interpret “a notice” as fulfilled by more than one notification.

FINNEGAN

See, <https://www.finnegan.com/en/insights/blogs/prosecution-first/supremely-confusing-on-that-complex-word-a-is-it-only-one-or-is-it-one-or-more.html>

4

Constitutionality of PTAB Judges



United States v. Arthrex, Inc., 141 S. Ct. 1970 (U.S., June 21, 2021)

- Federal Circuit: PTAB judges unconstitutionally appointed.
- Supreme Court vacated and remanded.
 - “APJs ... exercise power that conflicts with the design of the Appointments Clause ‘to preserve political accountability.’”
 - “Decisions by APJs must be subject to review by the Director.... The Director accordingly may review final PTAB decisions and, upon review, may issue decisions himself on behalf of the Board.”
- June 29, 2021: USPTO issued guidance on the implementation of an interim Director review process by which a party can request review by the Director of PTAB FWD,
https://www.uspto.gov/patents/patent-trial-and-appeal-board/procedures/uspto-implementation-interim-director-review?utm_campaign=subscriptioncenter&utm_content=&utm_medium=email&utm_name=&utm_source=govdelivery&utm_term=
- Epilogue: Acting Director Hirshfeld denied Arthrex's rehearing bid.
- Arthrex appealed, arguing that it "On remand, Arthrex never got the remedy the Supreme Court ordered."
- Meanwhile, first two post-Arthrex Director review cases going forward,
<https://www.finnegan.com/en/insights/blogs/at-the-ptab-blog/uspto-director-grants-first-director-review-petition-vacating-ptab-decision.html>

FINNEGAN

See, <https://www.finnegan.com/en/insights/blogs/at-the-ptab-blog/after-arthrex-uspto-creates-interim-director-review-process.html>

5

Assignor Estoppel

“May a defendant in a patent infringement action who assigned the patent, or is in privity with an assignor of the patent, have a defense of invalidity heard on the merits?”

FC: No.

Minerva Surgical, Inc. v. Hologic, Inc., 141 S. Ct. 2298 (U.S., June 29, 2021)

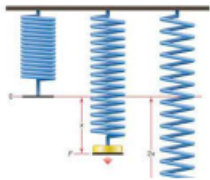
- Vacated and remanded.
- Doctrine of assignor estoppel limited it to situations where the claim of invalidity contradicts explicit or implicit representations the assignor made in assigning the patent.
 - **Applicability of the doctrine tied to representations made by the assignor.**
- “a bounded doctrine designed to prevent an inventor from first selling a patent and then contending that the thing sold is worthless.”

FINNEGAN

6

§ 101 Not Any Clearer in 2021

American Axle & Mfg. v. Neapco Holdings LLC, 939 F.3d 1355 (Fed. Cir. 2019), *pet. for cert. filed* Dec. 28, 2020 (Case No. 20-891)

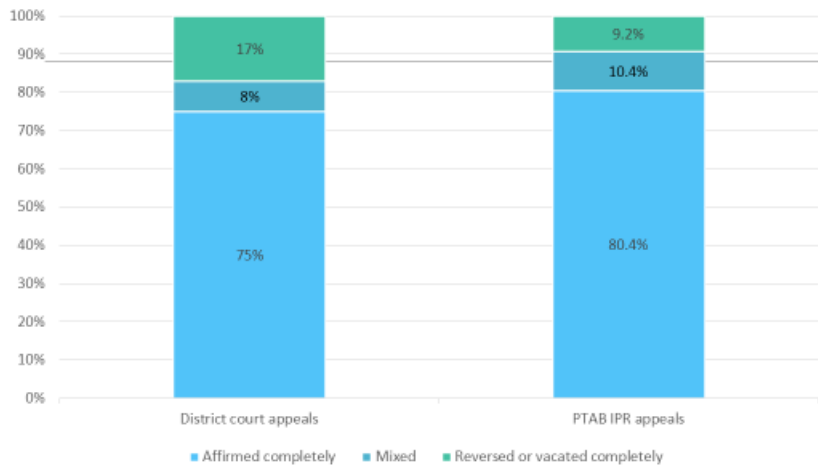


- FC: Affirmed district court's grant of summary judgment, finding American Axle's claims covering "a method of manufacturing a shaft assembly" patent ineligible under 35 U.S.C. § 101.
- Mayo/Alice* Step one: claims covered a natural law—Hooke's Law—noting "the claims' general instruction to tune a liner amounts to no more than a directive to use one's knowledge of Hooke's law."
- Mayo/Alice* Step two: claims did not recite an inventive concept or identify more than conventional pre- and post-solution activity.

FINNEGAN

7

CAFC Affirmance Rate Very High Whether From District Court or PTAB



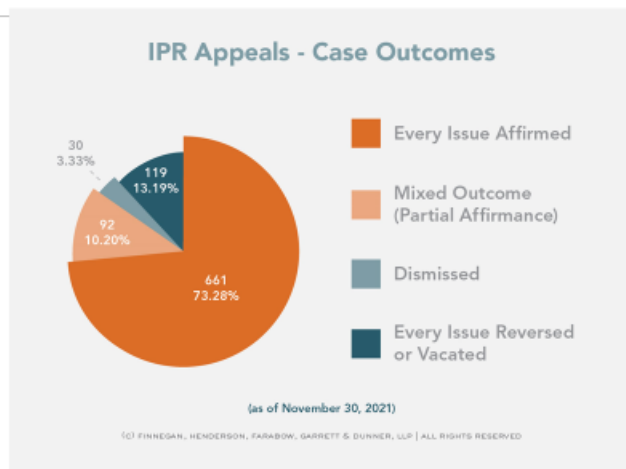
Note, this is not a patent owner win rate. Article shows patent owner win rate in appeals of district court cases is 23% (and another 10.5 % mixed outcomes) and patent owner win rate in appeals of PTAB IPR decisions 28% (plus another 17% mixed outcomes)

Source: Bagatell, Dan, "Fed. Circ. Patent Decisions In 2021: An Empirical Review," Law360, January 7, 2022.

FINNEGAN

8

CAFC Outcomes of PTAB Appeals: Finnegan Research



Inventorship/Ownership: Corroboration

- *Wagner v. Ashline*, 2021 U.S. App. LEXIS 34093 (Fed. Cir. Nov. 17, 2021) (unpublished)
 - In 2001, Ms. Wagner began work on a safety vest for children with shoulder (the "Guardian Angel Vest"). Around the same time, Mr. Ashline began developing a head and neck restraint (HNR) device for reducing serious injury during a high-performance vehicle collision.
 - 2003, Ms. Wagner and Mr. Ashline met about the vest.
 - 2006, relationship ended turbulently in 2006.
 - 2010, Ms. Wagner discovered that Mr. Ashline had filed a patent application on his HNR device
 - Patent issued in 2012, as U.S. Patent NO. 8,272,074 ("the '074 patent"). Claim 1 of the '074 patent recites "a member having shoulder portions at least partially positionable on top of at least a portion the shoulders of the driver."
 - Ms. Wagner alleged that she contributed to the "shoulder portions" limitation recited in claim 1 of the '074 patent, and sued Mr. Ashline and his company, Simpson Performance Products, Inc., to whom he had assigned the '074 patent, seeking to be added as a joint inventor.
 - FC: Affirmed district court decision to grant summary judgment against Ms. Wagner, agreeing that she failed to provide sufficient corroboration of her claim of joint inventorship under 35 U.S.C. § 256.
- Inventorship of a patent is important, and if an omitted inventor makes an evidentiary showing sufficient to establish that she should be named as a co-inventor on a patent, she will enjoy a presumption of ownership of the entire patent, even if her contribution pertained to a single claim in a patent having multiple claims.
- An alleged co-inventor must present sufficient independent evidence, outside of her own testimony, to corroborate her assertion of contribution to the conception of the invention as claimed. Evidence that merely demonstrates conversations between the alleged co-inventor and actual inventor regarding the invention or discussions of the prior art may not be sufficient to prove co-inventorship.

Inventorship/Ownership: Employment Contracts

Bio-Rad Labs., Inc. v. ITC, 998 F.3d 1320 (Fed. Cir. 2021)

- ITC: Bio-Rad infringed patents owned by 10X.
- Bio-Rad argued that it co-owned the asserted patents based on assignment provisions that two named inventors signed while employees of Bio-Rad, even though the claimed inventions were not made until after that employment.
- FC: Affirmed ITC.
- Asserted patent claims have January 2013 conception date—after Drs. Hindson and Saxonov left Bio-Rad.
- Agreements were limited by their terms to IP created during the employee's employment term.



Claim Construction Fundamentals Still Important

SIMO Holdings, Inc. v. Hong Kong uCloudlink Network Technology Limited, 2021 U.S. App. LEXIS 137 (Fed. Cir. Jan. 5, 2021)

- “a plurality of [a, b, c, d, e and/or f]
- Does “a plurality of” apply to each element in a series?
- DC: No, “a plurality of” requires only ‘at least two’ members selected from the entire list of identified items (memory, processors, etc.).”
- FC: Reversed.
- “We conclude, along with uCloudlink, that ‘a plurality of’ requires at least two of *each* of the listed items in the phrase at issue in claim 8.” (emphasis in original)
- Cites *SuperGuide Corporation v. DirecTV Enterprises, Inc.*, 358 F.3d 870 (Fed. Cir. 2004), “a phrase grammatically comparable to ‘a plurality of’ at the start of a list of items joined together by ‘and’ applied to each item in the list, not to the list considered as a whole.”

The Creative POSITA Finally Appears

- *CR Bard v. Medline Indus.*, 2021 U.S. App. LEXIS 24135 (Fed. Cir. Aug. 13, 2021) (unpublished)
 - Inventions relate to surgical trays.
 - PTAB: Some challenged claims not unpatentable for obviousness.
 - FC: affirmed-in-part, vacated-in-part, and remanded the cases for further proceedings.
 - The Board's obviousness analysis was too rigid and did not account for "a skilled artisan's 'creativity [] and common sense.'"
 - "Given the prior art disclosures and the finite number of predictable options, a skilled artisan would have been motivated to stack the syringes by height according to their order of use."
 - Obviousness analysis is not an anticipation analysis.
- *Before the Supreme Court decision in KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398 (2007), the person of ordinary skill in the art ("POSITA") was not creative. But in *KSR*, the Supreme Court explicitly noted that the POSITA has creativity.

Inherency Continues to Creep into Obviousness Analysis

L'Oréal USA, Inc. v. Olaplex, Inc., 844 Fed. Appx. 308 (Fed. Cir. Jan. 28, 2021) (unpublished)

- PTAB: Certain claims of Olaplex U.S. Patent No. 9,668,954 ("the '954 patent") were unpatentable as obvious; "breakage" claims were not unpatentable because L'Oréal failed to establish that the breakage claims' limitations (to decrease by a certain amount) were inherent in the prior art.
- FC: Affirmed.
 - L'Oréal did not prove that the breakage-decrease percentages in the breakage claims were necessarily present in, or the natural result of, the combined teachings of the prior art.

Obviousness: Basic Principles

Chemours Co. FC, LLC v. Daikin Indus., 2021 U.S. App. LEXIS 21690 (Fed. Cir. 2021)

- Motivation to combine/modify prior art must be explained.
- Nexus analysis may require evaluation of claims as a “unique combination”
- Blocking patents cannot block themselves.
- Modification may be nonobvious where the “inventive concept” of the prior art reference teaches away from that modification.
- Teaching away may preclude a motivation to modify.

See, <https://www.finnegan.com/en/insights/blogs/prosecution-first/blocking-patents-a-patent-cannot-block-itself.html>; <https://www.finnegan.com/en/insights/blogs/prosecution-first/objective-indicia-nexus-analysis-may-require-evaluation-of-claims-as-a-unique-combination.html>; <https://www.finnegan.com/en/insights/blogs/prosecution-first/teaching-away-may-preclude-motivation-to-modify-a-reference.html>

Obviousness: More Basic Principles

Takeda Pharm. Co. v. Torrent Pharms. Ltd., 844 Fed. Appx. 339 (Fed. Cir. Feb. 16, 2021): “merely asserting that a given modification would have been obvious to a skilled artisan does not make it so.”

Daikin Indus., Ltd v. Chemours Co. FC, LLC, 846 Fed. Appx. 907 (Fed. Cir. 2021): objective evidence (including unexpected results) must be commensurate with the full scope of the claimed invention.

CAFC Life Science WD Decisions Since 2019

- *Idenix v. Gilead*, 941 F.3d 1149 (Fed. Cir. 2019)
- *Purdue Pharma L.P. v. Iancu*, 767 Fed. Appx. 918 (Fed. Cir. 2019) (unpublished)
- *Nuvo Pharms. (Ir.) Designated Activity Co. v. Dr. Reddy's Labs. Inc.*, 923 F.3d 1368 (Fed. Cir. 2019)
- *Nalpropion Pharms., Inc. v. Actavis Labs. FL, Inc.*, 934 F.3d 1344 (Fed. Cir. 2019)
- *Merck Sharp & Dohme Corp. v. Microspherix LLC*, 814 Fed. Appx. 575 (Fed. Cir. 2020) (unpublished)
- *Immunex Corp. v. Sandoz, Inc.*, 964 F.3d 1049 (Fed. Cir. 2020)
- *Juno Therapeutics, Inc. v. Kite Pharma, Inc.*, 10 F.4th 1330 (Fed. Cir. 2021)
- *Bristol-Myers Squibb Co. v. Sigmapharm Labs. LLC*, 858 Fed. Appx. 359 (Fed. Cir. Sept. 3, 2021)
- *Biogen Int'l GmbH v. Mylan Pharms., Inc.*, 2021 U.S. App. LEXIS 35254 (Fed. Cir. 2021), *pet. for reh'g filed Dec. 30, 2021*

Whither Wertheim?

- *Indivior UK Ltd. v. Reddy's Labs. S.A.*, --F.4th__ (Fed. Cir. Nov. 24, 2021)
 - All but one challenged claim recited range, e.g., "about 40 wt% to about 60 wt% of a water-soluble polymeric matrix"
 - Claim 8 recited specific amount, 48.2 wt% of the water soluble polymeric matrix.
 - Specification included tables disclosing the weight percentages of individual polymeric components in film samples that, when combined, produced an aggregate polymer weight percentage value of 48.2 wt%.
 - FC: Majority affirmed PTAB FWD that claims unpatentable as anticipated because lacked written description support in priority document EXCEPT for Claim 8, which was adequately supported and therefore obtained the benefit of the priority date, antedating the Myers application.
 - No written description support of the ranges recited.
 - Faulted the disclosure in specification tables of weight percentages of individual polymer components in samples: **it does not show sufficient possession if a skilled artisan has to "cobble together [these] numbers after the fact"** after previously identifying and summing the weight percentages of each of the individual polymeric components in the samples.
 - Such an expectation when filing an application would amount to "an invitation to go on a hunting expedition to patch together after the fact a synthetic definition of an invention."
 - Also, statement in specification that "any desired level of . . . polymer" could be used in the film and disclosures of embodiments with polymer weight percentages outside of the claimed ranges (e.g., "at least 25[wt%]") would lead a skilled artisan away from the conclusion "that the inventor had possession of the claimed subject matter as of the filing date."
 - "no case, with necessarily varied facts, controls the resolution of the written description issue in this case."

Whither Wertheim?

• *Indivior* (con't)

- FC: Affirmed that a POSITA could readily determine—by identifying and summing the individual weight percentages of various polymers in the sample films—that Claim 8 had sufficient written description.
- Judge Linn’s opinion disagreed with the majority over the application of the Wertheim and Nalpropion case law. The claimed polymer ranges “are selections of aggregate polymer ranges that a reasonable artisan would understand endow the film with the identified and desired properties [found in the specification].”
- No authority for the majority’s position that “written description support for a ‘closed range’ requires a disclosure of a closed range rather than discrete values[.]”
- No “cobbling together” was required; adding up values to meet a desired disclosed characteristic was not beyond the person of ordinary skill.

Developments in Post-GSK Induced Infringement

Amarin Pharma v. Hikma Pharms. United States, 2022 U.S. Dist. LEXIS 1937 (D. NJ Jan. 4, 2022)

- Amarin sued Hikma for induced infringement of three patents that describe methods of using icosapent ethyl for the reduction of cardiovascular risk.
 - VASCEPA®
 - Amarin sells VASCEPA® for the treatment of severe hypertriglyceridemia (the “SH indication”) and cardiovascular risk reduction (the “CV indication”).
- Only the CV indication is covered by Amarin’s patents.
- Hikma received FDA approval to sell a generic version for the SH indication under the “skinny label” or “section viii carveout” regime.
- Basis of induced infringement: Hikma’s label and public statements.
- Hikma’s motion to dismiss granted.
 - Label mentioning side effects is not inducement; nor is silence as to CV limitation.
 - Press releases may go to intent but are not an inducing act.

DOE Still Alive in 2021: Claim Limitation Vitiating

Olaf Soot Design, LLC v. Daktronics, Inc., 839 Fed. Appx. 505 (Fed. Cir. 2021), *pet. for cert. filed*

- The only claim at issue on appeal recited several elements, a) through h).
- OSD argued that “the hub is a part of the drum.” Daktronics argued that the hub and drum are separate.
- Jury: Daktronics’ product infringed under the doctrine of equivalents.
- DC: Claim construed as OSD proposed.
- **FC: Reversed.** DC should have construed claim before trial.
 - The plain language of element h) and the specification clarify that the hollow hub is not part of the hollow drum.
 - No literal infringement - Daktronics’ product “does not literally meet element h of claim 27[;] the hollow drum of the Vortek is not able to receive the screw.”
 - No DOE infringement - Daktronics’ product has no equivalent function to element (h).

Warning from Judge Lourie

Olaf (con’t)

- Judge Lourie “express[ed] concern over the use of the doctrine of equivalents to find infringement when four claim limitations have not literally been met by the accused device.”
- Having multiple differences from the claim should be a hallmark of noninfringement. It fails the straight face test to assert that the accused subject matter does not meet the claims in multiple distinct ways but infringes anyway.
- “That would be equivalent” “to holding that the accused product infringes when it does not infringe.” “Designing around” is an important concept in patent law and finding a product with “multiple significant instances of inventing around still infringe runs counter to that important theory of patent law.”
- “[F]or if the public comes to believe (or fear) that the language of patent claims can never be relied on, and that the doctrine of equivalents is simply the second prong of every infringement charge, regularly available to extend protection beyond the scope of the claims, then claims will cease to serve their intended purpose.” [citation omitted]

Ex Parte Reexam Request After Multiple IPR Petition Filings

In re Vivint, 14 F.4th 1342 (Fed. Cir. 2021)

- Vivint sued Alarm.com for infringement of four patents, incl. U.S. 6,717,513.
- Alarm.com then filed 14 petitions for IPR, incl. three petitions challenging the '513 patent, which were denied under 35 U.S.C. § 314(a) and 35 U.S.C. § 325(d).
- Alarm.com then requested ex parte reexamination.
- Patent Office: ordered reexamination, finding Alarm.com had raised SNQ's.
- Vivint sought dismissal of the reexamination under 37 C.F.R. § 1.181 by exercise of discretion under 35 U.S.C. § 325(d).
- Patent Office dismissed Vivint's Rule 181 petition because it was filed after reexamination was ordered.
- Vivint's request for reconsideration was denied, in part due to the timing of Vivint's petition.
- Eventually, the examiner rejected the claims in the reexamination and the PTAB affirmed.
- Vivint appealed, arguing that "because the ex parte reexamination request repackaged arguments in the '091 petition, it did not present a new question of patentability."
- FC: Remanded with instructions to dismiss.
 - Each of Alarm.com's four questions of patentability in the reexamination request was new under § 303(a) because the USPTO did not consider any of them on the merits during its consideration of whether to institute IPR.
 - However, "the Patent Office abused its discretion and acted arbitrarily and capriciously by ordering reexamination, and thereafter, refusing to terminate that proceeding."
 - Noted that ruling was "limited" and that there may be circumstances under which the USPTO may order an ex parte reexamination despite an earlier petition for IPR or PGR.

Judicial Review Of Request For Ex Parte Reexam Applying Petitioner Estoppel?

2015: Vivint sued Alarm.com for infringement of U.S. Patent Nos. 6,147,601, 6,462,654, and 6,535,123.

Alarm.com filed IPR petitions.

2017: PTAB FWDs with mixed outcomes, affirmed on appeal (754 F. App'x 999 (Fed. Cir. 2018))

Alarm.com then requested *ex parte* reexaminations of the same 3 patents.

PTO vacated the proceedings rather than making a §303(a) determination.

- Alarm.com estopped from seeking reexamination; could have reasonably raised the unpatentability arguments it made in the reexam requests during the IPRs.

DC (2021 WL 2557948 (E.D. Va. June 22, 2021): Dismissed APA suit; lacked authority to review.

FC: *Alarm.com Inc. v. Hirshfeld*, No. 21-2102 (Fed. Cir. Feb. 24, 2022) (TARANTO, Chen and Cunningham), **reversed and remanded**.

- § 303(c) does not apply to the estoppel decisions at issue here.
- "In light of [the] case law, we reject the government's contention that the ex parte reexamination statutory scheme provides clear and convincing evidence that Congress intended to preclude judicial review of determinations like this one, not expressly barred by § 303(c)."

PTAB

Apple Inc. v. Fintiv, Inc., IPR2020-00019, Paper 11 (March 20, 2020)
(precedential)

- 6 factors (*Fintiv* factors) that the Board considers in determining whether to exercise its discretion to institute review when there is a related proceeding pending in district court, these factors are:
 1. Whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
 2. Proximity of the court's trial date to the Board's projected statutory deadline for a final written decision;
 3. Investment in the parallel proceeding by the court and the parties;
 4. Overlap between issues raised in the petition and in the parallel proceeding;
 5. Whether the petitioner and the defendant in the parallel proceeding are the same party; and
 6. Other circumstances that impact the Board's exercise of discretion, including the merits.
- Joins *NHK Spring Co. v. Intri-Plex, Techs., Inc.*, IPR2018-00752, Paper 8 (P.T.A.B. Sept. 12, 2018) (precedential)

Multiple Court Challenges

Lawsuit filed in N.D. Cal. by more than a dozen companies to strike down NHK/*Fintiv* rule. *Apple Inc. v. Hirshfeld*, N.D. Cal., No. 20-cv-06128.
Dismissed because institution decisions are not appealable.

Supreme Court petitions for certiorari challenging *Fintiv*:

- *Apple Inc. v. Optis Cellular Technology LLC*, case number 21-118, **denied** Jan. 18, 2022
- *Mylan Laboratories Ltd.v. Janssen Pharmaceutica NV*, case number 21-202, **denied** Jan. 18, 2022, and
- *Intel Corp. v. VLSI Technology LLC*, case number 21-888, pending.

Inequitable Conduct

Belcher Pharms. LLC v. Hospira, Inc., 11 F.4th 1345 (Fed. Cir. 2021)

- Patent directed to epinephrine formulations with claimed pH range of 2.8-3.3.
 - Overcame prior art rejection by showing criticality and unexpected results of claimed range.
- DC: Patent unenforceable for inequitable conduct.
 - Belcher CSO withheld material information with deceptive intent.
 - Material: JHP product; Sintetica product; and Stepensky reference.
 - Intent: knew of information, disclosed to FDA, argued unexpectedness to PTO
- FC: Affirmed.
 - Material: claims allowed after criticality argument and claims invalid as obvious over JHP product.
 - Intent to deceive is only reasonable inference.
 - CSO was active participant both the FDA approval process and the patent application drafting and prosecution; knew the unexpected results argument was false because knew of prior art using same range.
- Feb. 3, 2022, Judge Stark found case exceptional and awarded attorney's fees.
 - In approximately 30 patent bench trials, "this is the sole instance in which I have ever found an inequitable conduct case proven; and so clearly it stands out and is truly exceptional in every way."
 - This case is more than "just about a witness testifying poorly at trial or poorly drafted claims[.]"

FINNEGAN

See, <https://www.finnegan.com/en/insights/blogs/ip-fda-blog/testing-the-limits-of-the-sense-patent-owners-decision-not-to-appeal-obviousness-holding-created-but-for-materiality-and-knowledge-of-withheld-references-established-intent.html>

27

Prosecution Laches

Hyatt v. Hirshfeld, 998 F.3d 1347 (Fed. Cir. 2021)

- Hyatt filed 381 patent applications in the rush prior to June 8, 1995 ("GATT-Bubble" patents).
- Four at issue in this appeal; claim priority to applications filed in the 1970's and 80's.
 - Between October 1995 and 2003, Hyatt filed amendments to the four applications.
 - From 2003 to 2012, examination was stayed pending litigation (Hyatt filed district court complaints challenging USPTO rules).
 - In 2012, examination resumed in a special art unit, created specifically to examine Hyatt's applications.
 - The PTO issued a series of notifications to Hyatt to streamline prosecution, in light of significant challenges created by the large number of claims and priority assertions.
 - Claims were rejected, and the rejection was upheld on appeal with respect to some claims (leaving some in condition for allowance).
- Bench trial October 2017
 - Hyatt moved for judgment on partial findings pursuant to Rule 52(c) of the Federal Rules of Civil Procedure ("FED. R. CIV. P. 52(c)"). According to Hyatt, the USPTO failed to prove prosecution laches because:
- August 2018, the district court issued an order that prosecution laches did not bar issuance of those patents, and that the USPTO "failed to take the actions necessary to advance the prosecution of Hyatt's applications."
 - Only considering the time period prior to 2002; suspension of prosecution from 2003-2012 was the USPTO's responsibility. After 2012, the role of Hyatt's delays "in prosecuting applications other than the four at issue" is so circumspect that the [c]ourt must decline to consider it here."
 - Ordered the USPTO to issue patents.

FINNEGAN

See, <https://www.finnegan.com/en/insights/blogs/prosecution-first/if-you-snooze-you-lose-prosecution-laches-as-a-defense-by-the-pto.html>

28

Prosecution Laches

Hyatt v. Hirshfeld, 998 F.3d 1347 (Fed. Cir. 2021)

- FC: Reversed and remanded.
- District court misapplied the legal standard for prosecution laches.
 - “the PTO can assert the defense of prosecution laches in a § 145 action” “even if it did not previously issue rejections based on, or warnings regarding, prosecution laches during the prosecution of an application that is at issue in the § 145 action.”
- District court improperly discounted several factors that should have been considered in the totality of the circumstances.
- District court erred by placing all the blame for delay on the USPTO.
- USPTO’s prosecution laches evidence was sufficient to shift the burden to Hyatt to show that the delay was not “unreasonable and unexplained.”
- “Hyatt is entitled to present evidence that his delay did not cause prejudice.”
 - Show by preponderance of evidence that had a legitimate, affirmative reason to excuse Hyatt from responsibility for the delay.

What Will Happen?

Panasonic Corp. v. Getac Technology Corp., No. 8:19-cv-01118 (C.D. Cal.)

- Panasonic arguing that omicron, the latest COVID-19 variant, is “relatively mild” and not grounds to reschedule an in-person jury trial set to take place Feb. 15.
- Getac wants to postpone the trial until August.
- Judge: doesn’t really matter because court calendar is a “horror story” with many backlogged criminal cases and they’ll never get the Feb. 15 date anyway
 - “So when do I send the notice to you that you’re not going on that date? How polite would you like me to be?”
 - See <https://www.law360.com/articles/1455384?copied=1>

Polling Question 1

You file a U.S. patent application before June 8, 1995. But you don't want it to issue until the market matures and everyone infringes. You write a memo to your client extolling the virtue of issuance sometimes in the undetermined future. You appeal everything and really eat up those days and months. Finally, your pre-AIA patent issues. Is there a problem with prosecution laches?

Yes or No?

FINNEGAN

Polling Question 2

You file a U.S. patent application disclosing red, green, and yellow widgets. But you claim only a yellow widget and the patent ultimately issues. You maintain no continuations to pursue red or green widgets. Your competitor sells a green widget. Is there infringement under the Doctrine of Equivalents?

Yes or No?

FINNEGAN

Polling Question 3

You file a U.S. patent application disclosing red, green, and yellow widgets. But you claim only a yellow widget and the patent ultimately issues. You maintain no continuations to pursue red or green widgets. Your competitor sells a green widget. Is there infringement under the Doctrine of Equivalents?

Yes or No?

FINNEGAN

Polling Question 4

Your U.S. patent claim is directed to a machine comprising a widget and at least one surfboard. The alleged infringer uses two widgets and two surfboards in its machine. There is literal infringement.

Yes or No?

FINNEGAN

Thank You!



Contact Information:

Tom Irving
tom.irving@finnegan.com

Stacy Lewis
stacy.lewis@finnegan.com

Trademark Law Year in Review
The Trademark Modernization Act and
Select Cases from 2021



Nineteenth Annual IP and Social Justice Seminar

March 4, 2022

Doug (Chip) Rettew and Maxime Jarquin¹

¹ Doug Rettew is a partner in Finnegan's trademark and copyright group and focuses his practice on trademark, false advertising, design patent, and unfair competition litigation and disputes. Max Jarquin is a law clerk at Finnegan.

The Trademark Modernization Act

The Trademark Modernization Act of 2020 (TMA)² became effective on December 27, 2021. The Act's primary purpose is to provide the USPTO with new tools to clear unused (or "deadwood") registrations from the federal trademark register. To that end, the TMA creates two novel *ex parte* proceedings: expungement and reexamination.

By filing for expungement, a party may request the cancellation of a registration, for some or all of the goods or services, on the ground that the mark was *never* used in commerce for those goods or services.

When filing for reexamination, a party can cancel a registration on the ground that the mark was not used in commerce on or before a *relevant date* with respect to the registration's filing basis (use or intent-to-use). For a registration that was filed on a use-in-commerce basis (1(a)), the relevant date for reexamination is the *filing date* of the application. For a registration that was filed on an intent-to-use basis (1(b)), the relevant date for reexamination is the *later* between: the filing date for an amendment to allege use *or* the deadline for filing a statement of use, including all approved extensions thereof.

To be considered complete, a petition for expungement or reexamination must be made in writing and filed through TEAS, along with the following: a concise factual statement of the basis for the requested proceeding; evidence supporting a *prima facie* case of nonuse; evidence that the petitioner conducted a *reasonable investigation* to determine that the challenged mark was either never used in commerce (expungement) or not used in commerce on or before a relevant date (reexamination); and the payment of a \$400 fee per class of goods or services challenged. An expungement proceeding can only be brought 3 to 10 years after the registration date,³ and a reexamination proceeding must be brought within 5 years of the registration date.

Additionally, the TMA establishes nonuse as a new ground for cancellation. Third parties can now file a petition to cancel a registration any time after the first 3 years of the registration date of a mark on the ground that it was never used in commerce. The petition must be filed through ESTTA for a \$600 fee per class. This new development is significant because a petition to cancel on the ground of nonuse can provide quicker relief than an expungement proceeding, especially where the cancellation results in a default judgement.

Other important features of the Act include: the codification of the letter-of-protest procedure, shortened office action response deadlines, and the restoration of the presumption of irreparable harm (on a showing of success, or likely success, on the merits) under the Lanham Act. By codifying the existing letter-of-protest procedure whereby third parties submit evidence during prosecution to challenge the registrability of marks, the TMA provides that the

² Trademark Modernization Act of 2020 as incorporated in Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, Subtitle B, Section 221.

³ The ten-year limit does not apply for expungement proceedings instituted before December 27, 2023.

Director of the USPTO will consider whether to include letter-of-protest evidence into the record of an application within 2 months of a letter's filing date. The fees for letters of protest remain unchanged and are currently set at \$50 per submission.

Before the TMA was enacted, the response deadline for an office action was 6 months from the issuance of the office action. Now, under the implementing rule for the TMA, registrants have 3 months to respond to office actions issued during examination of an application or post-registration. This shortened timeframe does not apply to Madrid applications (filed under section 66(a)) for which the deadline remains 6 months. Registrants may request a single three-month extension for a \$125 fee. The new office action response deadlines will only come into effect on December 1, 2022.

Finally, the TMA also brings an important doctrinal shift for plaintiffs in trademark infringement cases. For over a decade, courts were split on the standard for injunctive relief in Lanham Act cases after the Supreme Court eliminated a presumption of irreparable harm in patent cases.⁴ The TMA settled the question by amending the Lanham Act to create a presumption of irreparable harm for plaintiffs seeking injunctive relief in trademark cases. This means that brand owners who prove success (or likely success, in certain circumstances) on the merits of their claim will once again enjoy a legal presumption that the harm caused by the violation is irreparable.⁵

New Developments in Functionality

2021 was an eventful year for the doctrine of functionality. Functionality effectively prevents the protection and registration of utilitarian products or product features (defined in different ways, as discussed below). Functionality is a powerful doctrine because once it is proven by the party challenging the feature or mark at issue, it outweighs any evidence of secondary meaning or actual confusion that the other side presents.⁶ If found functional, a feature or design is not protectable under any circumstance, and the existence of alternative designs capable of performing the same function is irrelevant.⁷ As such, functionality is often dispositive in trade dress disputes.

The functionality doctrine emerged as a way to confine the protection of utility and functional designs to the exclusive domain of patent law.⁸ Functionality also plays an important role in promoting free competition by allowing competitors to copy useful, functional features that are deemed necessary to compete effectively.⁹ The theory behind the doctrine was well articulated by the Supreme Court as follows:

⁴ See *eBay Inc. v. MercExchange*, 547 U.S. 388 (2006).

⁵ All the foregoing information is available at: <https://www.uspto.gov/trademarks/laws/2020-modernization-act>.

⁶ *Id.*

⁷ *TrafFix*, 532 U.S. at 33-34.

⁸ *Id.*

⁹ *Id.*

The functionality doctrine prevents trademark law, which seeks to promote competition by protecting a firm's reputation, from instead inhibiting legitimate competition by allowing a producer to control a useful product feature. It is the province of patent law, not trademark law, to encourage invention by granting inventors a monopoly over new product designs or functions for a limited time, 35 U. S. C. §§154, 173, after which competitors are free to use the innovation. If a product's functional features could be used as trademarks, however, a monopoly over such features could be obtained without regard to whether they qualify as patents and could be extended forever (because trademarks may be renewed in perpetuity).

Qualitex Co. v. Jacobson Prods. Co., 514 U.S. at 164-65 (1995).

In 1998, Congress amended the Lanham Act to make functionality (1) a ground for ex parte rejection, (2) a ground for opposition of an application and cancellation of a registration, and (3) a statutory defense to (*i.e.*, a way to challenge) an incontestably registered mark.¹⁰ Moreover, Section 43(a)(3) of the Lanham Act provides that: "In a civil action for trade dress infringement under this Act for trade dress not registered on the principal register, the person who asserts the trade dress protection has the burden of proving that the matter sought to be protected is not functional."¹¹ If a mark has been registered with the U.S. Patent and Trademark Office, it is presumed to be non-functional; although not impervious to challenge.¹²

Functionality essentially comes in two forms: utilitarian and aesthetic functionality. This year, a pair of appellate courts issued decisions shedding light on these potent tools for invalidating asserted trade dress: *Ezaki Glico Kabushiki Kaisha v. Lotte Int'l Am. Corp.*, 977 F.3d 261, 264 (3d Cir. 2020) (involving utilitarian functionality) and *LTTB LLC v. Redbubble, Inc.*, 840 F. App'x 148, 149 (9th Cir. 2021) (involving aesthetic functionality).

A. The "Pocky" Case: *Useful (Not Essential) Cookie Sticks are Functional*

They say imitation is the highest form of flattery, but for Ezaki Glico, the company behind the famous and beloved chocolate-covered cookie stick, Pocky, competitor imitation is a constant source of frustration. One competitor in particular, Lotte, sells its Pepero cookie, which, like Pocky, is stick-shaped and partly coated in chocolate or flavored cream.

¹⁰ *Id.*; see also Pub. L. No. 105-330, 112 Stat. 3064 (1998). See § 19:75 (ex parte bar to registration), § 20:21 (ground for opposition), § 20:56.50 (ground for cancellation), and § 7:84 (statutory defense to an incontestably registered mark).

¹¹ 15 U.S.C. § 1125(a)(3).

¹² 15 U.S.C. § 1052(e)(5).



In 2015, Ezaki Glico sued Lotte in the District Court for the District of New Jersey alleging trademark infringement and unfair competition in violation of the Lanham Act and the New Jersey Fair Trade Act.¹³ The District Court granted summary judgment for Lotte after finding Pocky's trade dress configuration is functional and therefore not protectable.¹⁴ Ezaki Glico appealed to the Third Circuit.

On appeal, the Third Circuit noted that both the Lanham Act and New Jersey Fair Trade Act claims depend on the validity of the Pocky trade dress and focused its analysis on whether or not the trade dress is functional.¹⁵ The court noted that because copying is a legal part of market competition, "even if copying would confuse consumers about a product's source, competitors may copy unpatented functional designs."¹⁶

Unsurprisingly, Ezaki Glico urged the court to adopt a narrow interpretation of what it means for a trade dress to be functional and argued that the term should be equated with what is "essential."¹⁷ But the court looked to the term's ordinary meaning and determined that a product's configuration is functional when it is useful.¹⁸ In so doing, the court looked to dictionary definitions; the Supreme Court decisions in *Qualitex*, *TrafFix*, and *Wal-Mart*; and the Lanham Act's relationship to the Patent Act.¹⁹ On the latter point, the Third Circuit reasoned that trade dress, like trademark law more broadly, is designed to protect the owner's goodwill and to prevent consumer confusion from occurring—not to defend against the copying of an original work (copyright law) or an invention (patent law).²⁰

Against this backdrop, the court turned its attention to whether or not functionality had been proven, noting the several ways in which this can be done. The court's non-exhaustive list of considerations included evidence directly showing "that a feature or design makes a product

¹³ *Ezaki Glico Kabushiki Kaisha v. Lotte Int'l Am. Corp.*, 977 F.3d 261, 264 (3d Cir. 2020).

¹⁴ *Id.*

¹⁵ *Id.* at 264-65.

¹⁶ *Id.* at 266.

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.* at 265-67.

²⁰ *Id.* at 265-66.

work better,” the recognition and praise of a feature’s usefulness by the product’s marketer, a utility patent on the feature, and the limited ways to design a product.²¹

Addressing each consideration in turn, the court first determined that “every feature of Pocky’s registration relates to the practical functions of holding, eating, sharing, or packing the snack.”²² Specifically, it noted that the uncoated handle of each stick allows people to eat it without getting their hands dirty, and the shape of the stick itself makes the cookie easy to hold, eat, and share.²³ Second, the court stated that Ezaki Glico promotes the design through advertisements, which tout its useful features and state “Pocky lends itself to sharing anytime, anywhere, and with anyone.”²⁴ Third, the court found Ezaki Glico’s utility patent irrelevant to the functionality analysis of the trade dress features as none of the claimed features in the manufacturing method overlapped with its trade dress.²⁵ Thus, any consideration of the utility patent by the district court was in error, though immaterial. Finally, even though there were alternative cookie designs available to Lotte, the court determined there was ample evidence that the product design was functional.²⁶

In conclusion, recognizing the separate domains of patents and trademarks, the court held that Ezaki Glico could not rely on its (now invalid) trade dress to prevent competitors from using the functional features of the cookie and affirmed the district court’s decision, aptly stating, “That’s the way the cookie crumbles.”²⁷

B. Pun Intended, but Not Infringing: Ninth Circuit Finds LETTUCE TURNIP THE BEET Aesthetically Functional

TTB, LLC is a small business that has seen success due to its vegetable-based pun LETTUCE TURNIP THE BEET.²⁸ LTTB owns four trademark registrations for the pun for various apparel products, tote bags, and online retail store services, among other things.²⁹ Many of LTTB’s products are emblazoned with the phrase:

²¹ *Id.* at 267-78.

²² *Id.* at 268.

²³ *Id.*

²⁴ *Id.* at 269.

²⁵ *Id.*

²⁶ *Id.*

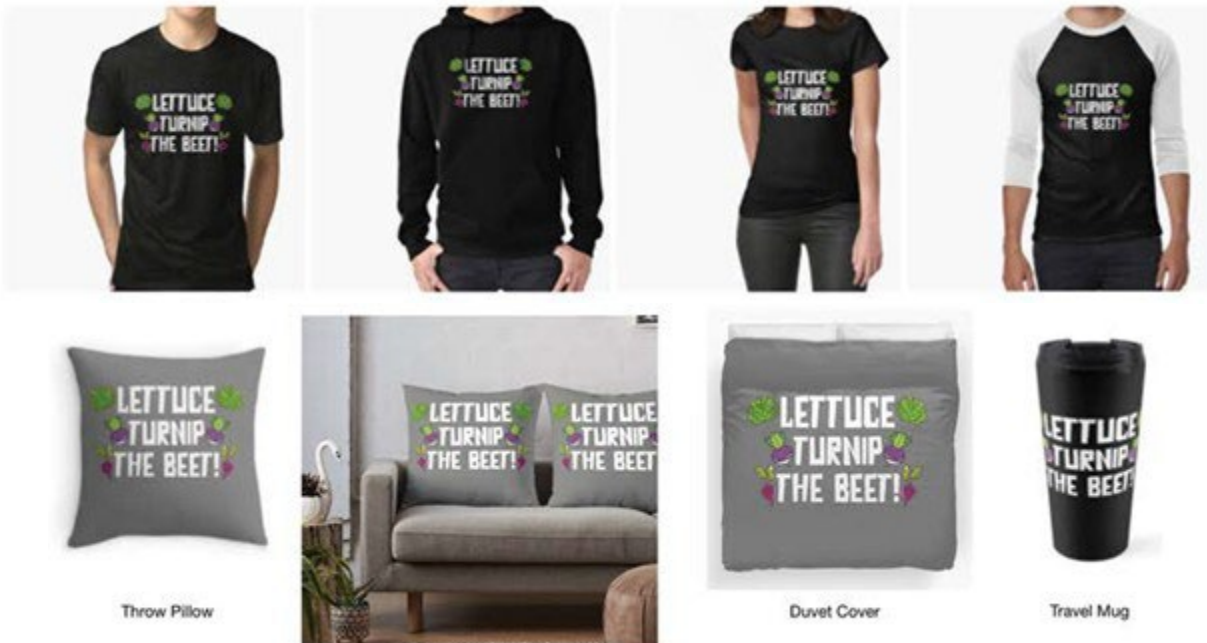
²⁷ *Id.* at 270.

²⁸ *LTTB LLC v. Redbubble Inc.*, 385 F. Supp. 3d 916, 917 (N.D. Cal. 2019).

²⁹ *Id.*



LTTB brought suit in the Northern District of California against Redbubble, Inc. in January 2018 for counterfeiting, trademark infringement, unfair competition, and false designation of origin.³⁰ Redbubble is an online marketplace where independent artists can upload and sell their designs on everyday products such as apparel, tote bags, stickers, etc.³¹ Some of the designs available on Redbubble's website include LETTUCE TURNIP THE BEET:



³⁰ *LTTB LLC v. Redbubble, Inc.*, 840 F. App'x 148, 149 (9th Cir. 2021).

³¹ *LTTB*, 385 F. Supp. 3d at 917.

In July 2019, the district court granted Redbubble’s motion for summary judgment, finding that, under the doctrine of aesthetic functionality, LTTB could not prevent others from displaying the LETTUCE TURNIP THE BEET pun on products.³² LTTB “[was] not entitled to preempt use of the pun under the guise of trademark law.”³³ The district court, however, was careful to note that its ruling did not mean that LTTB has *no* viable trademark rights, just that LTTB cannot “preclude others from displaying the pun on products, absent a showing of source-confusion.”³⁴ The Ninth Circuit upheld the ruling, concluding that LTTB “failed to raise a triable issue that its marks serve the trademark function”³⁵

The Ninth Circuit affirmed the district court’s findings that the LETTUCE TURNIP THE BEET pun was aesthetically functional.³⁶ First, it held that the district court did not erroneously rely on the test for aesthetic functionality articulated in *Job’s Daughters*³⁷ because the case remains good law and the result would be the same under the test as articulated in *Automotive Gold*, namely: (1) whether the alleged non-trademark function is essential to the use or purpose of the item or affects its cost or quality, and (2) whether protection of the feature would put competitors at a significant non-reputation-related disadvantage.³⁸ It found that the t-shirts would still function as t-shirts without the marks, use of the marks did not alter the cost structure or add to the quality of the products, and exclusive use of the marks would put competitors at a significant non-reputation-related disadvantage.³⁹ In short, LTTB presented no evidence that consumers buy its punny t-shirts because the t-shirts identify LTTB as the *source*, as opposed to because the consumers enjoy the aesthetic function of the pun.⁴⁰

The Ninth Circuit also held that, given the district court’s findings regarding functionality, the district court did not err in (1) failing to address uses of the marks on Redbubble’s website and in online advertising and (2) the issue of likelihood of

³² *LTTB*, 385 F. Supp. 3d at 920–22.

³³ *Id.* at 918.

³⁴ *Id.* at 922.

³⁵ *LTTB*, 840 F. App’x at 149.

³⁶ *Id.* at 152.

³⁷ In *Job’s Daughters*, the defendant produced jewelry bearing the plaintiff’s collective membership trademark for sale to the members of plaintiff’s organization. Int’l Ord. of Job’s Daughters v. Lindeburg and Co., 633 F.2d 912 (9th Cir. 1980). Noting that the plaintiff did not produce any evidence of actual confusion, the court held that the defendant’s use did not infringe the plaintiff’s mark, in part because the application of the mark to jewelry worn by members was “functional” in that it enabled the wearer to “express her allegiance to the organization.” 633 F.2d at 918. The reasoning of *Job’s Daughters* has been forcefully criticized by commentators and courts. 1 MCCARTHY, § 7:82; *W.T. Rogers Co. v. Keene*, 778 F.2d 334, 340 (7th Cir. 1985) (rejecting *Job’s Daughters* “as have most other circuits”); *Univ. of Georgia Athletic Ass’n v. Laite*, 756 F.2d 1535, 1546 (11th Cir. 1985).

³⁸ *LTTB*, 840 F. App’x at 150.

³⁹ *Id.* at 150–51.

⁴⁰ *Id.* at 151.

confusion.⁴¹ The Court also rejected LTTB's arguments that the district court improperly ignored LTTB's design marks and improperly relied on the U.S. Patent and Trademark Office's initial rejection of one of LTTB's trademark application as decorative or ornamental (the application was ultimately approved once LTTB submitted examples of the mark on product hang tags as opposed to on the front of its shirts).⁴²

While infringement was not found in this case, it is clear from the district court's ruling that aesthetic functionality is not an impermeable shield. Placing a mark on a t-shirt, tote bag, or mug is not an automatic defense:

. . . [C]ompanies that have already established [a] famous mark for selling a product—for instance Coca-Cola, Volkswagen, Audi, or Nike—may thereafter be able also to exploit consumer interest in the mark by selling t-shirts or other products emblazoned with such marks, and preclude others from doing so

. . .

Redbubble instead appropriately frames the argument as precluding LTTB from showing a likelihood of confusion as to source, where the mere use of the pun on the face of various products cannot be source-identifying.

. . .

[N]othing in this ruling precludes LTTB from enforcing its rights against a defendant who markets a products [sic] misleadingly suggesting LTTB is the source.

LTTB, 385 F. Supp. 3d at 921-22.

In the end, the Ninth Circuit's decision has kept the doctrine of aesthetic functionality alive, while being careful to caution that source-identifying uses are not exempt.

Initial Interest Confusion

In addition to functionality, another doctrine that was at the forefront of trademark jurisprudence in 2021 is initial interest confusion. Initial interest confusion is a theory defined as "infringement [] based upon confusion that creates initial customer interest, even though no actual sale is finally completed as a result of the confusion."⁴³ Most courts now recognize the initial interest confusion theory as part of the likelihood of confusion inquiry in trademark infringement.⁴⁴ Last year, the Eighth Circuit finally embraced the theory, and the Fifth Circuit recognized its application in the context of internet search engines—a matter of first impression for that court.

⁴¹ *Id.*

⁴² *Id.* at 151-52.

⁴³ 4 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION, § 23:6 (5th ed. 2021).

⁴⁴ *Id.*

In *Select Comfort v. Baxter*, plaintiff, a mattress company, sued a competitor for trademark infringement and dilution over its use of plaintiff's registered marks (including SLEEP NUMBER, and SELECT COMFORT) and similar phrases in various online advertising formats, such as website URLs, search inquiry paid terms, and embedded links in third-party sites.⁴⁵ Plaintiff's theory was that defendant used these techniques to divert customers to its own websites and phone lines and then failed to dispel consumer confusion and made false representations about its products and plaintiff's products.⁴⁶ The district court held that because purchasers of mattresses are careful and sophisticated consumers, a claim of initial interest confusion could not proceed, and plaintiff would have to prove and likelihood of confusion at the time of purchase.⁴⁷ On appeal, the Eighth Circuit reversed, holding that plaintiffs should not be barred from proving presale, initial-interest confusion.⁴⁸ The court came to this conclusion by stating that the likelihood of confusion inquiry in trademark infringement cases is a "flexible, context-specific, and relative-rather-than-mechanical approach," and because "the consumer experience differs by products," the likelihood of confusion determination is considered a finding of fact.⁴⁹ As such, the court's factors "provide guidance but do not draw bright lines that might constrain the general test for confusion."⁵⁰ In sum, the court adopted the initial interest confusion theory because it is consonant with the jury's discretion to make findings of fact (including presale confusion) as part of the likelihood of confusion analysis.

In *Jim S. Adler v. McNeil Consultants*, the Fifth Circuit held that a plaintiff had sufficiently alleged likelihood of confusion when defendant, a competitor, purchased keywords for search-engine advertising that included some of plaintiff's registered marks.⁵¹ Jim S. Adler is a personal injury law firm, and McNeil operates a lawyer-referral website and call center.⁵² When McNeil purchased Google keyword ads for Adler's marks, thereby ensuring that McNeil's advertisements would appear when a user performed a Google search for Adler's services, Adler sued McNeil for trademark infringement.⁵³ The district court granted McNeil's motion to dismiss when a magistrate judge found that Adler's claims were based solely on McNeil's *purchase* of the keywords and McNeil's generic advertisements did not include any of Adler's marks, and that as a result Adler could not plead a likelihood of confusion as a matter of law.⁵⁴ The Fifth Circuit reversed, holding that "whether an advertisement incorporates a trademark that is visible to the consumer is a relevant but not dispositive factor in determining a likelihood of confusion in search-engine advertising cases."⁵⁵ Moreover, the court noted that the generic

⁴⁵ See *Select Comfort Corp. v. Baxter*, 996 F.3d 925 (8th Cir. 2021).

⁴⁶ *Id.* at 930.

⁴⁷ *Id.* at 931.

⁴⁸ *Id.* at 935.

⁴⁹ *Id.* at 934-35.

⁵⁰ *Id.* at 935.

⁵¹ *Jim S. Adler, P.C. v. McNeil Consultants, L.L.C.*, 10 F.4th 422 (5th Cir. 2021).

⁵² *Id.* at 425.

⁵³ *Id.*

⁵⁴ *Id.* at 425-26.

⁵⁵ *Id.* at 430.

nature of McNeil's advertisements "enhances rather than dispels the likelihood of initial interest confusion."⁵⁶

Fraud in Trademark Prosecution

Finally, 2021 also marked a major procedural change for trademark owners and practitioners. Up until last year, plaintiffs before the Trademark Trial and Appeal Board (TTAB) could establish fraud in a declarant's statement only by showing that the declarant *intended* to deceive the USPTO.⁵⁷ This made fraud particularly difficult to prove without glaring evidence of fraudulent intent.⁵⁸ In *Chutter, Inc. v. Great Management Group*, the TTAB found that a declarant's failure to read an inaccurate declaration before submitting it to the USPTO constituted "reckless disregard for the truth" and therefore cancelled the registration on grounds of fraud.⁵⁹ In this case, Chutter filed a cancellation action and civil action against Great Management over registration of the mark DANTANNA, for restaurant services and marinara sauce, claiming prior rights to the mark DAN TANA's for restaurant services and marinara sauce. When Great Management filed a Section 15 declaration to obtain incontestable status for the DANTANNA registration, its counsel falsely stated in the declaration that there were no civil actions or USPTO proceedings pending against the registration. Chutter pointed to dicta in the Federal Circuit's opinion in *In re Bose* suggesting that situations of "reckless disregard" for the truth of a statement may satisfy the intent to deceive requirement to prove fraud.⁶⁰ The TTAB agreed with Chutter, stating that "[a] declarant is charged with knowing what is in the declaration being signed, and by failing to make an appropriate inquiry into the accuracy of the statements the declarant acts with a reckless disregard for the truth."⁶¹ As such, because Great Management's counsel was charged with knowledge that the statements in the declaration were false and still submitted it to the USPTO, the TTAB held that counsel had committed fraud, and it granted the cancellation of the DANTANNA registration. The *Chutter* decision is important because it has lessened the burden of proof for fraud in trademark prosecution. As a result, trademark practitioners will now have to exercise even greater caution and attention to detail in filing documents with the USPTO.

⁵⁶ *Id.* at 429.

⁵⁷ See *In re Bose Corp.*, 580 F.3d 1240, 1245 (Fed. Cir. 2009).

⁵⁸ See <https://www.finnegan.com/en/insights/blogs/incontestable/ttab-recklessly-false-trademark-filings-constitute-fraud.html>.

⁵⁹ *Chutter, Inc. v. Great Management Group, LLC*, 2021 U.S.P.Q.2d 1001 (T.T.A.B. 2021).

⁶⁰ *In re Bose Corp.*, 580 F.3d at 1246, n.2.

⁶¹ See <https://www.finnegan.com/en/insights/blogs/incontestable/ttab-recklessly-false-trademark-filings-constitute-fraud.html>.

CASE ACT SMALL-CLAIMS ENFORCEMENT THROUGH THE COPYRIGHT CLAIMS BOARD

Excerpted from the forthcoming 2022 updates to Chapter 4 (Copyright Protection in Cyberspace)

E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition

A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

(These excerpts are unrevised page proofs for the current update and may contain errors. Please email the author at ballon@gtlaw.com for a complimentary copy of the final published version.)

IP LAW YEAR IN REVIEW

4TH ANNUAL HBCU TECH LAW SUMMIT AND 19TH ANNUAL IP AND SOCIAL JUSTICE CLE SEMINAR

INSTITUTE FOR INTELLECTUAL PROPERTY AND SOCIAL JUSTICE
HOWARD UNIVERSITY SCHOOL OF LAW
MARCH 3-4, 2022

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles: 1840 Century Park East, Ste. 1900 Los Angeles, CA 90067 Direct Dial: (310) 586-6575 Direct Fax: (310) 586-0575	Silicon Valley: 1900 University Avenue, 5th Fl. East Palo Alto, CA 914303 Direct Dial: (650) 289-7881 Direct Fax: (650) 462-7881	Washington, D.C.: 2101 L Street, N.W., Ste. 1000 Washington, D.C. 20037 Direct Dial: (202) 331-3138 Fax: (202) 331-3101
--	---	--

Ballon@gtlaw.com

<www.ianballon.net>

LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
(Thomson West 2022 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (888) 728-7677
www.ianballon.net



Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal
Circuits

U.S. Supreme Court

JD, LLM, CIPP/US

Ballon@gtlaw.com

LinkedIn, Twitter, Facebook: IanBallon

Los Angeles

1840 Century Park East
Suite 1900

Los Angeles, CA 90067

T 310.586.6575

F 310.586.0575

Silicon Valley

1900 University Avenue
5th Floor

East Palo Alto, CA 94303

T 650.289.7881

F 650.462.7881

Washington, D.C.

2101 L Street, N.W.

Suite 1000

Washington, DC 20037

T 202.331.3138

F 202.331.3101

Ian C. Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and TCPA class action suits.

Ian is also the author of the leading treatise on internet and mobile law, [E-Commerce and Internet Law: Treatise with Forms 2d edition](#), the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of intellectual property law issues. In addition, he serves as [Executive Director of Stanford University Law School's Center for the Digital Economy](#). He also chairs [PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation](#) conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian was named the Lawyer of the Year for Information Technology Law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of Best Lawyers in America (including lawyer of the year for 2022). In 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder's* 2017 Litigation Departments of the Year Awards. He was also recognized as the 2012 [New Media Lawyer of the Year](#) by the Century City Bar Association. In 2010, he was the recipient of the California State Bar Intellectual Property Law section's [Vanguard Award for significant contributions to the development of intellectual property law](#). Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2021), and has been listed as a Northern California Super Lawyer every year from 2004 through 2021 and as one of the top 100 lawyers in California. He is also listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology.

Ian holds JD and LLM degrees and the [CIPP/US certification from the International Association of Privacy Professionals \(IAPP\)](#).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 1



THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

4.08[8] CASE Act Small-Claims Enforcement through the Copyright Claims Board

The Copyright Alternative in Small-Claims Enforcement Act of 2020—or CASE Act—provides for alternative resolution of certain small claims through the U.S. Copyright Office’s Copyright Claims Board.¹ Pursuant to the CASE Act, the Copyright Claims Board must be established by December 22, 2021 (with authority delegated to the Copyright Office to delay that time for up to an additional six months). Resolving eligible disputes before the Copyright Claims Board, instead of court, is supposed to be entirely voluntary, but persons and entities that fail to opt out within 60 days following service may find themselves subject to a CASE act proceeding that they might otherwise have preferred to resolve through federal court litigation (which, among other things, ensures the right to a jury trial, broader discovery, and adjudication by a federal judge subject to binding precedent with full rights of appeal) or not at all.² If a party opts out of a Copyright Claims Board proceeding, the other party may—but is by no means required to—file suit in federal court. Given the cap on damages applicable to CASE Act determinations by the Copyright Claims Board and the ability of individuals and even companies to represent themselves before the Board without having to retain counsel, opting out won’t necessarily trigger federal court litigation in every instance. The CASE Act, however, likely will increase the volume of copyright claims overall, as those who otherwise would not have chosen to file suit seek to vindicate their rights before the Copyright Claims Board. The CASE Act also potentially could be abused by copyright trolls seeking quick settlements from large companies and by copyright owners (or ostensible rights owners) or competitors seeking to use the Board’s procedures as an inexpensive mechanism to keep material offline in response to counter notifications submitted by users pursuant to 17 U.S.C.A. § 512(g) of the Digital Millennium Copyright Act, although the CASE Act directs the Copyright Office to take measures to avoid abuse.

The CASE Act provides a means for voluntary alternative

the claimant.”).

[Section 4.08[8]]

¹See 17 U.S.C.A. §§ 1501 to 1511.

²See 17 U.S.C.A. § 1506(g)(1) (providing that the right to opt-out is waived in most cases if not timely asserted within 60 days of service).

dispute resolution for three types of claims (and certain related counterclaims asserted solely against the claimant arising out of the same transaction or occurrence, or an agreement (such as a license) that could affect the relief awarded to the claimant)³ —

- infringement of an exclusive right in a copyrighted work⁴ by a legal or beneficial owner of the exclusive right at the time of infringement, for which the claimant seeks damages⁵ (pursuant to 17 U.S.C.A. § 1504(c)(1), for damages as permitted by 17 U.S.C.A. § 504(e)(1)),
- noninfringement (pursuant to 17 U.S.C.A. § 1504(c)(2)), or
- misrepresentation in connection with a notification of claimed infringement or a counter notification pursuant to 17 U.S.C.A. § 512(f) of the Digital Millennium Copyright Act⁶ (under 17 U.S.C.A. § 1504(c)(3), but with relief limited to that authorized by the CASE Act).⁷

Other potential claims or counterclaims may not be

³See 17 U.S.C.A. § 1504(c)(4). That section permits counterclaims asserted solely against a claimant (and not others):

- (A) pursuant to which the counterclaimant seeks damages, if any, within the limitations set forth in subsection (e)(1) [17 U.S.C.A. § 1504(e)(1)]; and
- (B) that—
 - (i) arises under section 106 or section 512(f) and out of the same transaction or occurrence that is the subject of a claim of infringement brought under paragraph (1), a claim of noninfringement brought under paragraph (2), or a claim of misrepresentation brought under paragraph (3) [of 17 U.S.C.A. § 1504(c)]; or
 - (ii) arises under an agreement pertaining to the same transaction or occurrence that is the subject of a claim of infringement brought under paragraph (1) [17 U.S.C.A. § 1504(c)(1)], if the agreement could affect the relief awarded to the claimant.

Id.

⁴The exclusive rights of a copyright owner pursuant to 17 U.S.C.A. § 106 are analyzed in section 4.04[1].

⁵As noted later in this section, the Board is also authorized to include a requirement that a party cease certain conduct, if a party agrees to do so in order to mitigate the amount of any damage award. See 17 U.S.C.A. §§ 1504(e)(2), 1504(e)(1).

⁶Section 512(f) of the DMCA is analyzed in section 4.12[9][D] in this chapter.

⁷See 17 U.S.C.A. §§ 1501(1), 1504(c).

brought.⁸ Nor may claims finally adjudicated by a court of competent jurisdiction be relitigated.⁹ Claims pending before a court of competent jurisdiction likewise are not subject to a determination by the Copyright Claims Board, unless the court has granted a stay to permit the claim or counterclaim to proceed before the Copyright Claims Board.¹⁰ Legal or equitable defenses, however, may be asserted in response to claims or counterclaims.¹¹

Complaints initiated with the Copyright Claims Board may involve a single claim or multiple claims, and may be brought by multiple claimants against multiple respondents, provided that all claims asserted in any one proceeding “arise out of the same allegedly infringing activity or continuous course of infringing activities and do not, in the aggregate, result in a recovery . . . for damages that exceed the limitations . . .” for recovery in Copyright Claims Board proceedings set forth in 17 U.S.C.A. § 1504(e)(1),¹² which are discussed below later in this subsection and typically will be capped at \$30,000 per proceeding (or less for claims for infringement of untimely registered works).

Thus, claims for injunctive relief or more complicated multi-party or multi-claim disputes will not be suitable for Copyright Claims Board adjudication (except if and to the extent that a court stays individual claims or counterclaims to allow resolution of just those claims or counterclaims before the Board). Parties with potentially substantial damage claims may also prefer to file suit in court. On the other hand, individuals and smaller companies may prefer to avoid the legal fees associated with litigation, by initiating a claim with the Copyright Claims Board and either representing themselves, obtaining pro bono representation from a law student, or retaining a lawyer willing to handle a dispute where the maximum potential recovery is \$30,000. Parties seeking to assert claims for misrepresentations in notifications and counter notifications, pursuant to 17 U.S.C.A. § 512(f), may also prefer to avail themselves of the remedies available before the Copyright Claims Board given that damages in section 512(f) cases are often difficult to prove or *de*

⁸See 17 U.S.C.A. § 1504(d)(1).

⁹See 17 U.S.C.A. § 1504(d)(2).

¹⁰See 17 U.S.C.A. § 1504(d)(2).

¹¹See 17 U.S.C.A. § 1504(c)(5).

¹²See 17 U.S.C.A. § 1504(c)(6).

minimis (especially when asserted by individual users, as opposed to copyright owners or service providers).¹³

Claims may be brought by both eligible U.S. and foreign persons and entities. Claims may not be asserted, however, *against* a person or entity residing outside the United States, but if such a person or entity brings a claim, a counterclaim may be asserted against that person or entity.¹⁴

Claims and counterclaims likewise may not be asserted by or against federal or state government entities.¹⁵

Copyright Claims Board complaints alleging copyright infringement also may qualify as actions taken in response to counter notifications under 17 U.S.C.A. § 512(g) of the Digital Millennium Copyright Act¹⁶ and therefore may provide copyright owners with a lower cost and lower risk alternative to filing suit in federal court to prevent material from being restored by a service provider in response to a DMCA counter notification. This provision of the CASE Act, however, potentially could be abused by some copyright owners (especially mere applicants for registration¹⁷) to keep material offline for extended period of time. Conversely, the restriction on initiating Copyright Claims Board proceedings against foreign nationals may limit its utility for copyright owners in cases of alleged infringement by non-Americans. While a user who submits a counter notification to a service provider to restore access to material taken down in response to a DMCA notification must assent to jurisdiction in a U.S. court as part of the counter notification,¹⁸ that user need not consent to proceedings before the Copyright Claims Board

¹³See *infra* § 4.12[9][D] (analyzing section 512(f) claims).

¹⁴See 17 U.S.C.A. § 1504(d)(4).

¹⁵See 17 U.S.C.A. § 1504(d)(3).

¹⁶See 17 U.S.C.A. § 1507(d); see generally *infra* § 4.12[9][C] (analyzing counter notifications and the requirements for copyright owners to submit evidence of filing a lawsuit or initiating a Copyright Claims Board action to prevent restoration of removed material in response to a DMCA notification).

¹⁷As discussed later in this section, when a claim is brought by an applicant, the proceeding may be held in abeyance pending a determination on registration—potentially for a year or longer. See 17 U.S.C.A. §§ 1505(a), 1505(b). Yet under the DMCA, the material would remain offline pending a legal determination of the merit of the claim. See 17 U.S.C.A. § 512(g); *infra* § 4.12[9][C].

¹⁸See 17 U.S.C.A. § 512(g)(2)(C); see generally *infra* § 4.12[9][C] (analyzing counter notifications and the requirements for copyright own-

(and likely would have little incentive to do so) and the 60 day period to opt out would not apply since any complaint brought against a foreign person or entity would be invalid.

Copyright Claims Board proceedings will be adjudicated pursuant to the Copyright Act, judicial precedent, and regulations to be promulgated by the Copyright Office.¹⁹ Given circuit splits and local practice under different provisions of the Copyright Act, parties will need to assess in individual cases whether they are better off proceeding before the Copyright Claims Board or in court, based on circuit court law and local practice. Where judicial precedents are in conflict, the CASE Act directs the Copyright Claims Board to apply the law of the federal jurisdiction where the case could have been brought or, where there are more than one such jurisdictions, the one that the “Board determines has the most significant ties to the parties and conduct at issue.”²⁰ Needless to say, a plaintiff may sue in any district where venue is proper (and where the court has personal jurisdiction over the defendant)—not simply in the court that has the most significant ties.²¹

Proceedings will take place at the office of the Copyright Claims Board, but in-person appearances will not be required. Decisions generally will be rendered based on written submissions and internet-based video applications and other telecommunications facilities (except where material evidence or testimony cannot be furnished by these means).²² A party may, but is not required, to be represented by an attorney or a law student qualified under applicable law that permits law students to appear pro bono.²³ Other aspects of Board proceedings (including provisions for settlement, evidentiary submissions, hearings and limited discovery) are set forth in 17 U.S.C.A. § 1506 and likely will be augmented by Copyright Office regulations. As noted earlier in this section, a party properly served with notice of a Copyright Claims Board proceeding has the unrestricted right to opt-

ers to submit evidence of filing a lawsuit or initiating a Copyright Claims Board action to prevent restoration of removed material in response to a DMCA notification).

¹⁹See 17 U.S.C.A. § 1503(b)(1).

²⁰See 17 U.S.C.A. § 1506(a)(2).

²¹See generally *infra* chapters 53 (personal jurisdiction), 54 (venue).

²²See 17 U.S.C.A. § 1506(c).

²³See 17 U.S.C.A. § 1506(d).

out, but loses that right, and accordingly also loses the right to litigate the claim in federal court (and is deemed to have waived its right to a jury trial), if it fails to do so within 60 days of being served²⁴ (although the Board has discretion to extend this period in exceptional circumstances²⁵). The CASE Act does, however, allow any party (including presumably a party who missed the opportunity to opt out) to obtain dismissal of the proceeding if the party receives notice of a pending or putative class action, arising out of the same transaction or occurrence.²⁶

Conversely, federal courts may refer eligible cases for adjudication of claims or counterclaims by the Copyright Claims Board, with the consent of the parties, as an alternative dispute resolution process.²⁷

Where a lawsuit is filed that is already the subject of a Copyright Claims Board proceeding, the court “shall issue a stay or enter such other relief as the court determines appropriate”²⁸

Damages in a Copyright Claims Board proceeding will be capped at \$30,000, exclusive of attorneys’ fees and costs.²⁹ In addition to the cap, the CASE Act creates a financial incentive for a respondent to agree to allow the Board to include in its final determination a requirement that the respondent cease activity that is found to be infringing, including removing or disabling access to, or destroying, infringing materials (or for claims brought under section 512(f) for misrepresentations in a DMCA notification or counter notification, that the respondent cease sending takedown notices or counter notices to the other party regarding the conduct at issue before the Board, if that notice or counter notice is found to be a knowing material misrepresentation).³⁰

For infringement, a claimant may elect, at any time before a final determination is rendered, actual damages and profits

²⁴See 17 U.S.C.A. § 1506(g)(1).

²⁵See 17 U.S.C.A. § 1506(i).

²⁶See 17 U.S.C.A. § 1506(q)(3). Other grounds for voluntary dismissal are set forth in section 1506(q).

²⁷See 17 U.S.C.A. § 1509(a); 28 U.S.C.A. § 651.

²⁸See 17 U.S.C.A. § 1509(a).

²⁹See 17 U.S.C.A. § 1504(e)(1)(D).

³⁰See 17 U.S.C.A. § 1504(e)(2).

or statutory damages (or no damages at all).³¹ The Board may hold parties jointly and severally liable “if all such parties and relevant claims or counterclaims arise from the same activity or activities.”³²

As in court under the Copyright Act, but subject to the \$30,000 cap per proceeding, actual damages and profits may be recovered, pursuant to the provisions of 17 U.S.C.A. § 504(b),³³ with the award taking into consideration, in appropriate cases, whether the accused infringer has agreed to cease or mitigate the infringing activity.³⁴

Statutory damages alternatively may be sought, and may be awarded pursuant to 17 U.S.C.A. § 504(c),³⁵ but subject to four additional considerations and limitations. First, as noted above, recovery in any one proceeding is limited to \$30,000, excluding attorneys’ fees and costs.³⁶ Second, the amount of any statutory damage award must be determined without any consideration of willfulness.³⁷ Third, the Copyright Claims Board has discretion to consider, as an additional factor in awarding statutory damages, whether the alleged infringer has agreed to cease or mitigate the infringing activity pursuant to 17 U.S.C.A. § 1504(e)(2).³⁸ Fourth, statutory damages for infringement of any one work is capped at (a) \$15,000 for a work that has been timely registered and (b) \$7,500 for a work that has not been timely registered (further capped to a total of \$15,000 in any one proceeding).³⁹ Since statutory damages are not recoverable at all in a court proceeding when a work was untimely registered, copyright owners who failed to timely register their works, cannot es-

³¹See 17 U.S.C.A. § 1504(e)(1)(B).

³²See 17 U.S.C.A. § 1504(f).

³³See generally *infra* §§ 4.14[1], 4.14[3] (analyzing actual damages and profits under the Copyright Act).

³⁴See 17 U.S.C.A. § 1504(e)(1)(A)(i).

³⁵See generally *infra* §§ 4.14[1], 4.14[2] (analyzing statutory damages under the Copyright Act).

³⁶See 17 U.S.C.A. § 1504(e)(1)(D).

³⁷See 17 U.S.C.A. § 1504(e)(1)(A)(ii)(III). In court proceedings, where willfulness is shown, a copyright owner may recover up to \$150,000 per work infringed for works timely registered, and may impact the size of an award even when a judge or jury awards a lower amount. See generally *infra* § 4.14[2][A] (analyzing willful, nonwillful and innocent infringement).

³⁸See 17 U.S.C.A. § 1504(e)(1)(A)(ii)(IV).

³⁹See 17 U.S.C.A. § 1504(e)(1)(A)(ii).

establish actual damages, and are willing to forego injunctive relief, may have an incentive to bring potentially meritorious claims before the Copyright Claims Board, rather than to file suit in court, although the \$15,000 cap per proceeding means that the incentive will mainly be attractive to individuals and smaller entities (and also may be used by copyright trolls willing to file multiple proceedings). To deter troll suits, the Register of Copyrights may establish regulations limiting the number of proceedings that the same claimant may bring in a given year.⁴⁰

Copyright damages are analyzed extensively below in section 4.14.

Attorneys' fees and costs generally will not be awarded, except in cases of bad faith, where the Board may award up to \$5,000 in attorneys' fees and costs (or \$2,500 in costs for those representing themselves without counsel) and, in extraordinary circumstances, such as where a party has demonstrated a pattern or practice of bad faith conduct, a higher amount above these limits.⁴¹

Proceedings before the Copyright Claims Board will be adjudicated by three Copyright Claims Officers, who will be attorneys who have each been in practice for at least seven years.⁴² Two of the Copyright Claims Officers must have substantial experience in the evaluation, litigation, or adjudication of copyright infringement claims, and, between the two Officers, have represented or presided over a diversity of copyright interests, including those of both owners and users of copyrighted works.⁴³ The third Claims Officer must have substantial familiarity with copyright law and experience in alternative dispute resolution.⁴⁴ Ultimately, it remains to be seen who the three Copyright Claims Officers will be, and what their specific prior experience will have been, as well as the identity of Copyright Claims Attorneys, who will assist in the administration of the Copyright Claims

⁴⁰See 17 U.S.C.A. § 1504(g); *see also id.* § 1510(a)(1).

⁴¹See 17 U.S.C.A. §§ 1504(e)(3), 1506(y)(2).

⁴²17 U.S.C.A. § 1502(b)(3). As discussed later in this section, claims for \$5,000 or less may be addressed by a single adjudicator pursuant to regulations that will be promulgated by the Copyright Office before the Copyright Claims Board becomes operations (between December 22, 2021 and June 22, 2022).

⁴³See 17 U.S.C.A. § 1502(b)(3).

⁴⁴See 17 U.S.C.A. § 1502(b)(3)(A)(ii)(III).

Board and who must have at least 3 years of substantial experience in copyright law but not necessarily diversity of experience representing both copyright owners and users.⁴⁵

As in federal court, proceedings before the Copyright Claims Board will be subject to the same three year statute of limitations as other copyright claims⁴⁶ (but a proceeding commenced before the Board will toll the time permitted under 17 U.S.C.A. § 507(b) for filing suit in federal court for copyright infringement (based on the same claim) during the time when the Board proceeding is pending⁴⁷). Claimants likewise generally must have a registered copyright to pursue a claim for infringement (which, as in a court proceeding, will be entitled to the presumptions provided by 17 U.S.C.A. § 410(c) if registered within 5 years of first publication).⁴⁸ Unlike in federal court, however, a claimant may also proceed, at least initially, based solely on a paid application provided that the Copyright Claims Board may not render a determination until a registration certificate has been obtained and copies have been given to the other parties to the proceeding (and, if a proceeding may not proceed further because a registration certificate has yet been obtained, the proceeding will be held in abeyance subject to provisions allowing for dismissal without prejudice if the proceeding has been held in abeyance for more than one year).⁴⁹ The Copyright Office's refusal to register a work will result in the dismissal without prejudice of a proceeding initiated based on a mere application.⁵⁰

The CASE Act requires the Register of Copyrights to establish regulations allowing the Copyright Office to determine registration applications on an expedited basis when an unregistered work is at issue before the Copyright Claims

⁴⁵See 17 U.S.C.A. § 1502(b)(3)(B).

⁴⁶See 17 U.S.C.A. § 1504(b); *see generally supra* § 4.08[7] (analyzing the statute of limitations in copyright litigation).

⁴⁷See 17 U.S.C.A. § 1504(b)(2). Once a final determination has been made, however, the same claims and counterclaims asserted and finally determined by the Board may not be relitigated between the same parties. *See id.*; *id.* § 1507(a).

⁴⁸See 17 U.S.C.A. §§ 1505(a), 1505(b)(3), 1505(c).

⁴⁹See 17 U.S.C.A. §§ 1505(a), 1505(b).

⁵⁰See 17 U.S.C.A. § 1505(b)(3); *see generally infra* § 4.19 (analyzing the requirement for registration or rejection of a copyright registration certificate to proceed in court and the mechanism available in federal court for challenging the Copyright Office's refusal to register a work).

Board.⁵¹ The regulations will also allow for libraries and archives to preemptively opt out of board proceedings and provide for single Officer determinations of claims of \$5,000 or less (exclusive of attorneys' fees and costs),⁵² among other things.

Determinations by the Board may be challenged by a request for reconsideration and, if unsuccessful, review by the Register of Copyrights "limited to consideration of whether the Copyright Claims Board abused its discretion in denying reconsideration of the determination."⁵³ A final determination also may be challenged in federal court, within 90 days, on narrow grounds, (a) if the determination was issued as a result of fraud, corruption, misrepresentation, or other misconduct, (b) if the Copyright Claims Board exceeded its authority or failed to render a final determination concerning the subject matter at issue, or (c) in the case of a default determination or determination based on a failure to prosecute, if it is established that the default or failure was due to excusable neglect.⁵⁴

Final determinations will have preclusive effect in any court or tribunal, but only between the same parties, and only with respect to claims and counterclaims asserted and finally determined by the Board.⁵⁵ Thus, the preclusive effect of a determination is narrower than in federal court and does not reach claims that could have, but were not in fact, asserted in a Copyright Claims Board proceeding. The CASE Act also provides that final determinations will not have a preclusive effect on determinations of ownership or have any effect on a class action proceeding in federal court.⁵⁶

Where a party fails to pay damage or otherwise comply with a final determination, the aggrieved party may apply to a federal court to confirm the award and reduce it to a judgment.⁵⁷ Such an application must be made within one year of the latest of the date the final determination issued, the date of any reconsideration by the Copyright Claims

⁵¹See 17 U.S.C.A. § 1506(aa).

⁵²See 17 U.S.C.A. § 1506(z).

⁵³See 17 U.S.C.A. §§ 1506(w), 1506(x).

⁵⁴See 17 U.S.C.A. § 1508(c).

⁵⁵See 17 U.S.C.A. § 1507(a).

⁵⁶See 17 U.S.C.A. § 1507.

⁵⁷See 17 U.S.C.A. § 1508.

Board or review by the Register of Copyrights is resolved, or the date an amended final determination issued.⁵⁸

Board determinations will be published and made available on a publicly accessible website,⁵⁹ and thus may be cited in subsequent Board proceedings as influential, although the CASE Act makes clear they “may not be cited or relied upon as legal precedent . . .” before the Board or in any court or tribunal.⁶⁰

The provisions governing CASE Act proceedings set forth in 17 U.S.C.A. § 1504—including the voluntary nature of the proceedings, right to opt-out, waiver of the right to opt-out by failing to respond within 60 days of being served with a copy of the complaint, tolling, the claims and counterclaims that may be asserted, and those that may not be, remedies and damage limitations, and joint and several liability—may not be waived except pursuant to the terms of the CASE Act.⁶¹ Thus, any effort to preemptively opt out of Copyright Claims Board proceedings or to require contracting parties to opt-out of CASE Act remedies or to agree by contract to expand or contract the scope of claims and defenses that could be considered or remedies awarded, will be void.

4.09 Liability Under the Computer Software Rental Amendments Act

The Computer Software Rental Amendments Act prohibits any person “for the purposes of direct or indirect commercial advantage [to] dispose of, or authorize the disposal of” a computer program acquired on or after Dec. 1, 1990, “by rental, lease or lending, or by any other act or practice in the nature of rental, lease or lending.”¹

In *Central Point Software, Inc. v. Global Software & Accessories, Inc.*,² the first reported case decided under the Act, Judge Leonard Wexler of the Eastern District of New York held that a computer software company’s “sale” of software

⁵⁸See 17 U.S.C.A. § 1508(a).

⁵⁹See 17 U.S.C.A. § 1506(t)(3).

⁶⁰See 17 U.S.C.A. § 1507(a).

⁶¹See 17 U.S.C.A. § 1504(a).

[Section 4.09]

¹17 U.S.C.A. § 109(b)(1)(A).

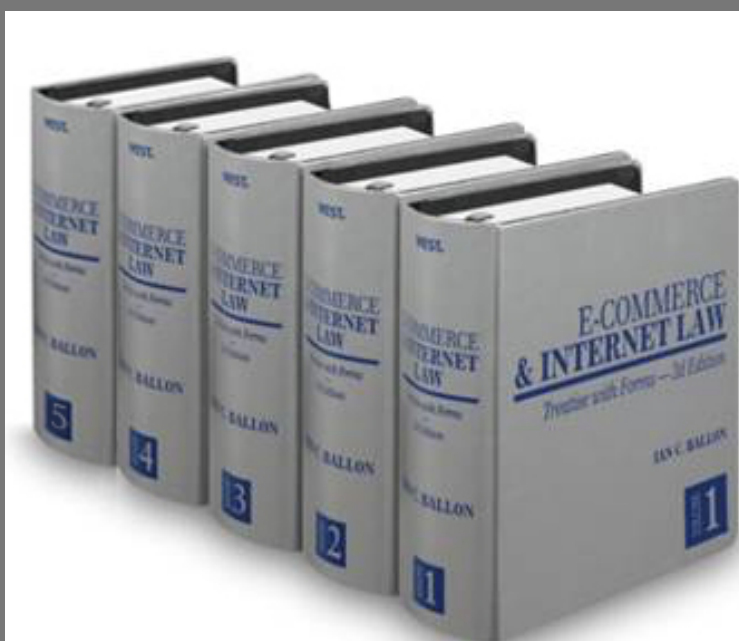
²*Central Point Software, Inc. v. Global Software & Accessories, Inc.*, 880 F. Supp. 957 (E.D.N.Y. 1995).

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2022

Ian C. Ballon

2022
UPDATES -
INCLUDING
NEW AND
IMPORTANT
FEATURES

THE PREEMINENT
INTERNET AND
MOBILE LAW
TREATISE FROM A
LEADING INTERNET
LITIGATOR — A
5 VOLUME-SET &
ON WESTLAW!



To order call **1-888-728-7677**
or visit **lanBallon.net**

Key Features of E-Commerce & Internet Law

- ◆ AI, ML, screen scraping and data portability
- ◆ Antitrust in the era of techlash
- ◆ The CPRA, Virginia, Colorado and Nevada privacy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- ◆ Software copyrightability and fair use after *Google v. Oracle*
- ◆ Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- ◆ TCPA law and litigation after *Facebook v. Duguid* - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- ◆ The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- ◆ Platform moderation and liability, safe harbors, and defenses (including the CDA and DMCA)
- ◆ Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- ◆ The law of SEO and SEM – and its impact on e-commerce vendors
- ◆ Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- ◆ IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi*, patentable subject matter, negative trade secrets, rights of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- ◆ Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- ◆ Sponsored links, embedded links, #hashtags, and internet, mobile and social media advertising
- ◆ Enforcing judgments against foreign domain name registrants
- ◆ Valuing domain name registrations from sales data
- ◆ Applying the First Sale Doctrine to virtual goods
- ◆ Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- ◆ Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- ◆ Click fraud
- ◆ Copyright and Lanham Act fair use
- ◆ Practical tips, checklists and forms that go beyond the typical legal treatise
- ◆ Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ AI/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- ◆ Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- ◆ Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- ◆ Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- ◆ Addresses both law and best practices
- ◆ Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- ◆ Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

Volume 1

Part I. Sources of Internet Law and Practice: A Framework for Developing New Law

- Chapter* 1. Context for Developing the Law of the Internet
2. A Framework for Developing New Law
3. [Reserved]

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Data Scraping, Database Protection, and the Use of Bots and Artificial Intelligence to Gather Content and Information
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names

Volume 2

- Chapter* 8. Internet Patents
9. Unique Intellectual Property Issues in Search Engine Marketing, Optimization and Related Indexing, Information Location Tools and Internet and Social Media Advertising Practices
10. Misappropriation of Trade Secrets in Cyberspace
11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property
12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace
13. Idea Submission, Protection and Misappropriation
- Part III. Licenses and Contracts**
14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: The Federal eSign Statute, Uniform Electronic Transactions Act, UCITA, and the EU Distance Selling Directive
16. Internet Licenses: Rights Subject to License and Limitations Imposed on Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content Licensing Pre-Existing Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements

Volume 3

- Chapter* 24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements
- Part IV. Privacy, Security and Internet Advertising**
25. Introduction to Consumer Protection in Cyberspace
26. Data Privacy
27. Cybersecurity: Information, Network and Data Security
28. Advertising in Cyberspace

Volume 4

- Chapter* 29. Email and Text Marketing, Spam and the Law of Unsolicited Commercial Email and Text Messaging
30. Online Gambling

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. State and Local Sales and Use Taxes on Internet and Mobile Transactions
34. Antitrust Restrictions on Technology Companies and Electronic Commerce
35. Dormant Commerce Clause and Other Federal Law Restrictions on State and Local Regulation of the Internet
36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

Part VI. Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption

37. Defamation, Torts and the Good Samaritan Exemption (47 U.S.C.A. § 230)
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression in Cyberspace

Part VII. Obscenity, Pornography, Adult Entertainment and the Protection of Children

40. Child Pornography and Obscenity
41. Laws Regulating Non-Obscene Adult Content Directed at Children
42. U.S. Jurisdiction, Venue and Procedure in Obscenity and Other Internet Crime Cases

Part VIII. Theft of Digital Information and Related Internet Crimes

43. Detecting and Retrieving Stolen Corporate Data
44. Criminal and Related Civil Remedies for Software and Digital Information Theft
45. Crimes Directed at Computer Networks and Users: Viruses and Malicious Code, Service Disabling Attacks and Threats Transmitted by Email

Volume 5

- Chapter* 46. Identity Theft
47. Civil Remedies for Unlawful Seizures
- Part IX. Liability of Internet Sites and Service (Including Social Networks and Blogs)**
48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Content Moderation and Platform Liability: Service Provider and Website, Mobile App, Network and Cloud Provider Exposure for User Generated Content and Misconduct
50. Cloud, Mobile and Internet Service Provider Compliance with Subpoenas and Court Orders
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites
- Part X. Civil Jurisdiction and Litigation**
52. General Overview of Cyberspace Jurisdiction
53. Personal Jurisdiction in Cyberspace
54. Venue and the Doctrine of Forum Non Conveniens
55. Choice of Law in Cyberspace
56. Internet ADR
57. Internet Litigation Strategy and Practice
58. Electronic Business and Social Network Communications in the Workplace, in Litigation and in Corporate and Employer Policies
59. Use of Email in Attorney-Client Communications

“Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet.”

Jay Monahan

General Counsel, ResearchGate

ABOUT THE AUTHOR

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator in the firm's Silicon Valley Los Angeles and Washington, DC offices. He defends data privacy, cybersecurity breach, AdTech, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database, AI and other intellectual property cases, including disputes involving safe harbors and exemptions, platform liability and fair use.



Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top Intellectual Property litigators in every year the list has been published (2009-2021), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was selected as the Lawyer of the Year for information technology law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. He also serves as Executive Director of Stanford University Law School's Center for the Digital Economy.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

Mr. Ballon is also the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.IanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@IanBallon).

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2022

- > **Antitrust in the era of techlash** (chapter 34)
- > **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- > **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- > **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurity breach, data privacy, AdTech and TCPA class action suits.**
- > **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- > **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- > **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- > **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States*, 141 S. Ct. 1648 (2021)** (ch5)
- > **FOSTA-SESTA and ways to maximize CDA protection** (ch 37)
- > **IP aspects of the use of #hashtags in social media** (ch 6)
- > **The CLOUD Act** (chapter 50)
- > **Virginia, Colorado and Nevada privacy laws** (ch 26)
- > **Applying the single publication rule to websites, links and uses on social media** (chapter 37)
- > **Digital economy litigation strategies**
- > **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- > **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- > **Website and mobile accessibility under the ADA and state laws** (chapter 48)
- > **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- > **Updated Defend Trade Secrets Act and UTSA case law** (chapter 10)
- > **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- > **AdTech law** (chapter 28, Darren Abernethy)
- > **The risks of being bound by the CASE Act's ostensibly voluntary jurisdiction over small copyright cases**
- > **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- > **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- > **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- > **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 26)
- > **Patent law** (updated by Josh Raskin) (chapter 8)
- > **Idea protection & misappropriation** (ch 13)
- > **Revisiting links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- > **eSIGN case law** (chapter 15)

**SAVE 20% NOW!! To order call 1-888-728-7677
or visit IanBallon.net
enter promo code **WPD20** at checkout**

List Price: \$3,337.00
Discounted Price: \$2,669.60

COPYRIGHT FAIR USE

Excerpted from the forthcoming 2022 updates to Chapter 4 (Copyright Protection in Cyberspace)

E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition

A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

(These excerpts are unrevised page proofs for the current update and may contain errors. Please email the author at ballon@gtlaw.com for a complimentary copy of the final published version.)

IP LAW YEAR IN REVIEW

4TH ANNUAL HBCU TECH LAW SUMMIT AND 19TH ANNUAL IP AND SOCIAL JUSTICE CLE SEMINAR

INSTITUTE FOR INTELLECTUAL PROPERTY AND SOCIAL JUSTICE
HOWARD UNIVERSITY SCHOOL OF LAW
MARCH 3-4, 2022

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles: 1840 Century Park East, Ste. 1900 Los Angeles, CA 90067 Direct Dial: (310) 586-6575 Direct Fax: (310) 586-0575	Silicon Valley: 1900 University Avenue, 5th Fl. East Palo Alto, CA 914303 Direct Dial: (650) 289-7881 Direct Fax: (650) 462-7881	Washington, D.C.: 2101 L Street, N.W., Ste. 1000 Washington, D.C. 20037 Direct Dial: (202) 331-3138 Fax: (202) 331-3101
--	---	--

Ballon@gtlaw.com
<www.ianballon.net>
LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
(Thomson West 2022 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (888) 728-7677
www.ianballon.net



Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal
Circuits

U.S. Supreme Court

JD, LLM, CIPP/US

Ballon@gtlaw.com

LinkedIn, Twitter, Facebook: IanBallon

Los Angeles

1840 Century Park East
Suite 1900

Los Angeles, CA 90067

T 310.586.6575

F 310.586.0575

Silicon Valley

1900 University Avenue
5th Floor

East Palo Alto, CA 94303

T 650.289.7881

F 650.462.7881

Washington, D.C.

2101 L Street, N.W.

Suite 1000

Washington, DC 20037

T 202.331.3138

F 202.331.3101

Ian C. Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and TCPA class action suits.

Ian is also the author of the leading treatise on internet and mobile law, [E-Commerce and Internet Law: Treatise with Forms 2d edition](#), the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of intellectual property law issues. In addition, he serves as [Executive Director of Stanford University Law School's Center for the Digital Economy](#). He also chairs [PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation](#) conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian was named the Lawyer of the Year for Information Technology Law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of Best Lawyers in America (including lawyer of the year for 2022). In 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder's* 2017 Litigation Departments of the Year Awards. He was also recognized as the 2012 [New Media Lawyer of the Year](#) by the Century City Bar Association. In 2010, he was the recipient of the California State Bar Intellectual Property Law section's [Vanguard Award for significant contributions to the development of intellectual property law](#). Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2021), and has been listed as a Northern California Super Lawyer every year from 2004 through 2021 and as one of the top 100 lawyers in California. He is also listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology.

Ian holds JD and LLM degrees and the [CIPP/US certification from the International Association of Privacy Professionals \(IAPP\)](#).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 1



THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

under a deferred billing plan amounted to the rental of software prohibited by the Act. Under the defendant's deferred billing plan, customers paid a small "nonrefundable deposit" for the software and were not billed for the balance if they returned it within five days. Judge Wexler found that the transactions were tantamount to rentals since (1) defendant's brochures advertised the "nonrefundable deposit," not the purchase price of software, (2) nearly 100% of the software was returned, (3) the deposits were comparable to rental fees, (4) the short term of the agreements was comparable to a rental term, obviously allowing the defendant to use the same copy of software in other transactions, and (5) the customer was not given the software manufacturer's registration card unless the full purchase price was paid.

Judge Wexler also held the defendant liable for renting customers post-Dec. 1, 1990, upgrades of programs it acquired before that date. Judge Wexler held that the company's right to lawfully rent software acquired before Dec. 1, 1990, did not extend to later upgrades of the same programs.

The potential opportunities for "sham" software transactions over the Internet are even greater than through traditional channels of retail trade. This is particularly true because of the number of people who, for ideological reasons, believe that software should be freely available.

4.10 Fair Use Defense and the Concept of Time in Cyberspace

4.10[1] The Fair Use Defense—In General

Fair use is a complete defense to copyright infringement¹ (although it is not a defense to a claim brought under the anticircumvention provisions of the Digital Millennium

[Section 4.10[1]]

¹17 U.S.C.A. § 107. As an affirmative defense, its proponent bears the burden of proving that it applies in a given case.

Fair use is a mixed question of law and fact. The determination ultimately is a legal one, but to render the issue of law there may be "subsidiary factual questions"—such as whether there was harm to the actual or potential markets for the copyrighted work or how much of the copyrighted work—that must be addressed, depending on the facts of a given case. See *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1199–1200 (2021).

Copyright Act).² Fair use encompasses First Amendment protections in copyright cases and, coupled with “the idea/expression dichotomy . . . , present the most important limitation on copyright law.”³ “In a sense, the grant to an author of copyright in a work is predicated upon a reciprocal grant to the public by the work’s author of an implied license for fair use of the work.”⁴ Where a secondary use is fair, the new work may even be entitled to copyright protection in its own right as a derivative work.⁵

What constitutes fair use in practice is, in many instances, difficult to evaluate. Fair use has been characterized as an “equitable rule of reason”⁶ and therefore must be proven on a case-by-case basis in litigation,⁷ rather than easily determined by a bright line test. Fair use is “an open-ended and context-sensitive inquiry”⁸ It is an exception that

²17 U.S.C.A. §§ 1201 *et seq.*; see generally *infra* § 4.21[2].

³*Cambridge University Press v. Patton*, 769 F.3d 1232, 1256 n.18 (11th Cir. 2014); see also *Eldred v. Ashcroft*, 537 U.S. 186, 219-20 (2003) (explaining that “copyright law contains built-in First Amendment accommodations.”); *Golan v. Holder*, 565 U.S. 302, 327-29 (2012) (holding that there was no need for heightened First Amendment review in copyright cases because of “the idea/expression distinction and the fair use defense.”); *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 556 (1985) (rejecting a First Amendment claim “[i]n view of the First Amendment protections already embodied in the Copyright Act’s distinction between copyrightable expression and uncopyrightable facts and ideas, and the latitude for scholarship and comment traditionally afforded by fair use”); *New Era Publications Int’l, ApS v. Henry Holt & Co.*, 873 F.2d 576, 584 (2d Cir. 1989) (summarizing earlier case law holding that the fair use defense encapsulated First Amendment protections), *cert. denied*, 493 U.S. 1094 (1990); *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 923 F. Supp. 1231, 1258 (N.D. Cal. 1995) (explaining, in an early internet copyright case, that the Supreme Court has recognized that the Copyright Act itself embodies a balance between the rights of copyright holders, which are guaranteed by Article I, section 8 of the Constitution, and the protections of the First Amendment).

The idea/expression dichotomy is separately analyzed in section 4.02.

⁴*Cambridge University Press v. Patton*, 769 F.3d 1232, 1257 (11th Cir. 2014).

⁵See *Keeling v. Hars*, 809 F.3d 43, 49-50 (2d Cir. 2015). Derivative works are analyzed in section 4.05[3].

⁶*Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 448 (1984).

⁷See *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 577 (1994).

⁸*Blanch v. Koons*, 467 F.3d 244, 251 (2d Cir. 2006).

“permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster.”⁹ As a consequence, “fair use is a context-sensitive inquiry that does not lend itself to simple bright-line rules.”¹⁰

The fair use defense generally applies where a work is used “for purposes *such as* criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship or research”¹¹

In evaluating whether the fair use defense is available, courts may consider other factors (as discussed later in this section), but *must* consider¹² four statutory factors:

- the purpose and character of the use, including whether it is of a commercial nature or is for nonprofit educational purposes;¹³

⁹*Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1196 (2021), quoting *Stewart v. Abend*, 495 U.S. 207, 236 (1990) (internal quotation marks omitted).

¹⁰*Andy Warhol Foundation for Visual Arts, Inc. v. Goldsmith*, 11 F.4th 26, 38 (2d Cir. 2021).

¹¹17 U.S.C.A. § 107 (emphasis added); see also *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 561 (1985) (holding that the examples set forth in the preamble to section 107 give an idea of activities that might be regarded as fair use but are not intended to be an exhaustive list or to single out any particular use as presumptively fair).

¹²*Stewart v. Abend*, 495 U.S. 207, 237 (1990).

¹³In evaluating the purpose and character of the use, courts typically consider whether a defendant’s use is (a) commercial and (b) transformative. Of these two considerations, transformativeness is by far the more important one.

While “[t]here is no doubt that a finding that copying was not commercial in nature tips the scales in favor of fair use. . . . the inverse is not necessarily true, as many common fair uses are indisputably commercial. For instance, the text of § 107 includes examples like ‘news reporting,’ which is often done for commercial profit.” *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1204 (2021) (finding that the purpose and character of the work weighed in favor of fair use because—even though Google’s use was a commercial endeavor— it was “not dispositive of the first factor, particularly in light of the inherently transformative role that the reimplementation played in the new Android system.”); *NXIVM Corp. v. Ross Institute*, 364 F.3d 471, 477-78 (2d Cir. 2004) (“The Supreme Court in *Campbell* rejected the notion that the commercial nature of [a] use could by itself be a dispositive consideration” given that “nearly all of the illustrative uses listed in the preamble of § 107, including news reporting, comment, criticism, teaching, scholarship, and research . . . ‘are generally

conducted for profit.’”), quoting *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 584 (1994).

In evaluating whether a work is commercial, the issue “is not whether the sole motive of the use is monetary gain, but whether the user stands to profit from exploitation of the copyrighted material without paying the customary price.” *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 562 (1985). In *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001), for example, the Ninth Circuit found that Napster’s peer-to-peer “file sharing” service was “commercial” even though it charged no fees for use because, among other things, it allowed users to “get for free something they would ordinarily have to buy.” The Ninth Circuit emphasized that “[d]irect economic benefit is not required to demonstrate a commercial use.” In *Napster*, there was evidence that the service, backed by venture capitalists, had hoped, like many Internet start-ups, to generate traffic and brand identity, so that it would eventually earn money. Likewise, in *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000), the court found defendant’s My.MP3.com service commercial because even though subscribers were “not currently charged a fee, defendant seeks to attract a sufficiently large subscription base to draw advertising and otherwise make a profit.” *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349, 351 (S.D.N.Y. 2000).

The central focus of the inquiry into the purpose and character of a work is whether (and to what extent) “the new work merely supersedes the objects of the original creation . . . or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning or message; . . . in other words, whether and to what extent the work is transformative.” *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994), quoting Pierre N. Leval, *Toward A Fair Use Standard*, 103 Harv. L. Rev. 1105, 1111 (1990). To be transformative, “[c]ommentators have put the matter more broadly, asking whether the copier’s use ‘fulfill[s] the objective of copyright law to stimulate creativity for public illumination.’” *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1202-03 (2021), quoting Leval, 103 Harv. L. Rev. at 1111. Accordingly, even copying 100% of a work could be transformative if it “adds something new and important.” See 141 S. Ct. at 1203, citing *Campbell*, 510 U.S. at 579. “An ‘artistic painting’ might, for example, fall within the scope of fair use even though it precisely replicates a copyrighted ‘advertising logo to make a comment about consumerism.’” 141 S. Ct. at 1203, citing 4 Nimmer on Copyright § 13.05[A][1][b] (quoting Netanel, *Making Sense of Fair Use*, 15 Lewis & Clark L. Rev. 715, 746 (2011)).

The evaluation of whether a work is transformative “may be guided by the examples given in the preamble to section 107, looking to whether the work is for criticism, or comment, or news reporting, and the like” *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 578–79 (1994). Although “transformative use is not absolutely necessary for a finding of fair use, the goal of copyright, to promote science and the arts, is generally furthered by the creation of transformative works.” *Id.* at 579.

The character of a work weighs in favor of finding fair use if it “adds value to the original” or uses the original “as raw material, transformed in the creation of new information, new aesthetics, new

insights and understandings.” *Castle Rock Entertainment, Inc. v. Carol publishing Group, Inc.*, 150 F.3d 132, 141 (2d Cir. 1998) (finding “slight to nonexistent” transformative value to a trivia quiz), *quoting* Leval, 103 Harv. L. Rev. at 1111. *Cf. Michaels v. Internet Entertainment Group Inc.*, 48 U.S.P.Q.2d 1891, 1998 WL 882848 (C.D. Cal. Sept. 10, 1998) (finding the use of twenty-seven seconds from a forty-five-minute videotape of actress Pamela Anderson Lee and a former boyfriend engaging in sexual relations (displayed in blurry two to five-second segments) transformative when used in a report aired on the television show “Hard Copy” about the plaintiff’s dispute over the pending unauthorized release of the video over the Internet).

The more transformative the new work, the less important other factors (including the commercial character of a work) become. *See, e.g., A.V. v. iParadigms, LLC*, 562 F.3d 630, 639 (4th Cir. 2009) (holding that defendants’ use of high school term papers in a database to compare and evaluate plagiarism claims was highly transformative and that the commercial aspect of the use was not significant in light of its transformative nature). Thus, even a practice that has a negative effect on the market for a genuine product may be found to be a fair use if it serves a transformative purpose. *See Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596, 607 (9th Cir.) (“some economic loss . . . does not compel a finding of no fair use.”), *cert. denied*, 531 U.S. 871 (2000); *see also Sony Computer Entertainment America, Inc. v. Bleem, LLC*, 214 F.3d 1022, 1027, (9th Cir. 2000) (holding that copying “screen shots” from Sony computer games for use in advertisements constituted a fair use under narrow circumstances in part because “comparative advertising redounds greatly to the purchasing public’s benefit with very little corresponding loss to the integrity of . . . [the] copyrighted material.”). Likewise, even an exact or complete copy of a work may be found to be a fair use if it is transformative. *See, e.g., Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1163–65 (9th Cir. 2007) (holding entire images copied in search results to be a fair use where the copying in connection with operation of a visual search engine was “highly transformative”); “As noted in *Campbell*, a ‘transformative work’ is one that alters the original work ‘with new expression, meaning, or message.’ . . . ‘A use is considered transformative only where a defendant changes a plaintiff’s copyrighted work or uses the plaintiff’s copyrighted work in a different context such that the plaintiff’s work is transformed into a new creation.’ ”) (emphasis added, citation omitted); *Nunez v. Caribbean Int’l News Corp.*, 235 F.3d 18, 22–23 (1st Cir. 2000) (holding republication of photos taken for a modeling portfolio in a newspaper to be transformative because the photos served to inform, as well as entertain); *Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1118–22 (D. Nev. 2006) (holding Google’s practice of caching content to be a fair use because it was highly transformative and served a noncompetitive purpose by enabling users to access a site when the original page was inaccessible, allowing users to compare changes to a site over time, highlighting search terms to allow users to understand why a page was deemed responsive to a query, using various design features to underscore that the cached copy is not intended to replace the original and encouraging users to access the original, and ensuring that site owners could disable the cache functionality so that their sites would not be copied by Google).

A use “can be transformative in function or purpose without altering or actually adding to the original work.” *A.V. v. iParadigms, LLC*, 562 F.3d 630, 639 (4th Cir. 2009) (holding that making an exact digital copy of a student’s thesis for the purpose of determining whether it included plagiarism was a fair use); *Swatch Group Mgmt. Servs. v. Bloomberg LP*, 756 F.3d 73, 84 (2d Cir. 2014) (quoting *iParadigms* for this proposition in a case in which the court held that a new service’s dissemination of verbatim transcripts of plaintiff’s recorded conference calls with securities analysts was a fair use and served at least an arguably transformative purpose—namely, to publish factual information, which otherwise was restricted to narrow group of analysts, to the public); see also *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 97-98 (2d Cir. 2014) (citing *iParadigms* and Ninth Circuit opinions for the proposition that copying entire books without substantive alteration nonetheless was transformative because “the creation of a full-text searchable database is a quintessentially transformative use.”); *Bill Graham Archives v. Dorling Kindersley Ltd.*, 448 F.3d 605, 609-11 (2d Cir. 2006) (holding the exact reproduction of reduced size Grateful Dead concert posters to be a fair use in connection with publication of a biography of the band; “DK’s purpose in using the copyrighted images at issue in its biography of the Grateful Dead is plainly different from the original purpose for which they were created. Originally, each of BGA’s images fulfilled the dual purposes of artistic expression and promotion. The posters were apparently widely distributed to generate public interest in the Grateful Dead and to convey information to a large number people about the band’s forthcoming concerts. In contrast, DK used each of BGA’s images as historical artifacts to document and represent the actual occurrence of Grateful Dead concert events featured on Illustrated Trip’s timeline.”); *Hughes v. Benjamin*, 437 F. Supp. 3d 382, 390 (S.D.N.Y. 2020) (collecting cases for the proposition that “a new work may be transformative even where it consists entirely of portions of the original work, or indeed even where it is an ‘exact replication’ of the original work.”); *Philpot v. Media Research Center Inc.*, 279 F. Supp. 3d 708, 717 (E.D. Va. 2018) (citing *iParadigms* and *Perfect 10* in holding that defendant’s use of exact copies of plaintiff’s concert photographs of Kenny Chesney and Kid Rock, on defendant’s pro-life website, to identify celebrities who support conservative political candidates, was transformative and a fair use because the images were used “in a completely different context.”). But see *Barcroft Media, Ltd. v. Coed Media Group, LLC*, 297 F. Supp. 3d 339, 351-55 (S.D.N.Y. 2017) (holding that a competing celebrity news site’s use of plaintiff’s photographs on its website was not transformative and not a fair use).

As explained by the Fourth Circuit, “even a wholesale reproduction may be transformed when placed in a ‘new context to serve a different purpose,’ but the secondary use still must generate a societal benefit by imbuing the original with new function or meaning.” *Brammer v. Violent Hues Productions, LLC*, 922 F.3d 255, 263 (4th Cir. 2019), quoting *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1165 (9th Cir. 2007). Surveying prior cases from both the Fourth Circuit and other circuits, the court in *Brammer* observed that “courts have typically found contextual changes sufficiently transformative in two recurring situations: technological uses and documentary uses.” 922 F.3d at 263-64. The panel elaborated that:

In the first category, copyrighted works provide raw material for new technological functions. These functions are indifferent to the expressive aspects of the copied works. For example, we have held transformative the total reproduction of student essays for a plagiarism detection service because the database served an “entirely different function” that was unrelated to the expressive content of those essays. *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 639 (4th Cir. 2009); accord *Google Books*, 804 F.3d at 216–17 (holding that an online book archive was “highly transformative” because it served the purpose of allowing users to search books for terms of interest); *Perfect 10*, 508 F.3d at 1165 (holding that an online image search index was “highly transformative”). This only makes sense: a contrary ruling would have risked impairing the functionality of these new information-sorting technologies.

In the second category, copyrighted works serve documentary purposes and may be important to the accurate representations of historical events. These representations often have scholarly, biographical, or journalistic value, and are frequently accompanied by commentary on the copyrighted work itself. See, e.g., *Bill Graham Archives v. Dorling Kindersley Ltd.*, 448 F.3d 605, 609 (2d Cir. 2006) (concert posters transformed when reproduced in pictorial history of the Grateful Dead); *Núñez v. Caribbean Int’l News Corp.*, 235 F.3d 18, 23 (1st Cir. 2000) (modeling photograph transformed when published as part of newspaper coverage of a related controversy).

Brammer v. Violent Hues Productions, LLC, 922 F.3d 255, 264 (4th Cir. 2019); see also *id.* at 263 & n.3 (reversing the district court’s holding that use of a photo found online, in connection with information about housing in the area depicted in the photograph, for attendees of defendant’s film festival, was used in a transformational manner and was a fair use, where the district court placed undue weight on the subjective intent of the parties, given that “[t]he transformational inquiry is largely objective.”).

When a work is simply retransmitted in a different medium, it is less likely to be found to be transformative. See, e.g., *Disney Enterprises, Inc. v. VidAngel, Inc.*, 869 F.3d 848, 861 (9th Cir. 2017) (DVD to streaming not transformative); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1015 (9th Cir. 2001) (concluding that “downloading MP3 files does not transform the copyrighted work.”); *Infinity Broadcast Corp. v. Kirkwood*, 150 F.3d 104, 108 & n.2 (2d Cir. 1998) (holding radio rebroadcasts over telephone lines were not transformative, noting that “a change of format, though useful, is not technically a transformation.”); *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349, 351 (S.D.N.Y. 2000) (finding that the reproduction of music from CD-ROMs to MP3 files did not transform the works; “defendant adds no ‘new aesthetics, new insights and understandings’ to the original music recordings it copies, . . . but simply repackages those recordings to facilitate their transmission through another medium.”).

Likewise, deleting offensive words from a motion picture to make them more accessible to people who otherwise might not watch them was held not to be transformative because “removing objectionable content may permit a viewer to enjoy a film, . . . [but that] does not necessarily ‘add . . . something new’ or change the ‘expression, meaning, or message’ of the film . . . *Star Wars* is still *Star Wars*, even without Princess Leia’s bikini scene.” *Disney Enterprises, Inc. v. VidAngel, Inc.*, 869 F.3d 848, 861 (9th Cir. 2017) (quotations omitted); see also *Disney Enterprises, Inc. v.*

VidAngel, Inc., 371 F. Supp. 3d 708, 719-22 (C.D. Cal. 2019) (rejecting VidAngel's fair use defense and granting summary judgment for plaintiffs).

As explained by Judge Leval, transformativeness is different from transformation for purposes of evaluating derivative works. He wrote that "derivative works generally involve transformations in the nature of *changes of form . . .*," such as the translation of a novel into another language, the adaptation of a novel into a movie or play, or the recasting of a novel as an e-book or an audio book. *Authors Guild v. Google Inc.*, 804 F.3d 202, 215 (2d Cir. 2015), *cert. denied*, 136 S. Ct. 1658 (2016). By contrast, copying from an original for the purpose of criticism or commentary about the original, or provision of information about it, "tends most clearly to satisfy *Campbell's* notion of the 'transformative' purpose involved in the analysis of Factor One." *Id.*; *see also supra* § 4.05[3] (analyzing derivative works).

Where a work is based on an earlier work, the new work may be deemed a fair use, if it is sufficiently transformative, or alternatively found to be merely an infringing derivative work. *See, e.g., Louis Vuitton Malletier, S.A. v. My Other Bag, Inc.*, 674 F. App'x 16, 19 (2d Cir. 2016) (affirming summary judgment for the defendant on the issue of fair use where the defendant's use of plaintiff's Louis Vuitton copyrighted pattern on a cheap canvas bag with the slogan "My Other Bag" was deemed to be a transformative parody); *Salinger v. Colting*, 607 F.3d 68, 83 (2d Cir. 2010) (agreeing with the district court that the author of "60 Years Coming: Through the Rye" was not likely to prevail on its fair use defense in a suit alleging that the novel was merely an infringing derivative work of J.D. Salinger's "The Catcher in the Rye"). In *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007), the Ninth Circuit rejected the argument that providing access to infringing websites could never be deemed transformative and is inherently not a fair use. The court acknowledged that a party claiming fair use must act in a manner generally compatible with principles of good faith and fair dealing. It distinguished *Video Pipeline, Inc. v. Buena Vista Home Entertainment, Inc.*, 342 F.3d 191, 198-200 (3d Cir. 2003), *cert. denied*, 540 U.S. 1178 (2004), and *Atari Games Corp. v. Nintendo of America Inc.*, 975 F.2d 832 (Fed. Cir. 1992) as cases where the alleged infringers "intentionally misappropriated the copyright owners' works for the purpose of commercial exploitation," whereas in *Amazon.com*, Google was "operating a comprehensive search engine that only incidentally indexes infringing websites. This incidental impact does not amount to an abuse of the good faith and fair dealing underpinnings of the fair use doctrine Google's inclusion of thumbnail images derived from infringing websites in its Internetwide search engine activities does not preclude Google from raising a fair use defense." *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d at 1164 n.8. In *A.V. v. iParadigms, LLC*, 562 F.3d 630 (4th Cir. 2009), the Fourth Circuit rejected the argument that a defendant's use could not be transformative where the defendant added nothing additional to the work. In that case, the defendant operated a database designed to detect plagiarism in assignments submitted by high school students. Plaintiffs argued that their term papers were copied into the database without authorization by the defendant, who in turn argued that its copying was a fair use. Judge Traxler, writing for the

panel, explained that “[t]he use of a copyrighted work need not alter or augment the work to be transformative in nature. Rather, it can be transformative in function or purpose without altering or actually adding to the original work.” *A.V. v. iParadigms, LLC*, 562 F.3d 630, 639 (4th Cir. 2009), citing *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1165 (9th Cir. 2007). He explained that just like Google’s use of copyrighted images in thumbnails as part of a search index was highly transformative even though the images themselves were not altered (in that they served a different function than the original images served), iParadigms’ use of plaintiffs’ works had an entirely different function and purpose than the original—to prevent plagiarism and stop student works from being plagiarized. Pierre Leval’s terminology, while adopted by the Supreme Court, has been criticized as somewhat confusing by Seventh Circuit Judge Posner, who in an opinion joined by then-Chief Judge Flaum and Judge Rovner, sought to recast consideration of whether a work was “transformative” or “superseding” in economic terms. According to Judge Posner, “copying that is complementary to the copyrighted work (in the sense that nails are complements of hammers) is fair use, but copying that is a substitute for the copyrighted work (in the sense that nails are substitutes for pegs or screws), or for derivative works from the copyrighted work . . . is not fair use.” *Ty, Inc. v. Publications Int’l Ltd.*, 292 F.3d 512, 517 (7th Cir. 2002) (citation omitted).

Whether a secondary user’s good faith or bad faith is relevant to fair use analysis is not entirely clear. In considering the purpose and character of the use, the Supreme Court observed in 1985 that “[f]air use presupposes ‘good faith’ and ‘fair dealing.’” *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 562 (1985); see also *Brammer v. Violent Hues Productions, LLC*, 922 F.3d 255, 266 (4th Cir. 2019) (explaining that “[b]ecause good faith is . . . presumed, most appellate courts, when considering a user’s mental state, have just asked whether the ‘bad faith subfactor weighs in plaintiffs’ favor.’”) (citing prior cases and holding that failing to appreciate that a photograph found online was copyrighted amounted to negligence, not good faith). In *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021), however, the Supreme Court, in finding fair use, opined that it had “no occasion” in that case “to say whether good faith is as a general matter a helpful inquiry.” *Id.* at 1204. As for bad faith, the Court reinforced its skepticism, as expressed in *Campbell*, “about whether bad faith has any role in a fair use analysis.” *Id.*, citing *Campbell*, 510 U.S. at 585 n.18. Justice Breyer, writing for the 6-2 majority in *Google v. Oracle America*, explained that “this skepticism justifiable, as ‘[c]opyright is not a privilege reserved for the well-behaved.’” 141 S. Ct. at 1204, quoting ; Pierre N. Leval, *Toward a Fair Use Standard*, 103 Harv. L. Rev. 1105, 1126 (1990); see also *id.* at 1128 (writing that fair use determinations depend “on factors pertinent to the objectives of copyright law and not on the morality or motives of either the secondary user or the copyright-owning plaintiff.”). “If the use is otherwise fair, then no permission need be sought or granted.” *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 585 n.18 (1994); see also, e.g., *Blanch v. Koons*, 467 F.3d 244, 256 (2d Cir. 2006) (suggesting that good faith was de-emphasized by the Supreme Court in *Campbell* but noting, in any case, that failing to seek permission for copying, by itself, does not amount to bad faith); *National*

- the nature of the copyrighted work;¹⁴

Football Scouting, Inc. v. Rang, 912 F. Supp. 2d 985, 992 (W.D. Wash. 2012) (rejecting the argument that a defendant's failure to respond to cease and desist letters should weigh against a finding of fair use, in entering summary judgment for the defendant based on fair use; "National points to its repeated cease and desist letters. However, if Rang was entitled to protection under fair use, the letters add nothing to the analysis because Rang would have been entitled to ignore them.").

¹⁴The nature of the copyrighted work focuses on whether a work is more creative or factual, and whether it is published or unpublished.

The Supreme Court has noted that creative works are "‘closer to the core of intended copyright protection’ than informational or functional works ‘with the consequence that fair use is more difficult to establish when the former works are copied.’" *Dr. Seuss Enterprises, L.P. v. Penguin Books USA, Inc.*, 109 F.3d 1394, 1402 (9th Cir. 1997), quoting *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 586 (1994); see also *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1201-02 (2021) (holding that Google's reimplementing of Java SE APIs was a fair use and that the nature of the work weighed in favor of fair use because "the declaring code is, if copyrightable at all, further than are most computer programs (such as the implementing code) from the core of copyright."; "Like other computer programs, it is functional in nature. But unlike many other programs, its use is inherently bound together with uncopyrightable ideas (general task division and organization) and new creative expression (Android's implementing code). Unlike many other programs, its value in significant part derives from the value that those who do not hold copyrights, namely, computer programmers, invest of their own time and effort to learn the API's system. And unlike many other programs, its value lies in its efforts to encourage programmers to learn and to use that system so that they will use (and continue to use) Sun-related implementing programs that Google did not copy."); *Stewart v. Abend*, 495 U.S. 207, 237 (1990) ("In general, fair use is more likely to be found in factual works than in fictional works."); *Brammer v. Violent Hues Productions, LLC*, 922 F.3d 255, 266-67 (4th Cir. 2019) (explaining that fair use is more difficult to establish where a work is protected by "thicker rights").

In evaluating this factor, unpublished works are entitled to enhanced protection. Once a work has been published, even a creative work will no longer be eligible for enhanced protection. See *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1167 (9th Cir. 2007).

Second Circuit Judge Pierre Leval has argued that the "transformative purpose inquiry" that is conventionally analyzed in connection with the purpose and character of the use, is also relevant to an evaluation of the nature of the work because "[o]ne cannot assess whether the copying work has an objective that differs from the original without considering both works, and their respective objectives." *Authors Guild v. Google Inc.*, 804 F.3d 202, 220 (2d Cir. 2015), cert. denied, 136 S. Ct. 1658 (2016).

Needless to say, "courts have hardly ever found that the second factor in isolation played a large role in explaining a fair use decision." 804 F.3d at 222; see also *Dr. Seuss Enters., L.P. v. Penguin Books USA, Inc.*, 109 F.3d 1394, 1402 (9th Cir. 1997) (noting that this second factor "typi-

- the amount and substantiality of the portion used in relation to the copyrighted work as a whole;¹⁵ and

cally has not been terribly significant in the overall fair use balancing.”). *But see Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1201 (2021) (beginning the Court’s analysis finding that Google’s reapplication of Java SE APIs constituted a fair use with consideration of the nature of the copyrighted work “[f]or expository purposes . . .”).

¹⁵In evaluating the amount and substantiality of the portion used, courts should look at the amount copied relative to the entire work (both quantitatively and qualitatively)—not as an absolute amount, in isolation—and the purpose for the copying. *See Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1204-05 (2021) (finding this factor weighed in favor of fair use; “If one considers the declaring code in isolation, the quantitative amount of what Google copied was large. Google copied the declaring code for 37 packages of the Sun Java API, totaling approximately 11,500 lines of code . . . [or] virtually all the declaring code needed to call up hundreds of different tasks. On the other hand, if one considers the entire set of software material in the Sun Java API, the quantitative amount copied was small. The total set of Sun Java API computer code, including implementing code, amounted to 2.86 million lines, of which the copied 11,500 lines were only 0.4 percent.”).

The extent of permissible copying varies with the purpose and character of the use. *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 586–87 (1994). “The ‘substantiality’ factor will generally weigh in favor of fair use where . . . the amount of copying was tethered to a valid, and transformative, purpose.” *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1205 (2021). Indeed, as noted in connection with the earlier discussion of transformation, “a new work may be transformative even where it consists entirely of portions of the original work, or indeed even where it is an ‘exact replication’ of the original work.” *Hughes v. Benjamin*, 437 F. Supp. 3d 382, 390 (S.D.N.Y. 2020) (collecting cases).

Wholesale copying does not preclude a finding of fair use *per se*, but may weigh against it. *See Cariou v. Prince*, 714 F.3d 694, 710 (2d Cir. 2013); *A.V. v. iParadigms, LLC*, 562 F.3d 630, 642 (4th Cir. 2009); *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 820 (9th Cir. 2003) (citing earlier case law). “[A]s the amount of the copyrighted material that is used increases, the likelihood that the use will constitute a ‘fair use’ decreases.” *Bond v. Blum*, 317 F.3d 385, 396 (4th Cir. 2003). “The larger the amount, or the more important the part, of the original that is copied, the greater the likelihood that the secondary work might serve as an effectively competing substitute for the original, and might therefore diminish the original rights holder’s sales and profits.” *Authors Guild v. Google Inc.*, 804 F.3d 202, 221 (2d Cir. 2015), *cert. denied*, 136 S. Ct. 1658 (2016). By contrast, “[i]f the secondary user only copies as much as is necessary for his or her intended use, then this factor will not weigh against him or her.” *Arriba Software*, 336 F.3d at 820. However, unlike trademark fair use (*infra* § 6.14), “the law does not require that the secondary artist may take no more than is necessary.” *Cariou v. Prince*, 714 F.3d 694, 710 (2d Cir. 2013). In short, “[t]here are no absolute rules as to how much of a copyrighted work may be copied and still be considered a fair use.” *Maxtone-Graham*

v. Burtchaell, 803 F.2d 1253, 1263 (2d Cir. 1986), *cert. denied*, 481 U.S. 1059 (1987).

Courts typically look at both the size of an excerpt and its quality (or whether the “essence” of the work was copied). For example, in *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 564–65 (1985), the Court found that a comparatively short, 300 word excerpt in a book review of President Gerald Ford’s memoirs supplanted the potential market for or value of the copyrighted work because it included many of the more important details that otherwise were to appear in a licensed excerpt in a competing newsmagazine.

By contrast, the defendant’s inclusion of twenty seconds of footage, edited from a promotional trailer, in a forty-four-minute television biography program, was found to be a fair use in *Hofheinz v. A & E Television Networks*, 146 F. Supp. 2d 442 (S.D.N.Y. 2001). Similarly, in *Hofheinz v. AMC Productions, Inc.*, 147 F. Supp. 2d 127 (E.D.N.Y. 2001), a court found that the unauthorized inclusion of certain movie clips and photographs in a documentary film, in addition to excerpts which had been expressly licensed, was likely to be found a fair use, in part because the clips did not amount to a substantial portion of the films from which they were excerpted. The court observed that the material did not “ge[t] at the ‘heart’ of the copyrighted works.” In evaluating the size of an excerpt, courts may focus both in absolute and percentage terms. *See, e.g., Iowa State University Research Foundation, Inc. v. American Broadcasting Companies, Inc.*, 621 F.2d 57, 61–62 (2d Cir. 1980) (holding that a television program’s copying of 2.5 minutes was held actionable, and not a fair use, because it amounted to 8% of the total show).

Courts will also look at the nature of the copying. Thus, copying even an entire work may be deemed a fair use “where the use of the original work is limited in purpose and scope.” *A.V. v. iParadigms, LLC*, 544 F. Supp. 2d 473, 483 (E.D. Va. 2008) (holding that the amount and substantiality of the portion used either favored neither party or a finding of fair use where the defendant used entire copies of high school students’ papers for the limited purpose of storing them digitally and reviewing them electronically in connection with running a plagiarism detection service, where the use was also found to be highly transformative), *aff’d*, 562 F.3d 630, 642 (4th Cir. 2009). Similarly, in *Authors Guild v. Google Inc.*, 804 F.3d 202, 221 (2d Cir. 2015), *cert. denied*, 136 S. Ct. 1658 (2016), the appellate panel held that copying 100% of plaintiff’s books nevertheless amounted to a fair use where the copying was undertaken for a highly transformative purpose of data mining, the copying did not have an adverse impact on the market of the genuine product, and each copy was made “to enable search functions to reveal limited, important information about the books.” 804 F.3d at 222. Needless to say, there is no magic number or percentage below which the quantity and quality of the portion copied automatically will be deemed a fair use.

In addition to being potentially relevant to the fair use defense, the amount and substantiality of material copied without authorization could support a defense of *de minimis* copying under very limited circumstances. *See supra* § 4.08[1].

- the effect of the use upon the potential market for, or value of, the copyrighted work.¹⁶

Even a relatively small amount of copying, however, may

¹⁶17 U.S.C.A. § 107. In evaluating the effect on the potential market for or value of the copyrighted work, courts should consider “whether the secondary use usurps or substitutes for the market of the original work.” *Castle Rock Entertainment, Inc. v. Carol publishing Group, Inc.*, 150 F.3d 132, 145 (2d Cir. 1998); see also *A.V. v. iParadigms, LLC*, 562 F.3d 630, 643 (4th Cir. 2009) (courts must determine whether a use would “materially impair the marketability of the work and whether it would act as a market substitute” for them; citing earlier cases). The Second Circuit has made clear that this factor focuses not on “whether the secondary use suppresses or even destroys the market for the original work, or its potential derivatives, but whether the secondary use *usurps* the market for the original work.” *Cariou v. Prince*, 714 F.3d 694, 708 (2d Cir. 2013) (holding that the use of plaintiff’s photographs in high end paintings that were marketed to a different sort of collector from the copyright owner’s original photographs did not usurp the copyright owner’s market), quoting *Blanch v. Koons*, 467 F.3d 244, 258 (2d Cir. 2006). Stated differently, a “fair use must not excessively damage the market for the original by providing the public with a substitute for that original work.” *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 95 (2d Cir. 2014). In the Eleventh Circuit, “[t]he central question under the fourth factor is not whether Defendants’ use of Plaintiffs’ works caused Plaintiff to lose *some* potential revenue. Rather, it is whether Defendants’ use—taking into account the damage that might occur if ‘everybody did it’—would cause *substantial* economic harm such that allowing it would frustrate the purposes of copyright by materially impairing Defendants’ incentive to publish the work.” *Cambridge University Press v. Patton*, 769 F.3d 1232, 1276 (11th Cir. 2014) (emphasis in the original).

While there is no bright line test for determining how much of an impact on the market is too much—especially because fair use fundamentally involves a balancing of interests—in *Disney Enterprises, Inc. v. VidAngel, Inc.*, 869 F.3d 848, 861 (9th Cir. 2017), the court held that VidAngel’s “family friendly” service, which deleted certain dialogue deemed to be offensive from plaintiffs’ motion pictures, had an adverse impact on the potential market for or value the copyrighted work where slightly less than half of VidAngel’s customers (49%) said in a survey that they would watch unedited versions if VidAngel’s versions were unavailable.

While an unauthorized use usually will be considered less fair when it is readily available for license, in some cases courts have found this factor weighs against fair use even where the work is not commercially available if a potential future market is harmed by the use. See, e.g., *Balsley v. LFP, Inc.*, 691 F.3d 747, 761 (6th Cir. 2012) (finding that a publisher had failed to rebut a presumption of market harm where it published a photo in which plaintiffs had acquired the copyright to prevent its dissemination), cert. denied, 568 U.S. 1124 (2013); *Monge v. Maya Magazines, Inc.*, 688 F.3d 1164, 1181-82 (9th Cir. 2012) (finding a use not fair where the potential market for unpublished photos was harmed by the defendant’s

be found impermissible if it deprives a copyright owner of its

infringing publication). Ultimately, this factor focuses on the impact of a use on the potential market for or value of the copyrighted work..

In general, “the more transformative the secondary use, the less likelihood that the secondary use substitutes for the original” even though “the fair use, being transformative, might well harm, or even destroy, the market for the original.” *A.V. v. iParadigms, LLC*, 562 F.3d 630 (4th Cir. 2009), citing *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 591–93 (1994) (“[A] lethal parody, like a scathing theater review, kills demand for the original, [but] does not produce a harm cognizable under the Copyright Act.”); see also *Brownmark Films, LLC v. Comedy Partners*, 682 F.3d 687, 692–93 (7th Cir. 2012) (affirming dismissal of a suit where the defendant’s use was “clearly a parody” and did not supplant the market for the original product, meaning that it could not have had “an actionable effect on the potential market for or value of” the copyright holder’s video); *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596, 607 (9th Cir.) (“Whereas a work that merely supplants or supersedes another is likely to cause a substantially adverse impact on the potential market of the original, a transformative work is less likely to do so.”), cert. denied, 531 U.S. 871 (2000). As the Second Circuit explained, “[f]actor Four analysis is concerned with only one type of economic injury to the copyright holder: the harm that results because the secondary use serves as a substitute for the original work [A]ny economic ‘harm’ caused by transformative uses does not count because such uses, by definition, do not serve as substitutes for the original work.” *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 99 (2d Cir. 2014).

The Supreme Court has cautioned against a mechanical approach in evaluating the impact of a use on the market for the genuine product—writing that “a potential loss of revenue is not the whole story”—which requires consideration of both the amount and the source of the loss. See *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1206 (2021). A “‘lethal parody, like a scathing theatre review,’ may ‘kill[] demand for the original.’” *Id.*, quoting *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 591–92 (1994). “Yet this kind of harm, even if directly translated into foregone dollars, is not ‘cognizable under the Copyright Act.’” *Google v. Oracle*, 141 S. Ct. at 1206, quoting *Campbell*, 510 U.S. at 592. In evaluating the impact on the market, courts, besides looking at the actual or potential market loss to the copyright owner, should also “consider the public benefit resulting from a particular use notwithstanding the fact that the alleged infringer may gain commercially.” *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1523 (9th Cir. 1992). The Supreme Court has cautioned that public benefit considerations may not be relevant in all cases, but they were relevant to the Court’s finding of fair use in *Google v. Oracle*. Justice Breyer explained that the Court’s holding took into account the public benefits the copying would likely produce, suggesting that courts, in evaluating this fair use factor, consider, among other things, whether those benefits related to “copyright’s concern for the creative production of new expression” and whether they were “comparatively important or unimportant, when compared with dollar amounts likely lost (taking into account as well the nature of the source of the loss)” *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1206 (2021), citing

ability to exploit the work.¹⁷

MCA, Inc. v. Wilson, 677 F.2d 180, 183 (2d Cir. 1981) (calling for a balancing of public benefits and losses to copyright owner under this factor). In *Google v. Oracle*, the Supreme Court concluded that given programmers' investment in learning Java APIs, allowing enforcement of Oracle's copyright would risk harm to the public. *See* 141 S. Ct. at 1208.

In *Google v. Oracle*, the jury's finding of fair use was supported by evidence that Android was not a market substitute for Java, that Android did not harm the actual or potential market for Java SE, that regardless of Android's smartphone technology, Sun was poorly positioned to succeed in the mobile phone market, and that Sun foresaw a benefit from the broader use of the Java programming language in a new platform like like Android, which would further expand the network of Java-trained programmers. 141 S. Ct. at 1206-07. In affirming the jury verdict and reversing the Federal Circuit's ruling, the Supreme Court rejected the Federal Circuit's analysis that the market was adversely affected because Google had sought unsuccessfully to obtain a license to use Java before reimplementing 37 APIs, noting that "those licensing negotiations concerned much more than 37 packages of declaring code, covering topics like 'the implementation of [Java's] code' and 'branding and cooperation' between the firms." *Id.* at 1207. Justice Breyer, writing for majority, noted that in every fair use case the plaintiff suffers "a loss of a *potential* market if that potential is defined as the theoretical market for licensing the very use at bar" *Id.* (emphasis in original), *quoting* 4 Nimmer on Copyright § 13.05[A][4]. The Court also observed that Android's profitability had much to do with third party programmers' investment in Sun Java programs; "It has correspondingly less to do with Sun's investment in creating the Sun Java API. We have no reason to believe that the Copyright Act seeks to protect third parties' investment in learning how to operate a created work." *Id.* at 1208, *citing Campbell*, 510 U.S. at 591-92 (discussing the need to identify those harms that are "cognizable under the Copyright Act").

The Supreme Court also observed that consideration of the impact on the market may prove complex "where computer programs are at issue" *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1206 (2021).

While an alleged infringer bears the evidentiary burden on all four factors, where the copyright owner has evidence of whether and under what terms a work has been exploited, the burden of going forward with this evidence rests with the copyright owner. *Cambridge University Press v. Patton*, 769 F.3d 1232, 1279-80 & n.34 (11th Cir. 2014).

¹⁷*See American Geophysical Union v. Texaco Inc.*, 60 F.3d 913, 923 (2d Cir.), *cert. dismissed*, 516 U.S. 1005 (1995). Moreover, the absence of an existing market for the genuine work may not be determinative if a defendant's use adversely affects the copyright owner's ability to later exploit it. The statute refers to the potential market for or value of the protected work. Thus, in *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000), the court rejected MP3.com's fair use defense in part because a copyright owner is entitled to refuse to license a work or to do so only on terms acceptable to it. The court found that the plaintiffs' ability to market digital music in the future had been damaged by

These fair use factors should not be applied mechanically, with each given equal weight.¹⁸ Rather, they must be balanced against one another.

While no single factor necessarily will be determinative,¹⁹ the effect of a defendant's use on the potential market for or value of the copyrighted work generally had been viewed as

MP3.com's unauthorized practices. Likewise, in a subsequent case brought against MP3.com, the court reiterated, in response to the argument that the plaintiffs themselves had offered free downloads of their protected MP3 music files, that "even if plaintiffs' own uses were more exploitative (as . . . defendant claimed . . .), defendant's activities would still 'invade plaintiffs' statutory right to license their copyrighted sound recordings to others for reproduction' and would still infringe 'a copyright holder's exclusive rights . . . within broad limits, to curb the development of such a derivative market by refusing to license a copyrighted work or by doing so only on terms the copyright owner finds acceptable.'" *Teevee Toons, Inc. v. MP3.com, Inc.*, 134 F. Supp. 2d 546, 547 (S.D.N.Y. 2001), *quoting UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d at 352 (internal quotation marks omitted).

The fact that a particular unauthorized use may actually enhance demand for the genuine work likewise has not necessarily been found to be a mitigating factor if the copyright owner in fact does not approve of the use. The court in *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349 (S.D.N.Y. 2000), for example, rejected as relevant the argument that defendant's service enhanced sales of plaintiffs' works because subscribers were required to show that they already owned a genuine copy of a CD, or simultaneously purchase one, before being able to copy it from the My.MP3.com online database to their personal folders. Judge Rakoff wrote that "[a]ny allegedly positive impact of defendant's activities on plaintiffs' prior market [for the sale of CDs] in no way frees defendant to usurp a future market [online music sales] that directly derives from reproduction of the plaintiffs' copyrighted works." *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349, 352 (S.D.N.Y. 2000).

On the other hand, if a copyright owner cannot articulate any credible theory of loss, the fact that a use enhances demand for the genuine product would weigh in favor of a finding of fair use, at least for purposes of assessing the fourth fair use factor. Judge Posner, in describing fair use of a book in connection with a book review, wrote that it would be "perverse" to treat copying that "increase[d] demand for the copyrighted works" as infringing. *See Ty, Inc. v. Publications Int'l Ltd.*, 292 F.3d 512, 517 (7th Cir. 2002).

¹⁸*Cambridge University Press v. Patton*, 769 F.3d 1232, 1260 (11th Cir. 2014).

¹⁹Congress intended the four statutory criteria to serve as guidelines for "balancing the equities" rather than "definitive or determinative" tests, which "are to be . . . weighed together, in light of the objectives of copyright 'to promote the progress of science and the useful arts.'" H.R. Rep. No. 94-1476, 94th Cong. 2d Sess. 65 (1976), *reprinted in* 1976 U.S.C.-C.A.N. 5659, 5679.

the most important factor in the past²⁰ and may be especially significant where a use substitutes for the original work. Increasingly, however, the first of the four considerations, the purpose and character of the use (and specifically whether the use is transformative), is viewed as “[t]he heart of the fair use inquiry.”²¹ As the Second Circuit explained, “the Supreme Court has made clear that some of the statute’s four listed factors are more significant than others. The

²⁰See *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 566 (1985) (describing this factor as “the single most important”); *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 642 (4th Cir. 2009); *Princeton University Press v. Michigan Document Services, Inc.*, 99 F.3d 1381, 1385 (6th Cir. 1996), *cert. denied*, 520 U.S. 1156 (1997). *But see Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 577-78 (1994) (backing away from the notion that any single factor was more important than any other, holding that fair use determinations required a “case-by-case analysis” and explaining that no single fair use factor should be considered in isolation; “All are to be explored, and the results weighed together, in light of the purposes of copyright.”).

²¹*On Davis v. The Gap, Inc.*, 246 F.3d 152, 174 (2d Cir. 2001); *see also Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579, 594 (1994) (rejecting the lower court’s analysis that the use at issue was presumptively unfair because it was commercial and explaining that “the more transformative the new work, the less will be the significance of other factors, like commercialism, that may weigh against a finding of fair use.”); *American Geophysical Union v. Texaco Inc.*, 60 F.3d 913, 926 (2d Cir.) (suggesting that the U.S. Supreme Court has abandoned the view that the most important factor is the effect on the potential market), *cert. dismissed*, 516 U.S. 1005 (1995); *Hofheinz v. Discovery Communications, Inc.*, 60 U.S.P.Q.2d 1845, 2001 WL 1111970, at *3 n.6 (S.D.N.Y. Sept. 20, 2001) (describing the Second Circuit as following what at the time was a minority view in placing greater emphasis on this factor). Other circuits also have considered transformativeness to be either the more important factor or potentially determinative in some cases. *See, e.g., A.V. v. iParadigms, LLC*, 562 F.3d 630, 639 (4th Cir. 2009) (holding that making an exact digital copy of a student’s thesis for the purpose of determining whether it included plagiarism was a fair use); *Seltzer v. Green Day, Inc.*, 725 F.3d 1170, 1178-79 (9th Cir. 2013) (holding the defendant’s use to be transformative and therefore a fair use). *But see Kienitz v. Sconnie Nation LLC*, 766 F.3d 756, 758-59 (7th Cir. 2014) (expressing skepticism with the Second Circuit’s approach to transformativeness “because asking exclusively whether something is ‘transformative’ not only replaces the list in § 107 but also could override 17 U.S.C. § 106(2), which protects derivative works” and reiterating, in an opinion written by Judge Easterbrook, that it was “best to stick with the statutory list, of which the most important usually is the fourth (market effect).”), *cert. denied*, 575 U.S. 913 (2015). Ultimately, neither the first nor the fourth factor should be viewed in isolation, but most courts today consider transformativeness to often be the more important consideration.

Court observed in *Harper & Row* . . . that . . . the harm the secondary use can cause the market for, or the value of, the copyright for the original, ‘is undoubtedly the single most important element of fair use.’ . . . In *Campbell*, the Court stressed also the importance of . . . ‘the purpose and character of the secondary use.’”²²

The four factors expressly listed in 17 U.S.C.A. § 107 are not exclusive.²³ Section 107 codified the common law doctrine of fair use that existed prior to the enactment of the 1976 Copyright Act. The four factors “are a checklist of things to be considered rather than a formula for decision; and likewise the list of statutory purposes.”²⁴ They “provide only general guidance about the sorts of copying that courts and Congress most commonly had found to be fair uses.”²⁵ They “are to be explored, and the results weighed together, in light of the purpose of copyright [law].”²⁶ Congress “intended that courts continue the common law tradition of fair use adjudication” and section 107 “permits and requires courts to avoid rigid application of the copyright statute, when, on occasion, it would stifle the very creativity which that law is designed to foster.”²⁷ According to the Second Circuit, “[t]he ultimate test of fair use, therefore, is whether the copyright law’s goal of ‘promoting the progress of science and useful

²²*Authors Guild v. Google Inc.*, 804 F.3d 202, 213-14 (2d Cir. 2015) (quoting *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 566 (1985) and 17 U.S.C.A. § 107 and citing *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 591 (1994)), *cert. denied*, 136 S. Ct. 1658 (2016).

²³Even though section 107 uses the mandatory term *shall*, a close reading of the somewhat unusual sentence structure preceding the four criteria shows that Congress did not intend that the four factors be the only ones considered; merely that in every fair use determination, each of the four factors (among other things) must be considered. *See* 17 U.S.C.A. § 107 (“In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include . . .”).

²⁴*Ty, Inc. v. Publications Int’l Ltd.*, 292 F.3d 512, 522 (7th Cir. 2002); *see also Peter Letterese & Associates, Inc. v. World Institute of Scientology Enterprises, Int’l*, 533 F.3d 1287, 1308 (11th Cir. 2008) (reiterating that neither the examples found in the preamble to section 107 nor the four statutory factors are to be considered exclusive). In the words of Judge Posner, the statutory definition, “while though extensive, is not illuminating. (More can be less, even in law).” *Ty, Inc. v. Publications Int’l Ltd.*, 292 F.3d 512, 522 (7th Cir. 2002).

²⁵*Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 577–78 (1994).

²⁶*Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 577–78 (1994).

²⁷*Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 577 (1994) (internal quotation marks omitted).

arts,’ ‘would be better served by allowing the use than by preventing it.’”²⁸ As a practical matter, since courts *may* evaluate other factors consistent with the underlying objectives of the Copyright Act, but *must* consider each of the four statutory criteria, in many cases the four factors alone are determinative. Nevertheless, fair use may be found in cases where the four criteria alone might not otherwise justify the finding.

Examples of fair use, when unauthorized copying has been deemed lawful, include parody, in cases involving sampling copyrighted music in a rap song,²⁹ and use of a photograph,³⁰

²⁸*Castle Rock Entertainment, Inc. v. Carol publishing Group, Inc.*, 150 F.3d 132, 141 (2d Cir. 1998) (quoting an earlier case and U.S. Const., art. I, § 8, cl. 8). In this regard, “excessively broad protection would stifle, rather than advance, the [Copyright Act’s] objective.” *Blanch v. Koons*, 467 F.3d 244, 250 (2d Cir. 2006), quoting Pierre N. Leval, *Toward A Fair Use Standard*, 103 Harv. L. Rev. 1105, 1109 (1990).

²⁹*See Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994) (sampling of a copyrighted song for use in a new parody composition); *Smith v. Graham*, 799 F. App’x 36 (2d Cir. 2020) (affirming summary judgment for the defendants, holding that Drake’s use of the “Jimmy Smith Rap” in “Pound Cake” was transformative, did not usurp the original or cause a negative market effect, and was a fair use); *Chapman v. Maraj*, 2:18-cv-09088-VAP-SSx, 2020 WL 6260021 (C.D. Cal. Sept. 16, 2020) (holding that Nicki Minaj sampling a song without permission from Tracy Chapman, for use on an unreleased track, was a fair use, but finding a disputed issue of fact over whether Minaj had leaked the track and, if she had, could be held liable for infringement).

³⁰*See, e.g., Leibovitz v. Paramount Pictures Corp.*, 137 F.3d 109 (2d Cir. 1998) (holding that a famous Annie Leibovitz photograph of the actress Demi Moore, while pregnant, in a well known pose evocative of Botticelli’s *Birth of Venus*, which appeared on the cover of *Vanity Fair* in 1991, was used permissibly as a fair use parody when Paramount restaged the photoshoot and superimposed the face of a male actor on a female model’s body to advertise an upcoming movie); *Kienitz v. Sconnie Nation LLC*, 766 F.3d 756 (7th Cir. 2014) (holding that the defendant’s use of a photograph of the mayor of Madison, Wisconsin, in a parody poster and on t-shirts making fun of the mayor’s prior involvement as a student in the annual Mifflin Street Block Party, which as mayor he had sought to shut down, was a fair use), *cert. denied*, 575 U.S. 913 (2015); *Schwartzwald v. Oath Inc.*, No. 19-CV-9938 (RA), 2020 WL 5441291, at *4-6 (S.D.N.Y. Sept. 10, 2020) (dismissing plaintiff’s claim for copyright infringement of a photograph of actor John Hamm walking down the street apparently without wearing underwear, finding that the use of the photo by *Huffington Post*, in an article entitled *25 Things You Wish You Hadn’t Learned in 2013 and Must Forget in 2014*, where the portion of the photo that showed a bulge in Hamm’s pants was replaced with a graphic stating “Image Loading,” was a fair use; rejecting the argument that alternative photos

mask,³¹ and literary work³² (although satire, *per se*, is not automatically a fair use³³), taping television transmissions

could have been used because they “would not have accomplished Oath’s goals of mocking both Hamm and those who obsess over viral photographs of this sort” and holding that “Oath’s use of the Photograph was transformative because it used the Photograph in service of its dual goals of mocking both Hamm and those who fixate over such suggestive photos of him—a use distinct from that which Schwartzwald intended—and because Oath obscured the very portion of the Photograph that made it most valuable or unique in the first instance.”).

³¹See *Easter Unlimited, Inc. v. Rozier*, 18-CV-06637 (KAM), 2021 WL 4409729, at *10-17 (E.D.N.Y. Sept. 27, 2021) (granting summary judgment to the defendant on plaintiff’s claim of copyright infringement, holding that Boston Celtics’ player Terry Rozier’s use of plaintiff’s “Ghost Face Mask” in a cartoon parody of himself as “Scary Terry,” a nickname intended to humorously invoke the fear that Mr. Rozier’s “dangerous” ability to score supposedly instilled in his NBA opponents, was a fair use as a matter of law).

³²See *Suntrust Bank v. Houghton Mifflin Co.*, 268 F.3d 1257 (11th Cir. 2001) (finding the defendant likely to prevail on its fair use defense in connection with “The Wind Done Gone,” a spoof of “Gone With the Wind” written from the perspective of slaves).

³³A number of courts apply the “conjure up” test to determine the “purpose and character of the use,” under which “the parodist is permitted a fair use of a copyrighted work if it takes no more than necessary to ‘recall’ or ‘conjure up’ the object of his parody.” *Dr. Seuss Enterprises, L.P. v. Penguin Books USA, Inc.*, 109 F.3d 1394, 1400 (9th Cir. 1997); see also, e.g., *MCA, Inc. v. Wilson*, 677 F.2d 180, 184 (2d Cir. 1981). To constitute a fair use parody—as opposed to mere satire—a work generally must be targeted at the original work and not merely borrow its style “to get attention or to avoid the drudgery in working up something fresh” *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. at 580; see also *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 597 (1994) (Kennedy, J., concurring); *Rogers v. Koons*, 960 F.2d 301, 310 (2d Cir.) (“the copied work must be, at least in part, an object of the parody, otherwise there would be no need to conjure up the original work”), *cert. denied*, 506 U.S. 934 (1992).

Thus, for example, the satiric book “The Cat Not in the Hat! By Dr. Juice,” a poetic account of the O.J. Simpson murder trial in the style of Dr. Seuss’s “The Cat in the Hat” was held to not be a fair use in *Dr. Seuss Enterprises, L.P. v. Penguin Books USA, Inc.*, 109 F.3d 1394, 1400-03 (9th Cir. 1997) because the defendant’s book used the style of plaintiff’s work to mimic the O.J. Simpson trial, rather than “The Cat in the Hat.”

Similarly, in a later case involving Dr. Seuss’s book, *Oh The Places You’ll Go!*, the Ninth Circuit held that a comic book mashup between that Dr. Seuss book and the original *Star Trek* television series, was not a fair use (rejecting the district court’s analysis that the book, although not a parody, was highly transformative and a fair use). See *Dr. Seuss Enterprises, L.P. v. ComicMix LLC*, 983 F.3d 443, 450-61 (9th Cir. 2020), *cert. denied*, 141 S. Ct. 2803 (2021), *rev’g in relevant part*, 372 F. Supp. 3d 1101, 1114-25 (S.D. Cal. 2019) (granting summary judgment for ComicMix).

on a videocassette recorder for future viewing,³⁴ reimplementing (37 of 166 of Java SE) application programming interfaces (APIs) in a new mobile operating system (by using declaring code for the APIs in connection with an original, noninfringing implementing code, written for the Android operating system),³⁵ linking and copying visual images for

ComicMix's book—*Oh, the Places You'll Boldly Go!*—was written by Star Trek episodes author David Gerrold, and borrowed “liberally—graphically and otherwise—from [*Oh The Places You'll Go!*] and other works by Dr. Seuss, and . . . use[d] Captain Kirk and his spaceship Enterprise to tell readers that ‘life is an adventure but it will be tough.’ ” 983 F.3d at 448. In reversing the district court's finding of fair use, the Ninth Circuit panel wrote: “The creators thought their Star Trek primer would be ‘pretty well protected by parody,’ but acknowledged that ‘people in black robes’ may disagree. Indeed, we do.” *Id.* Judge M. Margaret McKeown wrote that “[a]lthough ComicMix's work need not boldly go where no one has gone before, its repackaging, copying, and lack of critique of Seuss, coupled with its commercial use of *Go!*, do not result in a transformative use.” *Id.* at 455. ComicMix had argued that the work was transformative based on “extensive new content,” but Judge McKeown wrote that “the addition of new expression to an existing work is not a get-out-of-jail-free card that renders the use of the original transformative. The new expression must be accompanied by the benchmarks of transformative use. . . . Instead of possessing a further purpose or different character, *Boldly* paralleled *Go!*'s purpose. In propounding the same message as *Go*, *Boldly* used expression from *Go!* to “keep to [*Go!*]'s sentiment.” Absent new purpose or character, merely recontextualizing the original expression by ‘plucking the most visually arresting excerpt[s]’ of the copyrighted work is not transformative.” *Id.* at 453-54. The appellate panel also found that ComicMix's mashup adversely impacted the market for the genuine product because Dr. Seuss Enterprises had licensed *Oh The Places You'll Go!* for other uses, including a collaboration with The Jim Henson Company and a digital game, among other things. *Id.* at 458-61; *see also infra* § 6.14[7] (analyzing the Lanham Act holding in the same case, in which the Ninth Circuit ruled that the defendant's use was protected by the First Amendment, and not actionable under *Rogers v. Grimaldi*).

³⁴*See Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

³⁵*See Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021) (holding that all four fair use factors favored fair use); *see also supra* § 4.07 (discussing the *Google v. Oracle* case in the context of copyright protection for software). An API is a user interface that allows programmers to call upon prewritten computing tasks for use in their own programs. Google had reimplemented Java SE APIs “taking only what was needed to allow users to put their accrued talents to work in a new and transformative program,” *Id.* at 1209. Google had written its own original code to perform the tasks, but had copied the declaring code of the APIs to make them easy for JAVA language programmers to use. As explained by the Court:

the purpose of indexing websites as part of a visual search

The API reflects Sun's division of possible tasks that a computer might perform into a set of actual tasks that certain kinds of computers actually will perform. Sun decided, for example, that its API would call up a task that compares one integer with another to see which is the larger. Sun's API (to our knowledge) will not call up the task of determining which great Arabic scholar decided to use Arabic numerals (rather than Roman numerals) to perform that "larger integer" task. No one claims that the decisions about what counts as a task are themselves copyrightable—although one might argue about decisions as to how to label and organize such tasks (e.g., the decision to name a certain task "max" or to place it in a class called "Math." Cf. *Baker v. Selden*, 101 U.S. 99 (1880)).

114 S. Ct. at 1201. Justice Breyer wrote, for the majority, that one could think of the technology as having three essential parts:

First, the API includes "implementing code," which actually instructs the computer on the steps to follow to carry out each task. Google wrote its own programs (implementing programs) that would perform each one of the tasks that its API calls up.

Second, the Sun Java API associates a particular command, called a "method call," with the calling up of each task. The symbols **java.lang.**, for example, are part of the command that will call up the program (whether written by Sun or, as here, by Google) that instructs the computer to carry out the "larger number" operation. Oracle does not here argue that the use of these commands by programmers itself violates its copyrights.

Third, the Sun Java API contains computer code that will associate the writing of a method call with particular "places" in the computer that contain the needed implementing code. This is the declaring code. The declaring code both labels the particular tasks in the API and organizes those tasks, or "methods," into "packages" and "classes." We have referred to this organization, by way of rough analogy, as file cabinets, drawers, and files. Oracle does claim that Google's use of the Sun Java API's declaring code violates its copyrights.

The declaring code at issue here resembles other copyrighted works in that it is part of a computer program. Congress has specified that computer programs are subjects of copyright. It differs, however, from many other kinds of copyrightable computer code. It is inextricably bound together with a general system, the division of computing tasks, that no one claims is a proper subject of copyright. It is inextricably bound up with the idea of organizing tasks into what we have called cabinets, drawers, and files, an idea that is also not copyrightable. It is inextricably bound up with the use of specific commands known to programmers, known here as method calls (such as **java.lang.Math.max**, etc.), that Oracle does not here contest. And it is inextricably bound up with implementing code, which is copyrightable but was not copied.

Id. at 1201 (emphasis in original).

With respect to the nature of the work, the Court concluded that it weighed in favor of fair use, writing that "the declaring code is, if copyrightable at all, further than are most computer programs (such as the implementing code) from the core of copyright." *Id.* at 1202. Justice Breyer explained that "the copied declaring code and the uncopied implementing programs call for, and reflect, different kinds of capabilities. A single implementation may walk a computer through dozens of different steps. To write implementing programs, witnesses told the jury, requires balancing such considerations as how quickly a computer can execute a task or the likely size of the computer's memory. One witness described

that creativity as “magic” practiced by an API developer when he or she worries ‘about things like power management’ for devices that ‘run on a battery.’ . . . This is the very creativity that was needed to develop the Android software for use not in laptops or desktops but in the very different context of smartphones.” *Id.* at 1202. Consequently, Justice Breyer explained, “[t]he declaring code (inseparable from the programmer’s method calls) embodies a different kind of creativity. Sun Java’s creators, for example, tried to find declaring code names that would prove intuitively easy to remember. . . . They wanted to attract programmers who would learn the system, help to develop it further, and prove reluctant to use another. . . . It sought to make the API ‘open’ and ‘then . . . compete on implementations.’” *Id.* Thus, “the declaring code differs to some degree from the mine run of computer programs. Like other computer programs, it is functional in nature. But unlike many other programs, its use is inherently bound together with uncopyrightable ideas (general task division and organization) and new creative expression (Android’s implementing code). Unlike many other programs, its value in significant part derives from the value that those who do not hold copyrights, namely, computer programmers, invest of their own time and effort to learn the API’s system. And unlike many other programs, its value lies in its efforts to encourage programmers to learn and to use that system so that they will use (and continue to use) Sun-related implementing programs that Google did not copy.” *Id.*

The Supreme Court characterized the purpose and character of the use as transformative, and held that it too weighed in favor of fair use. Justice Breyer wrote that “Google copied portions of the Sun Java API precisely, and it did so in part for the same reason that Sun created those portions, namely, to enable programmers to call up implementing programs that would accomplish particular tasks. But since virtually any unauthorized use of a copyrighted computer program (say, for teaching or research) would do the same, to stop here would severely limit the scope of fair use in the functional context of computer programs. Rather, in determining whether a use is ‘transformative,’ we must go further and examine the copying’s more specifically described ‘purpose[s]’ and ‘character.’” *Id.* at 1203. In so doing, the Court focused on the fact that Google used the APIs “to create new products. . . . To the extent that Google used parts of the Sun Java API to create a new platform that could be readily used by programmers, its use was consistent with that creative ‘progress’ that is the basic constitutional objective of copyright itself.” *Id.* Justice Breyer emphasized evidence at trial that reimplementing of APIs is common in the industry (and that Sun itself had used pre-existing interfaces in creating Java) and that Google copied only those desktop APIs necessary for tasks useful for smartphone programs, and did so “only insofar as needed to allow programmers to call upon those tasks without discarding a portion of a familiar programming language and learning a new one. . . . Google, through Android, provided a new collection of tasks operating in a distinct and different computing environment. Those tasks were carried out through the use of new implementing code (that Google wrote) designed to operate within that new environment . . . [or, in the words of some *amici*] ‘reimplementation,’ defined as the ‘building of a system . . . that repurposes the same words and syntaxes’ of an existing

system—in this case so that programmers who had learned an existing system could put their basic skills to use in a new one.” *Id.*

The Supreme Court found that the amount and substantiality of the portion used likewise weighed in favor of fair use. The Supreme Court disagreed with the Federal Circuit’s conclusion that Google could have achieved its Java-compatibility objective by copying only the 170 lines of code that were “necessary to write in the Java language,” which the Supreme Court found viewed “Google’s legitimate objectives too narrowly. Google’s basic objective was not simply to make the Java programming language usable on its Android systems. It was to permit programmers to make use of their knowledge and experience using the Sun Java API when they wrote new programs for smartphones with the Android platform. In principle, Google might have created its own, different system of declaring code. But the jury could have found that its doing so would not have achieved that basic objective. In a sense, the declaring code was the key that it needed to unlock the programmers’ creative energies. And it needed those energies to create and to improve its own innovative Android systems.” *Id.* at 1205-06. In so ruling the Court observed that while the quantitative amount of what Google copied was large if the declaring code were viewed in isolation (37 packages totaling approximately 11,500 lines of code—“virtually all of the declaring code needed to call up hundreds of different tasks”), it was small if considered in the context of the entire set of software material in the Java API, including implementing code—“2.86 million lines, of which the copied 11,500 lines were only 0.4 percent.” *Id.* at 1205.

The Supreme Court also found that the fourth factor—the impact on the market for the genuine product—weighed in favor of fair use given the uncertain nature of Sun’s ability to compete in the smart phone market, the sources of lost revenue, and “the risk of creativity-related harms to the public” *Id.* at 1208. Justice Breyer explained that consideration of this factor can be complex when computer programs are at issue because a court must consider not merely lost revenue but “the public benefits the copying will likely produce.” *Id.* at 1206. The court noted that, with respect to the amount of loss, the jury could have found that Android did not harm the actual or potential markets for Java SE because Sun would not have been able to enter those markets successfully whether Google did or did not copy a part of its APIs. *Id.* The Court also emphasized evidence before the jury that devices using Google’s Android platform were different in kind from the feature phones that licensed Sun technology, and thus, rather than merely repurposing Sun’s code from larger computers to smaller computers, “Google’s Android platform was part of a distinct (and more advanced) market than Java software.” *Id.* at 1207. Looking at “these important differences,” the jury was presented with evidence to show that Android was not a market substitute. *Id.* In addition, the jury heard evidence that Sun foresaw a benefit from the broader use of the Java programming language in a new platform like Android. As for past efforts to seek a license, the Court noted that potential licensing negotiations concerned far more than the 37 packages of declaring code and involved use of Java implementing code, branding and cooperation. Ultimately, “the jury’s fair use determination means that neither Sun’s ef-

engine,³⁶ caching (in connection with operation of an Internet

fort to obtain a license nor Oracle's conflicting evidence can overcome evidence indicating that, at a minimum, it would have been difficult for Sun to enter the smartphone market, even had Google not used portions of the Sun Java API." *Id.* While the Court conceded that copying Java APIs helped Google "make a vast amount of money from its Android platform . . . , [but t]his source of Android's profitability has much to do with third parties' (say, programmers') investment in Sun Java programs. It has correspondingly less to do with Sun's investment in creating the Sun Java API." *Id.* at 1207-08. The Court observed that the Copyright Act does not seek "to protect third parties' investment in learning how to operate a created work." *Id.* at 1208, citing *Campbell*, 510 U.S. at 591-92 (discussing the need to identify those harms that are "cognizable under the Copyright Act"). Finally, the Court opined that "given programmers' investment in learning the Sun Java API, to allow enforcement of Oracle's copyright here would risk harm to the public." *Id.* at 1208. Justice Breyer explained:

Given the costs and difficulties of producing alternative APIs with similar appeal to programmers, allowing enforcement here would make of the Sun Java API's declaring code a lock limiting the future creativity of new programs. Oracle alone would hold the key. The result could well prove highly profitable to Oracle (or other firms holding a copyright in computer interfaces). But those profits could well flow from creative improvements, new applications, and new uses developed by users who have learned to work with that interface. To that extent, the lock would interfere with, not further, copyright's basic creativity objectives. *See Connectix Corp.*, 203 F.3d at 607; *see also Sega Enterprises*, 977 F.2d at 1523-1524 ("An attempt to monopolize the market by making it impossible for others to compete runs counter to the statutory purpose of promoting creative expression"); *Lexmark Int'l*, 387 F.3d at 544 (noting that where a subsequent user copied a computer program to foster functionality, it was not exploiting the programs "commercial value as a copyrighted work" (emphasis in original)). After all, "copyright supplies the economic incentive to [both] create and disseminate ideas," *Harper & Row*, 471 U.S. at 558, and the reimplementing of a user interface allows creative new computer code to more easily enter the market.

Id.

In ruling that Google's reimplementing of Java SE APIs was a fair use, the Court explained that software programs were functional and therefore had to be treated somewhat differently from other literary works. *See id.* at 1198. Justice Breyer emphasized the importance of the idea/expression dichotomy to the Court's analysis (*id.* at 1196) and elaborated that "[t]he fact that computer programs are primarily functional makes it difficult to apply traditional copyright concepts in that technological world." *Id.* at 1208. The Court also made clear that its ruling, in the context of a software program, was not meant to "overturn or modify . . . earlier cases involving fair use—cases, for example, that involve 'knockoff' products, journalistic writings, and parodies." *Id.*

³⁶*See Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1163-67 (9th Cir. 2007); *Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003). In *Kelly v. Arriba Software Corp.*, Ditto.com (previously Arriba Software Corp.) operated a visual search engine that allowed users to locate images on the Web. In response to a query, small, low-resolution "thumbnail" images were displayed next to a link and brief description of the correspond-

ing site where the photograph could be found. Images were obtained automatically by a crawler program that downloaded full-size copies to Arriba's server, where they were converted to thumbnails. Thumbnail images could be copied by users, but their resolution could not be improved. Users, in turn, could access the site where a thumbnail originated from via a link or, for brief periods in 1999 and 2000, view full-size copies of the photographs via in-line links or frames (*see infra* §§ 9.03, 9.04), separate and apart from the rest of the content on the linked site. The Ninth Circuit ruled that the reproduction of thumbnail images constituted a fair use because defendants' copying was transformative (to index images on the Web) and did not adversely affect the potential market for the genuine works because the thumbnails were not a substitute for full-size, high-resolution images. The court found that the nature of the work (creative photographs) weighed slightly in favor of the plaintiff and the amount and substantiality of the portion used was a neutral factor because if Arriba had copied anything less than the complete works it would have been more difficult to identify each image, which would have reduced the usefulness of the search engine. In an earlier ruling that was subsequently vacated because the issue had not been properly preserved for appeal, the Ninth Circuit had ruled that the defendant's initial practice of also making available via in-line links and frames full size copies of the photographs that appeared on indexed sites (with the surrounding text and other Web content removed) was not a fair use. Displaying the exact image from a site in isolation from the surrounding material via a frame or in-line link was held to serve no transformative purpose and to harm the market for genuine works because people receiving photographs in this format would have had no reason to visit the website from which it had been copied. *See Kelly v. Arriba Soft Corp.*, 280 F.3d 934, 947–48 (9th Cir. 2002), *vacated*, 336 F.3d 811 (9th Cir. 2003).

In *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1163–67 (9th Cir. 2007), the Ninth Circuit reaffirmed its 2003 opinion in a case involving very similar facts. In that case, Perfect 10, an adult magazine whose images were widely available without authorization on the Internet, sued Google and Amazon.com arguing that their visual search engines made unauthorized thumbnail reproductions of infringing copies of their works that were displayed with search results. To distinguish *Kelly v. Arriba Software Corp.*, Perfect 10 had argued that these thumbnail images undermined a market for thumbnail images sold for display on cell phones. Unlike in *Kelly*, Perfect 10 had argued (and the district court had agreed), the thumbnails displayed by Google had an adverse impact on the market for genuine products and therefore were not a fair use. The Ninth Circuit reversed, however, concluding that “the significantly transformative nature of Google’s search engine, particularly in light of its public benefit, outweighs Google’s superseding and commercial uses of the thumbnails in this case.” *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1166 (9th Cir. 2007). The court noted that no downloads for mobile phones in fact had taken place, making the superseding use “not significant.” Likewise, although thumbnails directed users to Google AdSense partners, including partners that hosted infringing images, which the court conceded added “a commercial dimension that did not exist in *Kelly*,” the Ninth Circuit emphasized that the district court had not determined that this com-

mercial element was significant. *Id.* at 1167. Judge Ikuto, writing for the court, concluded that “the transformative nature of Google’s use is more significant than any incidental superseding use or the minor commercial aspects of Google’s search engine and website.” *Id.* With respect to the nature of the copyrighted work, the court found the photos to be creative but because the images appeared on the Internet before used in search engine results, this factor weighted only slightly against a finding of fair use. *Kelly v. Arriba* and *Perfect 10 v. Amazon* were cited with approval by the Second Circuit in *Authors Guild v. Google Inc.*, 804 F.3d 202, 217, 227 (2d Cir. 2015), *cert. denied*, 136 S. Ct. 1658 (2016).

In a subsequent case brought by Perfect 10 against a Russian search engine that, unlike Google, displayed full size versions of Perfect 10 images via in line links (and not merely thumbnails) and also displayed them separate and apart from the websites on which they appeared, the district court, in granting in part the defendant’s motion for summary judgment, ruled, among other things, that the defendant’s use of the images in connection with a search engine nonetheless constituted a fair use because it was highly transformative. *See Perfect 10, Inc. v. Yandex, N.V.*, 962 F. Supp. 2d 1146, 1154–55 (N.D. Cal. 2013). The court wrote that “whether a browser window shows only a thumbnail and the full-size image—instead of the full-size image along with part of the surrounding web page—does not affect whether the use of the thumbnail has been transformed.” *Id.* (emphasis in original). Further, the court held that “even if yandex.com’s use of the thumbnail were broadly described as an ‘in-line link connected to a full-size image,’ that use remains highly transformative.” *Id.*; *see generally infra* § 9.03[3][B] (discussing the case at greater length).

By contrast, in *VHT, Inc. v. Zillow Group, Inc.*, 918 F.3d 723, 742-44 (9th Cir.), *cert. denied*, 140 S. Ct. 122 (2019), the Ninth Circuit held that the unauthorized use of copyrighted photos in connection with a visual search engine used on a commercial real estate service’s website was not a fair use, explaining that “the label ‘search engine’ is not a talismanic term that serves as an on-off switch as to fair use.” *Id.* at 742. Unlike the search engines at issue in *Kelly v. Arriba* and *Perfect 10 v. Amazon* (or *Perfect 10 v. Yandex*), Digs, the search engine employed on the Zillow.com website for home improvement and remodeling, was “a closed-universe search engine” that did not crawl the web. Users could search a “searchable set” of images within a “walled garden” *Id.* The search results did not direct users to the original sources of the photos, such as the plaintiff’s website, but rather linked to other pages within Zillow’s website. The Ninth Circuit found that making these images searchable did not fundamentally change their original purpose when produced by the plaintiff. Additionally, Digs displayed entire copies of plaintiff’s images, not merely thumbnails. Zillow’s use, the court found, merely superseded plaintiff’s purpose in creating the images in the first place. As in *Kelly v. Arriba* and *Perfect 10 v. Amazon*, the images at issue were found to be creative. But unlike in those cases, the court found Zillow’s use to have few, if any, transformative qualities. In addition, “[i]n contrast to *Amazon* and *Kelly*, nothing justifie[d] Zillow’s full copy display of VHT’s photos on Digs.” *Id.* at 744. Finally, unlike in those cases, the court found that Zil-

search engine),³⁷ viewing and printing copies of archived

low's use undermined plaintiff's market for licensing the photographs. *Id.* Although the plaintiff had only licensed a handful of photos for secondary uses (and none on a searchable database), the court characterized the market as more significant than the merely hypothetical market at issue in *Perfect 10 v. Amazon*. The appellate panel also found it significant that the plaintiff was "actively exploring" the market for licensing its photos to home design websites like Digs—including with Zillow itself. *Id.*

The Eleventh Circuit in *MidlevelU, Inc. v. ACI Information Group*, 989 F.3d 1205 (11th Cir. 2021), *cert. denied*, 141 S. Ct. 2863 (2021), following *VHT*, likewise affirmed a jury finding that Newstex (operator of ACI Information Group, a wholesale news content aggregator)'s use of MidlevelU (operator of the ThriveAP blog)'s copyrighted articles in the Scholarly Blog Index, a curated index of abstracts and full-text articles of academic blogs, was not a fair use, even though its database was searchable, because, among other things, the jury "could have reasonably found that the Index was not a transformative use based on the Index's inclusion of iFrames showing the full-text content of MidlevelU's articles. A reasonable juror could have found that the iFrames obviated any need for an Index subscriber to visit MidlevelU's website directly, so the Index superseded the use of the originals." *Id.* at 1222.

Although admittedly commercial, placing thumbnail images on an art gallery's website to help potential purchasers decide whether to buy a work was held to be highly transformative and a fair use. *See Magnum Photos Int'l, Inc. v. Houk Gallery, Inc.*, No. 16-CV-7030 (VSB), 2018 WL 4538902 (S.D.N.Y. Sept. 21, 2018).

In *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004), the court found links to a database company's internal emails explaining technical flaws in its electronic voting machines constituted a fair use (for purposes of evaluating an award of fees for knowingly and materially misrepresenting information in a DMCA notification pursuant to 17 U.S.C.A. § 512(f); *see infra* § 4.12[9][D]), where at least some of the emails were not entitled to copyright protection, even though the links directed users to the defendant's entire database. By contrast, creating links to a stream of a live webcast of motor races that were shown in real time was held not be a fair use in *Live Nation Motor Sports, Inc. v. Davis*, 81 U.S.P.Q.2d 1826, 2007 WL 79311 (N.D. Tex. Jan. 9, 2007).

³⁷*Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1118–22 (D. Nev. 2006). In *Field*, the court held that Google's practice of caching websites was highly transformative because it "added something new" rather than supplanting the genuine work, based on five separate functions. First, Google's cache functionality enables users to access content when the original page is inaccessible, thus providing archival copies of value to academics, researchers and journalists. Second, providing cached links allows users to detect changes that have recently been made to a site. Third, because it controls the archived copy cached on its servers, Google provides highlighting, which allows users to quickly see where searched terms are located within a page. Fourth, Google uses several design features to make it clear that the cached copy is not intended to be a substitute for the original page (including using a prominent disclaimer at the top of the page).

website pages from the Wayback Machine (www.Archive.org),³⁸ authorizing automated copying and distribution of images over a Content Delivery Network (CDN),³⁹

Fifth, Google ensures that any site owner can disable the cache functionality. In the court's view, "site owners, not Google, control whether 'cached' links will appear for their pages. The fact that the owners of billions of Web pages choose to permit these links to remain is further evidence that they do not view Google's cache as a substitute for their own pages." *Id.* at 1119. The court found that the commercial nature of the enterprise did not negate its fair use. With respect to the nature of the works, the court deemed it significant that the photographs at issue had been made available for free on the plaintiff's own website and that Field had affirmatively sought to have the site indexed by Google by adding a "robots.txt" file to ensure that all search engines would index it, when he could have prevented Google from indexing and caching the site by simply using the "no archive" metatag. With respect to the amount and substantiality of the portion used, the court found that factor to be neutral because even though the entire work is used, Google used no more of the work than necessary. With respect to the market for the genuine product, the court found no evidence that there was any market for Field's photographs and no evidence of any harm, making this factor weigh strongly in favor of fair use. Finally, the court concluded that Google's good faith in operating the system was an independent factor weighing in favor of fair use.

³⁸*Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F. Supp. 2d 627 (E.D. Pa. 2007) (granting summary judgment for the defendants).

³⁹*See Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *20-21 (C.D. Cal. Jan. 16, 2015). The court explained that

to ensure adequate and efficient service, service providers across the internet use CDNs to actually distribute their content. This practice ensures that a service provider does not rely on a single server of its own to maintain full operation of its service and means that the burden is spread and networks operate smoothly. In essence, rather than keeping everything in one place, an outsourced network of multiple servers is used to ensure smooth operation of the internet generally and a service provider's services in particular. The widespread use of CDNs means that most content is passed from a service provider to one or more third parties before reaching an end user.

Id. at *20-21. In finding distribution to a CDN network to be a fair use, Judge Michael Fitzgerald explained that "this distribution is an inevitable and necessary part of using the internet, and ultimately a trivial activity that falls within the protections of the fair use doctrine." *Id.* at *20. He elaborated that "such usage is minimal and is a crucial part of maintaining not only internet commerce, but the efficient operation of the internet generally. It also causes only minor and wholly incidental copying and distribution of images." *Id.* at *21. Analogizing the use to caching found permissible by the Ninth Circuit in *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1169-77 (9th Cir. 2007), Judge Fitzgerald explained that "[a]s in *Amazon.com*, eBay's use of CDNs is designed to 'enhance [a user's] use, not to supersede the copyright holders' exploitation of their works.'"

digitizing books to allow their texts to be fully searchable (and, among other things, used for data mining⁴⁰) or to allow print-disabled library patrons access to works in formats ac-

2015 WL 1600081, at *21, quoting *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1169 (9th Cir. 2007).

⁴⁰*Authors Guild v. Google Inc.*, 804 F.3d 202 (2d Cir. 2015), cert. denied, 136 S. Ct. 1658 (2016); *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87 (2d Cir. 2014). In *Authors Guild, Inc. v. HathiTrust*, the Second Circuit held that allowing library patrons to access the digitized book collections of member-research university libraries that had allowed Google to electronically scan and place their collections in a repository was a fair use where HathiTrust (1) allowed the general public to search for particular terms across all digital copies but, unless the copyright holder authorized broader use, the search results only showed page numbers on which the search term was found within each work and the number of times the word appeared on each page and (2) permitted member libraries to provide patrons with certified print disabilities access to the full text of copyrighted works in a format where they could perceive the works (such as via software that converted the text into spoken words or magnified the text). The appellate court remanded for further consideration the question of whether permitting members to create a replacement copy of a work, if the member already owned an original copy, where the original copy was lost, destroyed or stolen and where a replacement copy was unavailable at a “fair price” constituted a fair use.

Judge Barrington D. Parker, writing for himself and Judges Walker and Cabranes, characterized the creation of a full-text searchable database as “a quintessentially transformative use” that was “different in purpose, character, expression, meaning, and message from the page (and the book) from which it was drawn” and did not merely supersede the purpose of the original creations or recast them in a new mode of presentation. *Id.* at 97. The court found the nature of the copyrighted work to be of limited usefulness because the creative works at issue were being used for a transformative purpose. With respect to the amount and substantiality of the portion taken, the court found that the amount copied was not excessive because it was reasonably necessary for the Trust “to make use of the entirety of the works in order to enable the full-text search function” *Id.* at 98. The appellate panel further found that maintaining four copies at two separate locations was “reasonably necessary” to facilitate legitimate uses (such as balancing the load of user web traffic to avoid burdening a single site and for use as a backup at each location). *Id.* at 99. Finally, the court rejected as irrelevant the argument that digitizing books for search adversely impacted the market for licensing books for digital search that could emerge in the future because lost licensing revenue would only be relevant if it served as a substitute for the original product which full-text search did not. The court also rejected the argument that the risk of a security breach could adversely impact the market for genuine works based on unrebutted evidence of the extent to which the HathiTrust had implemented security measures to reduce the risk of a breach, noting, however, that it was not “foreclosing a future claim based on circumstances not predictable” *Id.* at 101.

The court declined to determine whether making a replacement copy would be permissible if (1) the member already owned an original copy, (2) the member's original copy was lost or stolen and (3) a replacement copy was unavailable at a fair price, because the panel concluded the plaintiffs did not have standing to object to this practice. *See id.* at 103–04.

In *Authors Guild v. Google Inc.*, 804 F.3d 202 (2d Cir. 2015), *cert. denied*, 136 S. Ct. 1658 (2016), the Second Circuit, in an opinion written by Judge Pierre Leval on behalf of himself and Judges Cabranes and Parker, affirmed the lower court order entered by Second Circuit Judge Denny Chin, sitting as a district court judge, granting summary judgment for Google, based on the findings that Google's digitization of books for its library and book projects, provision of digital copies to participating libraries that already owned the books, and display of snippets in response to search queries for particular terms contained in digitized books, constituted fair use of plaintiffs' works.

Google, without permission of the rights holders, made digital copies of tens of millions of books that were submitted to it for that purpose by major libraries. Google scanned the digital copies and established a publicly available search tool. An Internet user could use this tool to search without charge to determine whether a book contained a specified word or term and would be shown "snippets" of text that included the searched-for terms. Google also allowed participating libraries to download and retain digital copies of the books they submitted, pursuant to agreements that committed the libraries not to use their digital copies in violation of copyright laws.

The appellate panel held that Google's making of a digital copy to provide what the court characterized as "a search function" was a transformative use that augmented public knowledge by "making available information *about* Plaintiffs' books without providing the public with a substantial substitute for matter protected by the Plaintiffs' copyright interests in the original works or derivatives of them." *Id.* at 207 (emphasis in original). The court found that Google's provision of the snippet function was also a fair use because Google imposed significant limitations on access to snippets, which meant that it did not supplant the market for those books that had been digitized. Specifically, Google's search tool displayed a maximum of three snippets containing a given search term. A snippet was a horizontal segment of non-overlapping text comprising ordinarily an eighth of a page (or approximately three lines of text for a book that contains twenty four lines per page). The search tool did not allow a searcher to increase the number of snippets revealed by repeated entry of the same search term or by entering searches from different computers (although a user could see different snippets by searching different terms). Google also made permanently unavailable for viewing one snippet on each page and one complete page out of every ten (through a process that Google called "blacklisting"). Google also disabled snippet view entirely for books for which a single snippet would likely satisfy a researcher's need for the book, such as dictionaries, cookbooks and books of short poems. Since 2005, Google also excluded books from snippet view at the request of the rights holder. No advertising was displayed to users

of its search tool. Nor did Google receive any payment by reason of a searcher's use of Google's link to purchase a book, in instances where a link to allow purchase of a book was provided.

Judge Leval found Google's digitization of books to allow data mining and "text mining" to be transformative because it "provide[d] otherwise unavailable information about the originals." *Id.* at 215. Judge Leval acknowledged that Google's use differed from *HathiTrust* in two significant respects. First, HathiTrust did not display any text from the underlying work to a user, whereas Google Books provided a searcher with snippets containing the word that was the subject of a given search. Second, HathiTrust was a nonprofit educational entity, whereas Google was "a profit-motivated commercial corporation." *Id.* at 217. Judge Leval found neither difference determinative, however.

Snippets, Judge Leval wrote, added "important value to the basic transformative search function, which tells only whether and how often the searched term appears in the book." *Id.* He explained that merely knowing that a given word is used a particular number of times does not tell the searcher whether he or she needs to obtain a copy of the book. For example, "a searcher seeking books that explore Einstein's theories, who finds that a particular book includes 39 usages of 'Einstein' will nonetheless conclude that she can skip that book if the snippets reveal that . . . 'Einstein' . . . is the name of the author's cat." *Id.* at 218. In finding the provision of snippets to be transformative, Judge Leval wrote that "Google's division of the page into tiny snippets is designed to show the searcher just enough context surrounding the searched term to help her evaluate whether the book falls within the scope of her interest (without revealing so much as to threaten the author's copyright interests)." *Id.*

With respect to Google's commercial motivation, Judge Leval conceded that although Google received no revenue from its operation of Google Books, Google indirectly profited from the service. He found, however, that Google's profit motivation did not outweigh Google Books' "highly convincing transformative purpose, together with the absence of significant substitutive competition" *Id.* at 219. In so ruling he noted that "[m]any of the most universally accepted forms of fair use, such as news reporting and commentary, quotation in historical or analytical books, reviews of books, and performances, as well as parody, are all normally done commercially for profit." *Id.*

The panel held that the second fair use factor—the nature of the work—was not determinative. Although plaintiffs' works were factual, Judge Leval wrote that the authors' manner of expressing facts and ideas was entitled to copyright protection. On balance, however, the court found more significant that "the secondary use transformatively provides valuable information about the original, rather than replicating protected expression in a manner that provides a meaningful substitute for the original." *Id.* at 220.

The appellate panel found that the amount and substantiality of the use favored Google because even though Google copied the entirety of each of plaintiffs' books, it did not reveal the digital copies to the public. Each copy was made "to enable search functions to reveal limited, important information about the books." *Id.* at 222.

The court likewise found that this factor weighed in favor of fair use with respect to the use of snippets because the amount and substantiality of the portion used in *making a copy* was not the relevant consideration. Rather, it was “the amount and substantiality of *what is thereby made accessible* to a public for which it may serve as a competing substitute.” *Id.* (emphasis in original). In that regard, Google had constructed the snippet feature to substantially protect against it serving as “an effectively competing substitute” for plaintiffs’ books through a variety of limitations, including the small size of each snippet, the blacklisting of one snippet per page and one page in every ten, the fact that no more than three snippets were shown—and no more than one per page—for each term searched, and the fact that the same snippets were shown for a searched term no matter how many times, or from how many different computers, the term was searched. Judge Leval explained that “[t]he result of these restrictions is, so far as the record demonstrates, that a searcher cannot succeed, even after long extended effort to multiply what can be revealed, in revealing through a snippet search what could usefully serve as a competing substitute for the original.” *Id.* He explained that blacklisting permanently blocked 22% of a book’s text from snippet view and the balance of the 78% that potentially could be shown in snippets was not in fact accessible. “[E]ven after protracted effort over a substantial period of time, only small and randomly scattered portions of a book will be accessible”—as evidenced by the fact that plaintiffs had employed researchers for a period of weeks to do multiple word searches on plaintiffs’ books and in no case were they able to access even 16% of the text “and the snippets collected were usually not sequential but scattered randomly throughout the book.” *Id.*

For similar reasons, the court held that the effect of the copying on the market for or the value of the copyrighted work weighed in favor of fair use. Judge Leval wrote that “[e]specially in view of the fact that the normal purchase price of a book is relatively low in relation to the cost of manpower needed to secure an arbitrary assortment of randomly scattered snippets, we conclude that the snippet function does not give searchers access to effectively competing substitutes.” *Id.* at 224. Although Judge Leval conceded that some sales would be lost, this was not enough to amount to “a meaningful or significant effect ‘upon the potential market for or value of the copyrighted work.’” *Id.*, quoting 17 U.S.C.A. § 107(4). Moreover, he observed that the type of loss of sales likely to be experienced probably would involve “interests that are not protected by the copyright.” *Id.* For example, Judge Leval wrote, a researcher who wanted to find out the date when President Roosevelt was stricken by polio likely could find this information from a snippet. He explained, however, that this detail is a historical fact that an author’s copyright does not cover. A copyright “does not extend to the facts communicated by . . . [a] book. It protects only the author’s manner of expression.” *Id.* Judge Leval commented that “[t]he fact that, in the case of the student’s snippet search, the information came embedded in three lines of . . . [an author’s] writing, which were superfluous to the searcher’s needs, would not change the taking of an unprotected fact into copyright infringement.” *Id.* He further elaborated that:

cessible to them⁴¹), using files from a company's mobile device operating system in order to virtualize it for use by security researchers,⁴² reprinting legal briefs that had been

Even if the snippet reveals some authorial expression, because of the brevity of a single snippet and the cumbersome, disjointed, and incomplete nature of the aggregation of snippets made available through snippet view, we think it would be a rare case in which the searcher's interest *in the protected aspect* of the author's work would be satisfied by what is available from snippet view, and rarer still—because of the cumbersome, disjointed, and incomplete nature of the aggregation of snippets made available through snippet view—that snippet view could provide a significant substitute for the purchase of the author's book.

Id. at 224–25. In so ruling, the court rejected plaintiffs' argument that plaintiffs had a derivative right in the application of search and snippet view functions, finding “no merit” to this argument, which in Judge Leval's view confused transformativeness with the type of transformation that might be found when a derivative work is created. The court further found that there was no market for search and snippet licenses. *Id.* at 225–27.

Judge Leval rejected plaintiffs' argument that exposure to risks of hacking undermined Google's fair use defense because of the potentially adverse impact on the market for the genuine products that a security breach could cause, because Google Books' digital scans were stored on computers walled off from public Internet access and the evidence presented suggested they were very secure. *Id.* at 227–28. The court noted, however, that:

If, in the course of making an arguable fair use of a copyrighted work, a secondary user unreasonably exposed the rights holder to destruction of the value of the copyright resulting from the public's opportunity to employ the secondary use as a substitute for purchase of the original (even though this was not the intent of the secondary user), this might well furnish a substantial rebuttal to the secondary user's claim of fair use.

Id. at 227. Finally, the appellate panel held that Google's distribution of digital copies to participant libraries was a fair use. The court observed that “[i]f the library had created its own digital copy to enable its provision of fair use digital searches, the making of the digital copy would not have been infringement.” *Id.* at 229. Similarly, Judge Leval wrote, the same act does not “become an infringement because, instead of making its own digital copy, the library contracted with Google that Google would use its expertise and resources to make the digital conversion for the library's benefit.” *Id.*

⁴¹*Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 101–03 (2d Cir. 2014). The court held that providing expanded access to the print disabled was not a transformative use, but was still permissible because the making a copy of a copyrighted work for the convenience of a blind person was identified by the U.S. Supreme Court as an example of fair use recognized in the legislative history of the 1976 Copyright Act. *Id.* at 102, *citing Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 455 n.40 (1984). The Second Circuit also found that the market for books accessible to visually impaired readers was so insignificant that authors typically forego royalties from specialized format versions of their works.

⁴²*See Apple Inc. v. Corellium, LLC*, 510 F. Supp. 3d 1269, 1285–92

publicly filed in court cases in a database of legal resources,⁴³ reproducing a copyrighted photograph in an article discussing a copyright infringement suit brought over the image⁴⁴ or on a blog post critical of the person depicted in the image⁴⁵ (or linking to an Instagram post that includes a

(S.D. Fla. 2020) (holding that a developer's use was highly transformative and a fair use). In rejecting Apple's argument that the defendant merely repacked its operating system, the court explained:

The Corellium Product is not merely a repackaged version of iOS—this time in a virtual environment as opposed to an iPhone. Rather, Corellium makes several changes to iOS and incorporates its own code to create a product that serves a transformative purpose. The Corellium Product makes available significant information about iOS, permitting users to, inter alia: (1) see and halt running processes; (2) modify the kernel; (3) use CoreTrace, a tool to view system calls; (4) use an app browser and a file browser; and (5) take live snapshots. These features are beneficial to security research. And, as Apple concedes, the Corellium Product adds significant features that are not available on Apple's devices running iOS.

Id. at 1286-87.

⁴³*White v. West Publishing Corp.*, 12 Civ. 1340 (JSR), 2014 WL 3385480 (S.D.N.Y. July 3, 2014) (granting summary judgment for West and Lexis).

⁴⁴*See, e.g., Leveyfilm, Inc. v. Fox Sports Interactive Media, LLC*, No. 13 C 4664, 2014 WL 3368893, at *9-12 (N.D. Ill. July 8, 2014) (holding that reprinting a copy of an image in an online article discussing a copyright infringement suit about the image was a fair use).

⁴⁵*See, e.g., Katz v. Google, Inc.*, 802 F.3d 1178 (11th Cir. 2015) (affirming the entry of summary judgment for the defendant-blogger in a suit where a real estate developer and part owner of the Miami Heat purchased the copyright to an unflattering image of himself and then sued the operator of a blog critical of his business practices for copyright infringement for displaying the image in connection with a critical post about him); *Weinberg v. Dirty World, LLC*, Case No. CV 16-9179-GW(PJWx), 2017 WL 5665023, at *5-13 (C.D. Cal. July 27, 2017) (granting partial summary judgment for the operator of *TheDirty.com*, holding that a photo posted on its website constituted a fair use; "The Post, especially viewed within the context of the Website was transformative. Rather than using the photo to merely identify Plaintiff or his wife, as Plaintiff did on her Facebook profile page, or glorify Plaintiff and his wife's lifestyle, as the creator of Astrid in Wonderland did, the entire Post uses the Video Image as part of a direct critique on Plaintiff's wife's appearance, her status as a model, her husband, and her relationship with her husband."); *Dhillon v. Does 1-10*, No. C 13-01465 SI, 2014 WL 722592 (N.D. Cal. Feb. 25, 2014) (granting summary judgment for the defendant, holding that the use of a political candidate's official campaign photograph on a blog critical of her views constituted a fair use).

By contrast, merely using a commercial photo available for license, in connection with a blog post unrelated to the photograph and not in transformative manner, is unlikely to be deemed a fair use. *See, e.g., Brammer v. Violent Hues Productions, LLC*, 922 F.3d 255 (4th Cir. 2019)

(holding that use of a stock photo of the Adams Morgan area of Washington DC, copied from Flickr in response to a Google search, to promote a film festival, was not a fair use); *Michael Grecco Productions, Inc. v. Valuewalk, LLC*, 345 F.Supp.3d 482, 504-09 (S.D.N.Y. 2018) (holding that copying a photo from a competitor's website for use in an article on the same subject was not a fair use).

In *O'Neil v. Ratajkowski*, 19 Civ. 9769 (AT), 2021 WL 4443259 (S.D.N.Y. Sept 28, 2021), the court denied cross-motions for summary judgment on the issue of whether model Emily Ratajkowski's posting a photograph of herself on her own Instagram account for 24 hours (on Instagram Stories, which disappear after that time) constituted a fair use. Judge Analisa Torres found that the purpose of paparazzi photos such as the one at issue in that case was to "document the comings and goings of celebrities, illustrate their fashion and lifestyle choices, and accompany gossip and news articles about their lives." *Id.* at *6, *quoting Barcroft Media, Ltd. v. Coed Media Group, LLC*, 297 F. Supp. 3d 339, 352 (S.D.N.Y. 2017). "Therefore, when news sites have copied paparazzi photographs to document celebrities' lives, courts have determined those uses are not transformative. . . . By contrast, where photographs are used to comment on the image—rather than to illustrate an independent news story—courts have found those uses to be transformative." *Ratajkowski*, 2021 WL 4443259, at *6. In holding the issue of transformativeness to be disputed, Judge Torres wrote that:

A reasonable observer could conclude the Instagram Photograph merely showcases Ratajkowski's clothes, location, and pose at that time—the same purpose, effectively, as the Photograph. On the other hand, it is possible a reasonable observer could also conclude that, given the flowers covering Ratajkowski's face and body and the text "mood forever," the Instagram Photograph instead conveyed that Ratajkowski's "mood forever" was her attempt to hide from the encroaching eyes of the paparazzi—a commentary on the Photograph. See *Ratajkowski Dep. Tr.* at 39:21–23 (noting that "mood is a millennial way of using an expression or an image to express how someone feels about something").

Id. at *7. The court found the use was only minimally commercial and did not reflect bad faith, as there was no evidence that Ratajkowski was aware that the photograph was not one of numerous ones forwarded to her by fans for resharing on social media. Judge Torres ruled that the nature of the work weighed in favor of the plaintiff, "but only marginally so" because it was essentially factual in nature. *Id.* at *8-9. The amount and substantially of the use weighed somewhat in favor of the plaintiff given that she used more of the photo than necessary for her purpose, but "the fact that it was posted on Instagram Stories lessens that weight." *Id.* at *10. Finally, with respect to the effect on the market, the court found insufficient evidence to rule either way. The photograph was offered for license on Splash but Ratajkowski's face was covered in the picture and plaintiff failed to make any money licensing it. *See id.* at *10-11; *see generally* Bill Donahue, *Celebrities Keep Getting Sued Over Instagrams of Themselves*, Law360, Sept. 17, 2020 (describing similar suits by Paparazzi photographers brought against LeBron James, Justin Bieber, Gigi Hadid, Khloe Kardashian, and Katy Perry for reposting photographs of themselves on their own Instagram accounts).

copyrighted photograph, in an article that discusses the post and the subject matter of the photo⁴⁶), or as part of a website exhibition by an art museum⁴⁷ or in new works of art,⁴⁸

⁴⁶See, e.g., *Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 6393010 (E.D.N.Y. Nov. 2, 2020) (dismissing, as fair use, a photographer's copyright infringement claim against a sports news publisher, which had included an embedded link to an Instagram post by professional tennis player Caroline Wozniacki, announcing her retirements (which included a low-resolution, cropped version of a photograph taken by the plaintiff), in an article it published about Wozniacki's career, which also quoted the text of the Instagram post); *Walsh v. Townsquare Media, Inc.*, 464 F. Supp. 3d 570 (S.D.N.Y. 2020) (entering judgment on the pleadings, based on fair use, on a Paparazzi photographer's copyright infringement claim, brought against the publisher of *XXL* magazine, which had embedded a link to an Instagram post by hip hop artist Cardi B, which included a photograph taken by plaintiff of Cardi B at a Tom Ford fashion show, in an article entitled *Cardi B Partners with Tom Ford for New Lipstick Shade*, which was focused on the event and referenced the Cardi B Instagram post which featured the photograph).

⁴⁷See, e.g., *Marano v. Metropolitan Museum of Art*, 844 F. App'x 436 (2d Cir. 2021) (affirming dismissal of plaintiff's Complaint alleging that the Met infringed his copyright in a 1982 photograph he took of Eddie Van Halen playing his "Frankenstein" guitar by including it in an exhibition of rock n' roll instruments on its website).

⁴⁸See, e.g., *Cariou v. Prince*, 714 F.3d 694 (2d Cir. 2013). But see *Andy Warhol Foundation for the Visual Arts, Inc. v. Goldsmith*, 11 F.4th 26 (2d Cir. 2021) (holding that Andy Warhol screenprint illustrations infringed plaintiff's photograph of the musician Prince, in a decision that has been widely criticized), *rev'g*, 382 F. Supp. 3d 312 (S.D.N.Y. 2019) (granting summary judgment for the Andy Warhol Foundation); see also, e.g., Blake Gopnik, *Warhol a Lame Copier? The Judges Who Said So Are Sadly Mistaken*, N.Y. Times, Apr. 5, 2021; see generally Ian C. Ballon, *Appropriation Art and Fair Use under U.S. Law* in *Art Law: Cases and Controversies* (2022).

In *Cariou v. Prince*, the Second Circuit held that twenty-five of Richard Prince's *Canal Zone* paintings and collages were transformative of Patrick Cariou's photographs as a matter of law (while five were close calls, remanded for the jury to evaluate). The *Canal Zone* paintings incorporated classical portraits and landscape photographs torn out from four (lawfully purchased) copies of Cariou's book *Yes Rasta*, which Prince altered by, among other things, painting "lozenges" over their subjects' facial features and using only portions of some of the images, imagining the characters to be part of a band.

In *Warhol v. Goldsmith*, the Second Circuit held that Andy Warhol's painting of the musician Prince infringed the plaintiff's copyright in a famous photograph of Prince, and was not a fair use, where both the photograph and painting had been considered for the same *Vanity Fair* cover. Unlike the typical case involving reuse of a photograph by a contemporary artist, Warhol's use was found to adversely impact the derivative market for licensing stylized portraits of musicians for magazine

incorporating logos, images or text in documentary or artistic films,⁴⁹ reproducing Grateful Dead concert posters in chronological order in a timeline in a book about the band to commemorate historic events (and arranged in a creative fashion and displayed in significantly reduced form),⁵⁰ taking a picture of a copyrighted object for the purpose of legitimately selling the object under the first sale doctrine,⁵¹

articles. The court also found the two works to have an identical purpose and character and, controversially, that Warhol's use was not transformative. On transformation, the appellate panel wrote that "where a secondary work does not obviously comment on or relate back to the original or use the original for a purpose other than that for which it was created, the bare assertion of a 'higher or different artistic use[]' is insufficient to render a work transformative." *Warhol v. Goldsmith*, 11 F.4th at 41, *quoting Rogers v. Koons*, 960 F.2d 301, 310 (2d Cir. 1992). *Rogers v. Koons*, however, was decided two years before the U.S. Supreme Court's decision in *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994), which endorsed and elevated Judge Leval's analysis of transformative use, and *Rogers* does not even discuss transformativeness (it addressed parody, which was not at issue in *Warhol*). *Rogers v. Koons* was based on pre-*Campbell* case and is not consistent with more current U.S. Supreme Court analysis. See Ian C. Ballon, *Appropriation Art and Fair Use under U.S. Law* in *Art Law: Cases and Controversies* (2022) (analyzing the Second Circuit's transformative use analysis in *Warhol* in light of controlling U.S. Supreme Court case law (primarily *Campbell* and *Google v. Oracle*) and other circuit court opinions).

⁴⁹See, e.g., *Bouchat v. Baltimore Ravens Limited Partnership*, 737 F.3d 932 (4th Cir. 2014) (holding that the NFL had a fair use right to display an artist's copyrighted logo that was used as part of the Baltimore Ravens football team logo incidentally in videos about the team featured on television and on the web and in team photographs displayed at football stadiums); *Arrow Productions, Ltd. v. Weinstein Co.*, 44 F. Supp. 2d 359 (S.D.N.Y. 2014) (holding that a movie production company's use of recreated scenes from the pornographic movie "Deep Throat" in a critical biographical film about Linda Lovelace, one of the actors in that movie, was a fair use where the scenes served a completely different and transformative purpose from the original film (to show how the actress was being manipulated)).

⁵⁰See *Bill Graham Archives v. Dorling Kindersley Ltd.*, 448 F.3d 605, 608-15 (2d Cir. 2006).

⁵¹See *Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *14-20 (C.D. Cal. Jan. 16, 2015) (photographs of magazines lawfully offered for resale that included licensed copies of plaintiff's Paparazzi photographs). In contrast to sales on eBay.com, courts have rejected fair use defenses raised against the same Paparazzi photographer where the original image was unlicensed or used in a way that supplanted the market for the genuine product. See *Rosen v. Masterpiece Marketing Group, LLC*, CV 15-06629 SJO (ASx), 2016 WL 7444688, at *11-13 (C.D. Cal. Nov. 29, 2016) (granting summary judgment for Rosen on the

displaying the copyrighted tattoos of NBA players in a videogame where the player's use has been licensed,⁵² posting a video commenting on or responding to another YouTuber's video,⁵³ copying a competitor's product bulletin and annotating it to dispute the competitor's claims,⁵⁴ posting a copyrighted solicitation advertisement and chart on Reddit to comment about the fundraising methods of the copyright owner,⁵⁵ and, under certain circumstances, temporary "intermediate copying" undertaken for the purpose of reverse

defendant's fair use defense where, among other things, the original photo was not licensed and the use of a high resolution copy to advertise the sale supplanted the market for the copyrighted work); *Rosen v. R&R Auction Co.*, Case No. CV 15-07950-BRO (JPRx), 2016 WL 7626443, at *7-10 (C.D. Cal. Aug. 31, 2016) (granting in part plaintiff's motion for summary judgment, holding that defendant's use of plaintiff's photo to advertise a signed copy available via online auctions was not a fair use where, among other things, the image supplanted the market for the genuine copy). *Rosen v. eBay* underscores that it can be a fair use to advertise a lawful copy of a photo, when offered for sale, if done correctly.

⁵²See *Solid Oak Sketches, LLC v. 2K Games, Inc.*, 449 F. Supp. 3d 333, 347-50 (S.D.N.Y. 2020). But see *Alexander v. Take-Two Interactive Software, Inc.*, 489 F. Supp. 3d 812, 820-22 (S.D. Ill. 2020) (holding that material factual disputes precluded summary judgment on the issue of whether the defendants' display of six tattoos inked by the plaintiff on a professional wrestler, in its video game (which depicted the wrestler), constituted a fair use).

⁵³See, e.g., *Hughes v. Benjamin*, 437 F. Supp. 3d 382, 390-94 (S.D.N.Y. 2020) (dismissing plaintiff's copyright infringement claim in a dispute between YouTubers with competing political views, holding that Benjamin copied 20% of Hughes' *We Thought She Would Win* for the transformative purposes of criticism and commentary, as was "apparent from the broader context of Benjamin's YouTube channel, where it was posted" where there was "no danger" that *SJW Levels of Awareness* would usurp the market of progressive commentaries such as *We Thought She Would Win* because "Benjamin's target audience (generally political conservatives and libertarians) is obviously not the same as Hughes's target audience (generally political liberals)."); *Hosseinzadeh v. Klein*, 276 F. Supp. 3d 34, 41-43 (S.D.N.Y. 2017) (granting summary judgment for defendant Klein on plaintiff's copyright infringement claim, holding that critical commentary on a creative video posted on YouTube constituted a fair use where Kleins' criticism and commentary was interwoven with clips from the Hoss video).

⁵⁴See *Miller UK Ltd. v. Caterpillar Inc.*, No. 10-cv-03770, 2015 WL 6407223, at *7-8 (N.D. Ill. Oct. 21, 2015) (granting summary judgment on Caterpillar's counterclaim for copyright infringement).

⁵⁵See, e.g., *In re DMCA Subpoena to Reddit, Inc.*, 441 F. Supp. 3d 875, 884-87 (N.D. Cal. 2020) (holding that the use of a chart and advertisement by an anonymous poster on the Jehovah's Witness forum on Reddit, for the purpose of discussing donations to Jehovah's Witnesses, was a fair use, and quashing a DMCA subpoena seeking disclosure of the poster's

engineering computer software.⁵⁶

identity).

⁵⁶Disassembly of object code was held to be a fair use in *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992) because (a) disassembly was necessary to analyze those aspects of the program that were unprotectable, and (b) Accolade had a legitimate interest in analyzing the program (to determine how to make its cartridges compatible with the Sega Genesis console). By contrast, disassembly was held not to be a fair use in *Atari Games Corp. v. Nintendo of America Inc.*, 975 F.2d 832, 834 (Fed. Cir. 1992), although the court noted in *dicta* that disassembly may be fair use when the nature of the work makes such copying necessary to understand the unprotectable ideas and processes inherent in the program, and the reproduction is limited in scope and does not involve commercial exploitation of the protected aspects of the work. Subsequently, in *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir.), *cert. denied*, 531 U.S. 871 (2000), the Ninth Circuit approved of disassembly of object code software for the purpose of creating simulated source code to allow the defendant to write an emulator program to be used to run plaintiff's protected video games—which are designed for proprietary PlayStation hardware—on Apple's operating systems. The Ninth Circuit ruled in favor of the defendant even though the process required the creation of multiple unauthorized temporary copies of plaintiff's work. *See Connectix Corp.*, 203 F.3d at 601. The panel elaborated that intermediate copying of software may be found to be a fair use where it is necessary to gain access to unprotectable, functional elements of the software itself. *See id.* at 603. The court clarified, however, that for purposes of evaluating whether intermediate copying of software is a fair use *necessity* means “the necessity of the method, i.e., disassembly, *not the necessity of the number of times that method was applied.*” *Id.* at 605 (emphasis in original). In so ruling, the Ninth Circuit rejected plaintiff's argument that repeated intermediate copying could be found infringing in circumstances where limited intermediate copying would amount to fair use. Such a rule, the panel wrote, would force engineers in many cases to select the least efficient solution simply to avoid liability, which would involve “the kind of ‘wasted effort that the proscription against the copy-right of ideas and facts . . . [is] designed to prevent.’” *Id.*, quoting *Feist Publications, Inc. v. Rural Telephone Service Co.*, 499 U.S. 340, 354 (1991).

Not all intermediate copying necessarily is a fair use. *See, e.g., DSMC Inc. v. Convera Corp.*, 479 F. Supp. 2d 68, 83 (D.D.C. 2007) (denying defendant's summary judgment motion on the issue of fair use intermediate copying where the defendant was a competitor undertaking intermediate copying of the plaintiff-software developer's database schema to write scripts to migrate data to his competing, replacement program); *Fox Broadcasting Co. v. Dish Network LLC*, 905 F. Supp. 2d 1088, 1102–06 (C.D. Cal. 2012) (holding that intermediate copies of television programs made by Dish to allow use of an advertisement-skipping technology was not a fair use), *aff'd on other grounds*, 747 F.3d 1060 (9th Cir. 2014) (affirming the district court's finding that the plaintiff had not shown irreparable injury without reaching the issue of liability for intermediate copies); *see also Fox Broadcasting Co. v. Dish Network LLC*, 160 F. Supp. 3d 1139, 1174–76 (C.D. Cal. 2015) (granting partial summary judgment in

On the other hand, repackaging in a CD-ROM and selling shareware software that was available free of charge over the Internet (subject to a unilateral license providing that it could not be commercially distributed),⁵⁷ making intermediate copies of television programs to allow subscribers to use an advertisement-skipping technology to replay the transmissions without commercial interruption,⁵⁸ streaming family-friendly versions of motion pictures that omitted strong language,⁵⁹ copying news programs to create a searchable index to allow paying subscribers to obtain relevant clips (in competition with the copyright owner),⁶⁰ publishing previously

favor of FOX based on the court's finding that Dish's practice of making QA copies to determine where in a given transmission advertisements appeared did not constitute a fair use).

For further discussion of reverse engineering as fair use, see William S. Coats & Heather D. Rafter, *The Games People Play: Sega v. Accolade and the Right to Reverse Engineer Software*, 15 *Hastings Comm. & Ent. L.J.* 557 (1993).

⁵⁷*Storm Impact, Inc. v. Software of the Month Club*, 13 F. Supp. 2d 782 (N.D. Ill. 1998).

⁵⁸*Fox Broadcasting Co. v. Dish Network LLC*, 905 F. Supp. 2d 1088, 1102–06 (C.D. Cal. 2012), *aff'd on other grounds*, 747 F.3d 1060 (9th Cir. 2014) (affirming the district court's finding that the plaintiff had not shown irreparable injury without reaching the issue of liability for intermediate copies); see also *Fox Broadcasting Co. v. Dish Network LLC*, 160 F. Supp. 3d 1139, 1174–76 (C.D. Cal. 2015) (granting partial summary judgment in favor of FOX based on the court's finding that Dish's practice of making QA copies to determine where in a given transmission advertisements appeared did not constitute a fair use).

⁵⁹*Disney Enterprises, Inc. v. VidAngel, Inc.*, 869 F.3d 848, 860–62 (9th Cir. 2017). The Ninth Circuit affirmed the lower court's entry of a preliminary injunction, finding that deleting words for family-oriented and religious viewers was not transformative because it did not change the expression, meaning or message of the motion pictures. The court also rejected VidAngel's argument that its service actually benefitted the plaintiffs because it purchased DVD copies of the movies and expanded the audience for the copyrighted works to viewers who would not have watched their works without filtering. The appellate panel concluded that it was not clearly erroneous for the district court to reject this argument, holding instead that VidAngel's service was "an effective substitute" for plaintiffs' unfiltered works because surveys suggested that 49% of VidAngel customers would have watched the movies without filters. *Id.* at 861; see also *Disney Enterprises, Inc. v. VidAngel, Inc.*, 371 F. Supp. 3d 708, 719–22 (C.D. Cal. 2019) (rejecting VidAngel's fair use defense and granting summary judgment for plaintiffs); see generally *supra* § 4.04[6] (discussing the company's business in the context of its unsuccessful Family Movie Act defense).

⁶⁰See *Fox News Network, LLC v. TVEyes, Inc.*, 883 F.3d 169 (2d Cir.

unpublished wedding pictures of a celebrity in a celebrity

2018) (holding that TVEyes' copying of Fox News' broadcast content for indexing and clipping services to its subscribers, while transformative, was not a fair use because it adversely impacted FOX's market for selling clips from its news programming). In *TVEyes*, the defendant recorded all television and radio broadcasts for more than 1,400 stations, 24 hours a day, every day, and transformed this material (by copying the closed captioned text that accompanied television content and using speech-to-text software) into a searchable database for its paying subscribers, which included the White House, more than 100 members of Congress and ABC Television, among others (but only businesses, not consumers), who could watch clips of up to ten minutes in length. Using this service, subscribers could search the content using keywords, which would then display thumbnail images of the videos and would play snippets (which began playing 14 seconds prior to the place where the keyword appeared) and display transactional data, including: the title of the program; the precise date and time of the clip; a transcript of the video; the name and location of the channel; market viewership of the clip according to the Nielsen Ratings data; the publicity value of the clip according to data from the television research company, SQAD; and a web address to the website for the channel that features the program or for the program itself if such a web address existed. *See Fox News Network, LLC v. TVEyes, Inc.*, 124 F. Supp. 3d 325 (S.D.N.Y. 2015), *aff'd in part, rev'd in part*, 883 F.3d 169 (2d Cir. 2018); *Fox News Network, LLC v. TVEyes, Inc.*, 43 F. Supp. 3d 379 (S.D.N.Y. 2014). The district court had deemed fair uses the functions enabling clients of TVEyes to search for videos using keyword search terms, to watch the resulting videos, and to archive the videos on the TVEyes servers; but had held that certain other functions were not a fair use, such as those enabling TVEyes's clients to download videos to their computers, to email videos to others, or to watch videos after searching for them by date, time, and channel (rather than by keyword). On appeal, Fox did not challenge the lower court's holding that the creation of the text-searchable database was a fair use but alleged infringement based on redistribution of audio-visual content.

The Second Circuit held that TVEyes's copying and redistribution of Fox content was not a fair use, based primarily on the fourth fair use factor—the impact on the potential market for or value of the copyrighted work. Specifically, it held that TVEyes's Watch function (which also enabled clients to archive, download and email clips, as well as to view clips after conducting a date/time search) was not a fair use and should be enjoined. *See* 883 F.3d at 181-82. The panel concluded that “TVEyes's redistribution of Fox's audiovisual content serves a transformative purpose in that it enables TVEyes's clients to isolate from the vast corpus of Fox's content the material that is responsive to their interests, and to access that material in a convenient manner. But because that re-distribution makes available virtually all of Fox's copyrighted audiovisual content—including all of the Fox content that TVEyes's clients wish to see and hear—and because it deprives Fox of revenue that properly belongs to the copyright holder, TVEyes has failed to show that the product it offers to its clients can be justified as a fair use.” *Id.* at 174.

gossip magazine,⁶¹ copying celebrity photographs on a wedding dress store's online blog,⁶² uploading to and downloading files from a storage locker located in the Cloud incident to the resale of digital music (as opposed to personal use),⁶³ publishing on Twitter a 55-second political campaign video that included an unlicensed 40-second excerpt of a song,⁶⁴ and automatically scraping news stories to include 300 character and 140 character excerpts in a subscription report service⁶⁵ have been held not to constitute a fair use. Needless

With respect to the first factor, the court found the service “at least somewhat transformative.” *Id.* at 178. The panel concluded that the second factor was neutral, while the third factor—the amount and substantiality of the portion taken—strongly favored Fox because TVEyes’s clients were able to “see and hear virtually all of the Fox programming” *Id.* at 181. Of greatest significance, the court found that that, with respect to the fourth factor, TVEyes “usurped a function for which Fox is entitled to demand compensation under a licensing agreement.” *Id.*

⁶¹*Monge v. Maya Magazines, Inc.*, 688 F.3d 1164 (9th Cir. 2012).

⁶²*See FameFlynet, Inc. v. Jasmine Enterprises, Inc.*, 344 F. Supp. 3d 906, 911-15 (N.D. Ill. 2018).

⁶³*Capitol Records, LLC v. ReDigi, Inc.*, 910 F.3d 649, 660–63 (2d Cir. 2018), *cert. denied*, 139 S. Ct. 2760 (2019). In *ReDigi*, the defendant created a secondary market for the resale of digital music. The defendant’s Media Manager software, when downloaded by a user, automatically identified legitimate copies of sound recordings purchased from iTunes (or other ReDigi users), which could then be uploaded to ReDigi’s “Cloud Locker,” at which point they would be deleted from the user’s hard drive so that no more than one copy of the work existed at any one time. A user’s music file could be sold to other ReDigi users, at which point the seller’s access to the file would be terminated and transferred to the purchaser, who could store it in the Cloud Locker, stream it, resell it or download it to his or her computer or other device.

⁶⁴*See Grant v. Trump*, __ F. Supp. 3d __, 2021 WL 4435443 (S.D.N.Y. 2021) (denying former President Trump’s motion to dismiss plaintiff’s copyright infringement suit arising out of Trump’s publication on Twitter of a 55 second video cartoon supporting his unsuccessful reelection effort, which included an unlicensed 40 second excerpt of plaintiff’s song, “Electric Avenue,” which the court characterized as a political satire, not a parody of Grant or his song; “The creator of the video here made a wholesale copy of a substantial portion of Grant’s music in order to make the animation more entertaining. The video did not parody the music or transform it in any way. The video’s overarching political purpose does not automatically make this use transformative, and the other fair use factors also favor the plaintiffs at this stage.”).

⁶⁵*Associated Press v. Meltwater U.S. Holdings, Inc.*, 931 F. Supp. 2d 562, 550–61 (S.D.N.Y. 2013). In *Meltwater*, the court held that the use of AP articles in Meltwater’s news summaries was not transformative and that the summaries were substitutes for the genuine works, with subscrib-

to say, simply using a copy to save the cost of buying additional software licenses⁶⁶ or downloading songs without paying for them ostensibly on a try-before-you-buy basis⁶⁷ have also been found not to be a fair use.

The fair use doctrine “has been called the most troublesome in the whole law of copyright.”⁶⁸

The statutory criteria codified by Congress in the 1970s do not always translate exactly to cyberspace, especially the first time a new use is considered. Among other things, there are many acts of copying that occur in cyberspace because of TCP/IP protocols (such as caching and routing)⁶⁹ or other information dissemination practices that may occur as the result of third-party conduct that may be virtually impossible to monitor or control (such as acts of infringement by individual subscribers of large, legitimate ISPs or people who anonymously post material to interactive areas of corporate websites)⁷⁰ that many people in the Internet community believe constitute—or should constitute—fair use.⁷¹ While there may be strong policy arguments why particular

ers clicking through to the AP articles only 0.08% of the time. The amount and substantiality of the portion taken also weighed against a finding of fair use because Meltwater’s scraping tool automatically took the lede from every AP story which, depending on the length of the article, amounted to between 4.5% and 61% of a genuine work. The court rejected Meltwater’s analogy of its service to the search engines at issue in *Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003) and *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1163–67 (9th Cir. 2007) because, among other things, Meltwater’s searches were not publicly available and were run against only a defined list of content providers.

⁶⁶See *Wall Data Inc. v. Los Angeles County Sheriff’s Dept.*, 447 F.3d 769, 778–82 (9th Cir. 2006).

⁶⁷See *BMG Music v. Gonzalez*, 430 F.3d 888, 889–91 (7th Cir. 2005), cert. denied, 547 U.S. 1130 (2006). Judge Easterbrook, on behalf of the panel, ridiculed Gonzalez’s argument that she only copied 30 files as “no more relevant than a thief’s contention that he shoplifted ‘only 30’ compact disks, planning to listen to them at home and pay later for any he liked.” 430 F.3d at 891. In any case, the defendant’s argument that she was merely sampling songs for potential purchase was undercut by the fact that none of the 30 songs at issue had either been purchased or deleted from her hard drive.

⁶⁸*Monge v. Maya Magazines, Inc.*, 688 F.3d 1164, 1170 (9th Cir. 2012), quoting *Dellar v. Samuel Goldwyn, Inc.*, 104 F.2d 661, 662 (2d Cir. 1939).

⁶⁹See *supra* §§ 1.04, 4.03.

⁷⁰See *infra* §§ 4.11, 4.12, chapters 48 to 50.

⁷¹Congress has established liability limitations that may apply to some of these acts. See *infra* § 4.12. Fair use in connection with informa-

practices should be considered fair use, the applicability of the defense in a given case generally is determined in litigation. Whether the fair use defense may be asserted successfully also depends in part on who is asserting it.⁷²

Because an evaluation of fair use involves a balancing of interests, the issue most often is resolved on motion for summary judgment or at trial.⁷³ Where fair use determinations may be made based on a side-by-side comparison, however, fair use may be resolved on a motion to dismiss.⁷⁴

tion distribution systems also is addressed in chapter 9. The potential relevance of Internet time in fair use analysis is addressed below in § 4.10[3].

⁷²As illustrated in the Church of Scientology cases analyzed below in § 4.10[4], the same act of copying may lead to liability for some defendants, while others may be exonerated under the fair use defense. For example, if an infringing film clip is posted on a website by its owner, the owner may be held liable for copyright infringement while the companies hosting the site or providing Internet access to it might avoid liability under the fair use defense, depending on the particular facts of the case.

⁷³Fair use is a mixed question of law and fact. The determination ultimately is a legal one, but to render the issue of law there may be “subsidiary factual questions”—such as whether there was harm to the actual or potential markets for the copyrighted work or how much of the copyrighted work—that must be addressed, depending on the facts of a given case. See *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183, 1199–1200 (2021).

⁷⁴See, e.g., *Brown v. Netflix, Inc.*, 855 F. App’x 61 (2d Cir. 2021) (affirming dismissal of plaintiff’s copyright infringement claims where Netflix used 8 seconds of plaintiff’s song as part of a documentary film’s commentary on burlesque art and its resurgence in Portland); *Marano v. Metropolitan Museum of Art*, 844 F. App’x 436 (2d Cir. 2021) (affirming dismissal of plaintiff’s Complaint alleging that the Met infringed his copyright in a 1982 photograph of Eddie Van Halen playing his “Frankenstein” guitar by including the photograph in an exhibition of rock n’ roll instruments on the Met’s website); *Brownmark Films, LLC v. Comedy Partners*, 682 F.3d 687, 690–94 (7th Cir. 2012) (affirming dismissal of a suit where the issue of whether an episode of South Park constituted a fair use parody of the viral Internet video “What What (In The Butt)” could be determined by a side-by-side comparison of the two videos); see also *Lombardo v. Dr. Seuss Enterprises, L.P.*, 729 F. App’x 121 (2d Cir. 2018) (affirming judgment on the pleadings for the plaintiff, who was held entitled to a declaratory judgment that his play did not infringe the defendant’s work because it was a fair use parody).

In most cases, however, “[b]ecause fair use is a fact-intensive inquiry, it is rarely appropriate for a court to make a determination of fair use at the motion to dismiss stage.” *Grant v. Trump*, — F. Supp. 3d —, 2021 WL 4435443, at *3 (S.D.N.Y. 2021) (denying former President Trump’s motion to dismiss a copyright infringement suit arising out of his

Although fair use is merely a defense, rather than an affirmative right, and may be difficult to gauge in some cases except through litigation, some users have sought to assert fair use affirmatively in declaratory judgment actions⁷⁵ or suits for damages based on the Digital Millennium Copyright Act⁷⁶ or state law,⁷⁷ where copyright owners have submitted notifications under the DMCA or otherwise alleged infringement involving material or activity that the users contend amount to fair use. Courts have also affirmatively held that copyright owners must consider fair use in certifying their good faith belief that a given use is unauthorized, in a DMCA notification (asking that a service provider disable access to or remove user-submitted content).⁷⁸

A list of reasonably current fair use opinions collected from Pacer is maintained by the U.S. Copyright Office in its

publication on Twitter of a 55 second video cartoon supporting his unsuccessful reelection effort, which included an unlicensed 40 second excerpt of plaintiff's song, "Electric Avenue").

⁷⁵Suits by users seeking a declaration that a given use is fair may be difficult to maintain as declaratory judgment actions where the copyright owner denies that it intends to sue the user for copyright infringement. See, e.g., *Brave New Films 501(C)(4) v. Weiner*, 91 U.S.P.Q.2d 1262, 2009 WL 1622385 (N.D. Cal. June 10, 2009). Users ultimately may have difficulty obtaining a judicial determination that a use is fair absent a real threat of litigation. It may also be difficult to bring a declaratory judgment action except with respect to particular uses of specific works, given that fair use determinations are often fact-specific and cannot be made in the abstract. Cf. *Windstream Services, LLC v. BMG Rights Management (US) LLC*, 16 Civ. 5015 (KMW) (RLE), 2017 WL 1386357 (S.D.N.Y. Apr. 17, 2017) (dismissing Windstream's suit for a declaratory judgment that Windstream was entitled to the safe harbors created by sections 512(a) and 512(c), for lack of subject matter jurisdiction), *appeal dismissed*, Docket No. 17-1515, 2017 WL 5329346 (2d Cir. Sept. 25, 2017); *Veoh Networks, Inc. v. UMG Recordings, Inc.*, 522 F. Supp. 2d 1265 (S.D. Cal. 2007) (dismissing a declaratory relief action brought by a user generated content site, where the plaintiff sought a declaration of its compliance with the Digital Millennium Copyright Act in general, rather than with respect to specific copyrighted works).

⁷⁶See 17 U.S.C.A. § 512(f); see generally *infra* § 4.12[9][D] (damages and attorneys' fees for misrepresentation in DMCA notices).

⁷⁷See *infra* § 4.12[9][F].

⁷⁸See, e.g., *Lenz v. Universal Music Corp.*, 815 F.3d 1145 (9th Cir. 2016); see generally *infra* § 4.12[9] (analyzing DMCA notifications and counter notifications).

Fair Use Index.⁷⁹

4.10[2] Case Study: Grappling with Technology
American Geophysical Union v. Texaco, Inc.

In a controversial decision, the Second Circuit held in 1994 in *American Geophysical Union v. Texaco, Inc.*,¹ that a scientist's practice of photocopying individual scientific articles that he kept in personal files in his office as a matter of convenience (to save the time it otherwise would have taken to retrieve the articles in journals maintained in Texaco's library) did not constitute fair use in view of the predominantly archival (rather than research-oriented) purpose of the copying, and because of the harm this practice caused to the publisher's market for licensing photocopying. The majority wrote that the scientist's copying "served, at most, to facilitate [his] research, which in turn might have led to the development of new products and technology that could have improved Texaco's commercial performance."²

The 1994 *Texaco* opinion could be explained in part because the economic consequences to plaintiffs in that case were more direct than in a typical case where a research scientist photocopies a few articles from a library for his own personal use. Although, by stipulation, the court ruled on the practices of only one Texaco scientist, who was selected at random, the *Texaco* suit actually was brought by a number of research publications which collectively offered a special license that would have allowed research facilities to make additional copies of articles from participating journals. Plaintiffs therefore arguably lost license fees that otherwise might have been earned.³

Read more broadly the *Texaco* opinion seemed to many to narrow the scope of the fair use defense. For this reason, in

⁷⁹See <https://www.copyright.gov/fair-use/fair-index.html>.

[Section 4.10[2]]

¹*American Geophysical Union v. Texaco Inc.*, 37 F.3d 881 (2d Cir. 1994). The opinion subsequently was modified in *American Geophysical Union v. Texaco Inc.*, 60 F.3d 913 (2d Cir.), *cert. dismissed*, 516 U.S. 1005 (1995).

²*American Geophysical Union v. Texaco Inc.*, 37 F.3d 881, 889 (2d Cir. 1994), *modified*, 60 F.3d 913 (2d Cir.), *cert. dismissed*, 516 U.S. 1005 (1995).

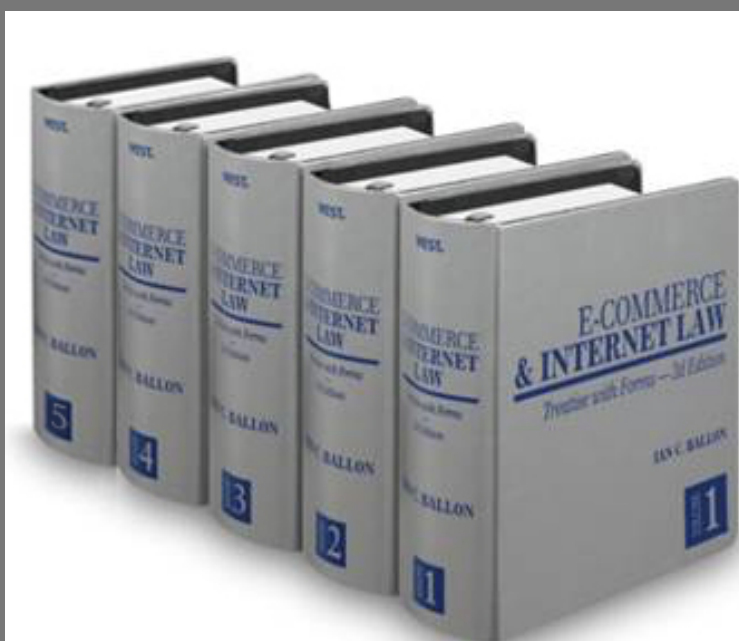
³See Ian C. Ballon, "Determining Fair Use in Cyberspace," L.A. Daily Journal, Sept. 6, 1995, at 7.

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2022

Ian C. Ballon

2022
UPDATES -
INCLUDING
NEW AND
IMPORTANT
FEATURES

THE PREEMINENT
INTERNET AND
MOBILE LAW
TREATISE FROM A
LEADING INTERNET
LITIGATOR — A
5 VOLUME-SET &
ON WESTLAW!



To order call **1-888-728-7677**
or visit **lanBallon.net**

Key Features of E-Commerce & Internet Law

- ◆ AI, ML, screen scraping and data portability
- ◆ Antitrust in the era of techlash
- ◆ The CPRA, Virginia, Colorado and Nevada privacy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- ◆ Software copyrightability and fair use after *Google v. Oracle*
- ◆ Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- ◆ TCPA law and litigation after *Facebook v. Duguid* - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- ◆ The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- ◆ Platform moderation and liability, safe harbors, and defenses (including the CDA and DMCA)
- ◆ Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- ◆ The law of SEO and SEM – and its impact on e-commerce vendors
- ◆ Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- ◆ IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi*, patentable subject matter, negative trade secrets, rights of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- ◆ Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- ◆ Sponsored links, embedded links, #hashtags, and internet, mobile and social media advertising
- ◆ Enforcing judgments against foreign domain name registrants
- ◆ Valuing domain name registrations from sales data
- ◆ Applying the First Sale Doctrine to virtual goods
- ◆ Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- ◆ Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- ◆ Click fraud
- ◆ Copyright and Lanham Act fair use
- ◆ Practical tips, checklists and forms that go beyond the typical legal treatise
- ◆ Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ AI/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- ◆ Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- ◆ Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- ◆ Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- ◆ Addresses both law and best practices
- ◆ Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- ◆ Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

Volume 1

Part I. Sources of Internet Law and Practice: A Framework for Developing New Law

- Chapter* 1. Context for Developing the Law of the Internet
2. A Framework for Developing New Law
3. [Reserved]

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Data Scraping, Database Protection, and the Use of Bots and Artificial Intelligence to Gather Content and Information
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names

Volume 2

- Chapter* 8. Internet Patents
9. Unique Intellectual Property Issues in Search Engine Marketing, Optimization and Related Indexing, Information Location Tools and Internet and Social Media Advertising Practices
10. Misappropriation of Trade Secrets in Cyberspace
11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property
12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace
13. Idea Submission, Protection and Misappropriation
- ### **Part III. Licenses and Contracts**
14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: The Federal eSign Statute, Uniform Electronic Transactions Act, UCITA, and the EU Distance Selling Directive
16. Internet Licenses: Rights Subject to License and Limitations Imposed on Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content Licensing Pre-Existing Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements

Volume 3

- Chapter* 24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements
- ### **Part IV. Privacy, Security and Internet Advertising**
25. Introduction to Consumer Protection in Cyberspace
26. Data Privacy
27. Cybersecurity: Information, Network and Data Security
28. Advertising in Cyberspace

Volume 4

- Chapter* 29. Email and Text Marketing, Spam and the Law of Unsolicited Commercial Email and Text Messaging
30. Online Gambling

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. State and Local Sales and Use Taxes on Internet and Mobile Transactions
34. Antitrust Restrictions on Technology Companies and Electronic Commerce
35. Dormant Commerce Clause and Other Federal Law Restrictions on State and Local Regulation of the Internet
36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

Part VI. Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption

37. Defamation, Torts and the Good Samaritan Exemption (47 U.S.C.A. § 230)
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression in Cyberspace

Part VII. Obscenity, Pornography, Adult Entertainment and the Protection of Children

40. Child Pornography and Obscenity
41. Laws Regulating Non-Obscene Adult Content Directed at Children
42. U.S. Jurisdiction, Venue and Procedure in Obscenity and Other Internet Crime Cases

Part VIII. Theft of Digital Information and Related Internet Crimes

43. Detecting and Retrieving Stolen Corporate Data
44. Criminal and Related Civil Remedies for Software and Digital Information Theft
45. Crimes Directed at Computer Networks and Users: Viruses and Malicious Code, Service Disabling Attacks and Threats Transmitted by Email

Volume 5

- Chapter* 46. Identity Theft
47. Civil Remedies for Unlawful Seizures
- ### **Part IX. Liability of Internet Sites and Service (Including Social Networks and Blogs)**
48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Content Moderation and Platform Liability: Service Provider and Website, Mobile App, Network and Cloud Provider Exposure for User Generated Content and Misconduct
50. Cloud, Mobile and Internet Service Provider Compliance with Subpoenas and Court Orders
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites
- ### **Part X. Civil Jurisdiction and Litigation**
52. General Overview of Cyberspace Jurisdiction
53. Personal Jurisdiction in Cyberspace
54. Venue and the Doctrine of Forum Non Conveniens
55. Choice of Law in Cyberspace
56. Internet ADR
57. Internet Litigation Strategy and Practice
58. Electronic Business and Social Network Communications in the Workplace, in Litigation and in Corporate and Employer Policies
59. Use of Email in Attorney-Client Communications

“Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet.”

Jay Monahan

General Counsel, ResearchGate

ABOUT THE AUTHOR

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator in the firm's Silicon Valley Los Angeles and Washington, DC offices. He defends data privacy, cybersecurity breach, AdTech, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database, AI and other intellectual property cases, including disputes involving safe harbors and exemptions, platform liability and fair use.



Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top Intellectual Property litigators in every year the list has been published (2009-2021), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was selected as the Lawyer of the Year for information technology law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. He also serves as Executive Director of Stanford University Law School's Center for the Digital Economy.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

Mr. Ballon is also the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.IanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@IanBallon).

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2022

- > **Antitrust in the era of techlash** (chapter 34)
- > **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- > **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- > **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurity breach, data privacy, AdTech and TCPA class action suits.**
- > **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- > **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- > **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- > **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States*, 141 S. Ct. 1648 (2021)** (ch5)
- > **FOSTA-SESTA and ways to maximize CDA protection** (ch 37)
- > **IP aspects of the use of #hashtags in social media** (ch 6)
- > **The CLOUD Act** (chapter 50)
- > **Virginia, Colorado and Nevada privacy laws** (ch 26)
- > **Applying the single publication rule to websites, links and uses on social media** (chapter 37)
- > **Digital economy litigation strategies**
- > **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- > **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- > **Website and mobile accessibility under the ADA and state laws** (chapter 48)
- > **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- > **Updated Defend Trade Secrets Act and UTSA case law** (chapter 10)
- > **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- > **AdTech law** (chapter 28, Darren Abernethy)
- > **The risks of being bound by the CASE Act's ostensibly voluntary jurisdiction over small copyright cases**
- > **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- > **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- > **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- > **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 26)
- > **Patent law** (updated by Josh Raskin) (chapter 8)
- > **Idea protection & misappropriation** (ch 13)
- > **Revisiting links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- > **eSIGN case law** (chapter 15)

**SAVE 20% NOW!! To order call 1-888-728-7677
or visit IanBallon.net
enter promo code **WPD20** at checkout**

List Price: \$3,337.00
Discounted Price: \$2,669.60

DMCA SAFE HARBORS: AN ANALYSIS OF THE STATUTE AND CASE LAW

Excerpted from the forthcoming 2022 updates to Chapter 4 (Copyright Protection in Cyberspace)
E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition
A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

(These excerpts are unrevised page proofs for the current update and may contain errors. Please email the author at ballon@gtlaw.com for a complimentary copy of the final published version.)

IP LAW YEAR IN REVIEW

4TH ANNUAL HBCU TECH LAW SUMMIT AND 19TH ANNUAL IP AND SOCIAL JUSTICE CLE SEMINAR

INSTITUTE FOR INTELLECTUAL PROPERTY AND SOCIAL JUSTICE
HOWARD UNIVERSITY SCHOOL OF LAW
MARCH 3-4, 2022

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles: 1840 Century Park East, Ste. 1900 Los Angeles, CA 90067 Direct Dial: (310) 586-6575 Direct Fax: (310) 586-0575	Silicon Valley: 1900 University Avenue, 5th Fl. East Palo Alto, CA 914303 Direct Dial: (650) 289-7881 Direct Fax: (650) 462-7881	Washington, D.C.: 2101 L Street, N.W., Ste. 1000 Washington, D.C. 20037 Direct Dial: (202) 331-3138 Fax: (202) 331-3101
--	---	--

Ballon@gtlaw.com
<www.ianballon.net>
LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
(Thomson West 2022 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (888) 728-7677
www.ianballon.net



Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal
Circuits

U.S. Supreme Court

JD, LLM, CIPP/US

Ballon@gtlaw.com

LinkedIn, Twitter, Facebook: IanBallon

Los Angeles

1840 Century Park East
Suite 1900

Los Angeles, CA 90067

T 310.586.6575

F 310.586.0575

Silicon Valley

1900 University Avenue
5th Floor

East Palo Alto, CA 94303

T 650.289.7881

F 650.462.7881

Washington, D.C.

2101 L Street, N.W.

Suite 1000

Washington, DC 20037

T 202.331.3138

F 202.331.3101

Ian C. Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and TCPA class action suits.

Ian is also the author of the leading treatise on internet and mobile law, [E-Commerce and Internet Law: Treatise with Forms 2d edition](#), the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of intellectual property law issues. In addition, he serves as [Executive Director of Stanford University Law School's Center for the Digital Economy](#). He also chairs [PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation](#) conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian was named the Lawyer of the Year for Information Technology Law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of Best Lawyers in America (including lawyer of the year for 2022). In 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder's* 2017 Litigation Departments of the Year Awards. He was also recognized as the 2012 [New Media Lawyer of the Year](#) by the Century City Bar Association. In 2010, he was the recipient of the California State Bar Intellectual Property Law section's [Vanguard Award for significant contributions to the development of intellectual property law](#). Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2021), and has been listed as a Northern California Super Lawyer every year from 2004 through 2021 and as one of the top 100 lawyers in California. He is also listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology.

Ian holds JD and LLM degrees and the [CIPP/US certification from the International Association of Privacy Professionals](#) (IAPP).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 1



THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

- 4.11[9][E] *Playboy Enterprises, Inc. v. Webworld, Inc.*
- 4.11[9][F] *A&M Records, Inc. v. Napster, Inc.*
 - 4.11[9][F][i] Overview
 - 4.11[9][F][ii] Contributory Infringement
 - 4.11[9][F][iii] Vicarious Liability
 - 4.11[9][F][iv] The District Court's Original Injunction Order
 - 4.11[9][F][v] Judge Patel's Order on Remand and the Second Ninth Circuit Appeal
 - 4.11[9][F][vi] Broader Implications
- 4.11[10] Case Study: Software Publishers Association's ISP Code of Conduct
 - 4.11[10][A] Overview
 - 4.11[10][B] ISP Code of Conduct
 - 4.11[10][C] SPA Demand Letters
 - 4.11[10][D] Related Litigation
- 4.12 Third-Party Liability Limitations Available to Service Providers Under the Digital Millennium Copyright Act**
 - 4.12[1] In General**
 - 4.12[2] Definition of a Service Provider**
 - 4.12[3] Threshold Prerequisites**
 - 4.12[3][A] In General**
 - 4.12[3][B] Adoption, Reasonable Implementation and Notice of the Policy**
 - 4.12[3][B][i] Adoption, Reasonable Implementation and Notice of the Policy—In General**
 - 4.12[3][B][ii] Operational Considerations and the Obligation to Inform Subscribers and Account Holders**

- 4.12[3][B][iii] Adopting a Policy and Defining “Repeat Infringer”
- 4.12[3][B][iv] Reasonable Implementation of A Service’s Repeat Infringer Policy
- 4.12[3][C] Standard Technical Measures
- 4.12[4] Transitory Digital Network Communications
- 4.12[5] System Caching
 - 4.12[5][A] System Caching—In General
 - 4.12[5][B] Transmission from a “Person Other than the Service Provider” Through the Service Provider’s System or Network to A “Person Other than” that Person
 - 4.12[5][C] Intermediate and Temporary Storage
- 4.12[6] Information Residing on Systems or Networks at the Direction of Users (User Storage)
 - 4.12[6][A] In General
 - 4.12[6][B] Designation of an Agent and the Obligation to Disable Access to or Remove Material in Response to Substantially Complying Notifications
 - 4.12[6][C] Knowledge, Awareness or Corrective Measures
 - 4.12[6][D] Direct Financial Benefit/Right and Ability to Control
- 4.12[7] Information Location Tools
- 4.12[8] Exemption from Liability to Subscribers for Removing or Disabling Access to Material Believed to be Infringing
- 4.12[9] Agent Designation, Notification, Counter Notification and Sanctions

**Under the System Caching, User
Storage and Information Location
Tools Limitations**

- 4.12[9][A] Designation of an Agent**
- 4.12[9][B] Notifications (and Service
Provider Obligations in
Response to Notifications)**
- 4.12[9][C] Counter Notification**
- 4.12[9][D] Section 512(f) Liability,
Injunctive Relief and Sanctions
for Misrepresentations in
Notifications and Counter
Notifications**
- 4.12[9][E] Subpoenas to Identify
Infringers**
- 4.12[9][F] Suits Against Copyright Owners
Over DMCA Notifications Based
on Theories Other Than Section
512(f)**
 - 4.12[9][F][i] In General**
 - 4.12[9][F][ii] Suits By Users Who Are
Accused Infringers**
 - 4.12[9][F][iii] Suits by Service
Providers**
- 4.12[10] Liability Limitation for Nonprofit
Education Institutions**
- 4.12[11] Injunctive Relief**
- 4.12[12] Extra-Judicial Remedies Available to
Copyright Owners**
- 4.12[13] Compliance Burdens Imposed on
ISPs**
- 4.12[14] Liability of NSPs and Downstream
Service Providers Under the Digital
Millennium Copyright Act**
- 4.12[15] Checklist of Service Provider
Compliance Issues**
- 4.12[16] Copyright Owners' Compliance
Checklist**
- 4.12[17] User Generated Content Principles**
 - 4.12[17][A] In General**

- 4.12[17][B] UGC Principles**
 - 4.12[18] Discovery Issues and Spoliation of Evidence in DMCA Litigation**
 - 4.12[19] The DMCA's Applicability to State Statutory and Common Law Copyright Claims**
 - 4.13 Equitable Remedies and Defenses in Civil Litigation**
 - 4.13[1] Injunctive Relief and Equitable Defenses (including waiver, estoppel, laches and unclean hands)**
 - 4.13[2] Seizure and Destruction**
 - 4.13[3] Security for Preliminary Equitable Relief**
 - 4.13[4] Asset-Freeze Injunctions**
 - 4.14 Copyright Damages in Internet and Software Infringement Litigation**
 - 4.14[1] Overview**
 - 4.14[2] Statutory Damages**
 - 4.14[2][A] In General**
 - 4.14[2][A][i] Overview**
 - 4.14[2][A][ii] Willful Infringement**
 - 4.14[2][A][iii] Innocent Infringement**
 - 4.14[2][A][iv] Fair Use, Nonprofit Educational Institutions and Public Broadcasting Entities**
 - 4.14[2][A][v] Infringement That is Neither Willful Nor Innocent**
 - 4.14[2][A][vi] Assessing Damages**
 - 4.14[2][A][vii] Providing Materially False Contact Information for a Domain Name Used in Connection with the Infringement**
 - 4.14[2][B] Multiple Awards and What Constitutes a "Work" in Software and Internet Cases**

leged that “[f]rom Community Connexion’s Internet site, persons are able to go to these other sites and retrieve the unauthorized copies of plaintiff’s software products.”² Plaintiffs further alleged that by allowing

the links to pirated copies of plaintiff’s software products to remain at the Community Connexion sites, where they are readily accessible, defendants implicitly authorize persons who access the Community Connexion sites to go to the linked sites and download copies of the plaintiff’s computer programs and reproduce them on their own computers.³

In addition to alleging that the ISP was liable for contributory copyright infringement, the complaint alleged that its owner was vicariously liable because he “participates in and has the right and ability to control the infringements of plaintiff’s copyrights, and derives financial benefit from the infringements of plaintiff’s copyrights.”⁴

Similar suits based on distribution of cracker tools, serial numbers and links were brought in the Central District of California and the District of Massachusetts.⁵

4.12 Third-Party Liability Limitations Available to Service Providers Under the Digital Millennium Copyright Act¹

4.12[1] In General

The Online Copyright Infringement Liability Limitation

²*Adobe Systems, Inc. v. Community Connexion, Inc.*, Case No. C-96-20833 SW EAI, Plaintiff’s Complaint § 30.

³*Adobe Systems, Inc. v. Community Connexion, Inc.*, Case No. C-96-20833 SW EAI, Plaintiff’s Complaint § 33.

⁴*Adobe Systems, Inc. v. Community Connexion, Inc.*, Case No. C-96-20833 SW EAI, Plaintiff’s Complaint § 38.

⁵*See Adobe Systems, Inc., v. Geocities, Inc.*, Case No. 96-7035 TJH (ANx), (C.D. Cal. filed Oct. 7, 1996) (suit by Adobe Systems, Inc., Claris Corp. and Traveling Software, Inc., against Geocities, Inc., and its president, David Bohnett, for, respectively, contributory copyright infringement and vicarious copyright infringement); *Adobe Systems, Inc. v. Tripod, Inc.*, Case No. 96-30189-MAP (D. Mass. Complaint filed Oct. 8, 1996) (suit by Adobe Systems, Inc., Claris Corp. and Traveling Software, Inc., against Tripod, Inc., and its president, Bo Peabody).

[Section 4.12]

¹Portions of this section were adapted in part from Ian C. Ballon & Keith M. Kupferschmid, “Third-Party Liability Under the Digital Millennium Copyright Act: New Liability Limitations and More Litigation for ISPs,” *The Cyberspace Law*, Nov. 1998, at 3.

Act incorporated as Title II of the Digital Millennium Copyright Act (DMCA), which is codified at 17 U.S.C. § 512 and took effect on the day it was signed into law on Oct. 28, 1998, potentially provides an affirmative defense¹ to claims

[Section 4.12[1]]

¹The DMCA provides an affirmative defense that potentially may be deemed to have been waived if not asserted in a party's answer to a complaint for copyright infringement. See *Society of Holy Transfiguration Monastery, Inc. v. Gregory*, 689 F.3d 29, 58–59 (1st Cir. 2012) (holding that the defendant waived its right to argue that it was insulated from liability by the DMCA by not pleading the affirmative defense in its answer to plaintiff's complaint).

Entitlement to, or compliance with, DMCA safe harbors also potentially may be the subject of an affirmative claim for declaratory relief. See, e.g., *Capitol Records, Inc. v. MP3tunes, LLC*, 611 F. Supp. 2d 342, 348 (S.D.N.Y. 2009) (denying plaintiffs' motion to dismiss a counterclaim for a declaratory judgment that the defendant complied with the DMCA and that notices sent by plaintiffs were deficient). A declaratory judgment, however, generally would have to be premised on compliance with particular copyrighted works, rather than in general. See, e.g., *Windstream Services, LLC v. BMG Rights Management (US) LLC*, 16 Civ. 5015 (KMW) (RLE), 2017 WL 1386357 (S.D.N.Y. Apr. 17, 2017) (dismissing Windstream's suit for a declaratory judgment that Windstream was entitled to the safe harbors created by sections 512(a) and 512(c), for lack of subject matter jurisdiction; "rather than seeking defined declarations of noninfringement regarding existing or foreseeable disputes about specific copyrights and instances of infringement, Windstream seeks broad declarations about every possible conflict that has occurred or could occur in the future. And Windstream seeks to obtain these declarations despite pleading that there is 'no direct evidence that any Windstream subscriber engaged in direct copyright infringement.'"), *appeal dismissed*, Docket No. 17–1515, 2017 WL 5329346 (2d Cir. Sept. 25, 2017); *Veoh Networks, Inc. v. UMG Recordings, Inc.*, 522 F. Supp. 2d 1265 (S.D. Cal. 2007) (dismissing a declaratory relief action brought by Veoh seeking a declaration that its user generated content site complied with the DMCA, shortly before Veoh was sued by UMG for copyright infringement in the Central District of California). Suits seeking a declaration of rights will be more difficult to maintain where the copyright owner denies that it intended to sue the declaratory judgment plaintiff for copyright infringement. See, e.g., *Brave New Films 501(C)(4) v. Weiner*, 91 U.S.P.Q.2d 1262, 2009 WL 1622385 (N.D. Cal. June 10, 2009).

While a service provider sued for copyright infringement bears the burden of proving its entitlement to the DMCA, the burden of notifying service providers of infringement under the DMCA is on copyright owners or their agents and cannot be shifted to the service provider to disprove. *Viacom Int'l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 113–15 (S.D.N.Y. 2013). Further, where a service provider meets its initial burden of proving entitlement to the DMCA safe harbor, the burden shifts to the copyright owner to prove that the service provider is not entitled to safe harbor

for damages and attorneys' fees for federal (and state common law or state statutory²) copyright infringement asserted against ISPs, website owners, search engine services, cloud service providers, blogs, portals, storage lockers, social networks, UGC sites, email providers, e-commerce sites, corporate intranets and all other entities that qualify as *service providers* as defined under the terms of the Act,³ but only if—and to the extent—eligible parties comply with multiple, specific technical eligibility requirements. Concurrently, Title II of the DMCA effectively provides copyright owners (or their exclusive licensees) with potentially valuable extra-judicial remedies to have infringing material blocked or removed and infringing activity stopped without having to file suit in most cases. Separate provisions of the DMCA providing remedies for circumvention of copy protection and access control mechanisms and removal, alteration or falsification of Copyright Management Information are addressed in section 4.21.

The DMCA has been described as “Congress’s foray into mediating the competing interests in protecting intellectual property interests and in encouraging creative development of devices for using the Internet to make information available.”⁴ Pursuant to the DMCA, a service provider that satisfies four threshold prerequisites⁵ may be entitled to liability limitations for copyright infringement based on (1) transmitting, routing, and providing connections to infringing material (the “routing” limitation, or what the statute refers to as “transitory digital network communications”),⁶ (2) system caching;⁷ (3) information stored at the direction of

protection based on knowledge or red flag awareness (if the service provider allegedly failed to remove infringing files in the face of knowledge or awareness). If that subsequent burden is not met by the copyright owner, the service provider is deemed subject to the safe harbor. See *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-95 (2d Cir. 2016).

²See *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 87-93 (2d Cir. 2016); see generally *infra* § 4.12[19].

³See generally *infra* § 4.12[2] (analyzing what constitutes a *service provider* under the DMCA).

⁴*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1024 (9th Cir. 2013).

⁵See *infra* § 4.12[3].

⁶See *infra* § 4.12[4].

⁷See *infra* § 4.12[5].

a user (the “user storage” limitation);⁸ or (4) linking or referring users to infringing material (the “information location tools” limitation);⁹ or to a broad exemption under any legal theory for (5) disabling access to or removing in good faith allegedly infringing material;¹⁰ but only if additional requirements specific to each of the five separate categories also are met. Service providers that qualify for any of the first four copyright infringement limitations also may be insulated from injunctive relief, except in limited circumstances. Special rules potentially further limit the liability of non-profit educational institutions NEIs for acts of infringement by faculty members or graduate students that otherwise might make the NEI ineligible for the four copyright liability limitations created by the Act.¹¹

Except for the broad exemption for removing or disabling access to material believed to be infringing (which in any event would not be premised on copyright law), section 512 merely limits a service provider’s potential exposure for damages and attorneys’ fees for copyright infringement, without creating an exemption from liability for the underlying conduct. Thus, even where a service provider’s liability is limited pursuant to one of the safe harbors, other parties may be held liable for direct, contributory or vicarious infringement or for inducement (based on the standards analyzed in section 4.11) for the same underlying act of infringement.

The first two limitations (routing and system caching) limit the risk of inadvertent liability that theoretically could arise for a service provider simply by virtue of the way the Internet operates. As discussed earlier in this chapter in section 4.03, under *MAI Systems Corp. v. Peak Computer, Inc.*¹² and subsequent cases, a copy for purposes of the Copyright Act may be created any time a “temporary copy” is made in a computer’s random access memory, or RAM. Infringing copies therefore potentially may be created whenever a temporary copy is automatically made as information is routed over various computers connected to the Internet

⁸See *infra* § 4.12[6].

⁹See *infra* § 4.12[7].

¹⁰See *infra* § 4.12[8].

¹¹See *infra* § 4.12[10].

¹²*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994).

or when a copy is temporarily cached.¹³ Even absent DMCA protection, however, the risk of liability for service providers for routing or system caching generally is very low.¹⁴

¹³See *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1378 n.25 (N.D. Cal. 1995) (*dicta*); see generally *supra* §§ 1.04, 4.03. But see *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008) (holding that a temporary copy is not actionable if it is fixed for merely a transitory duration), *cert. denied*, 557 U.S. 946 (2009); *supra* § 4.03[3].

¹⁴It is unlikely that material in transit would be deemed fixed for a sufficient duration to be actionable in the Second Circuit under *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008), *cert. denied*, 557 U.S. 946 (2009). Yet, even if it were—or in a court outside the Second Circuit applying *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 516 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994), pursuant to which information in transit likely would be deemed to create fixed copies—the risk of exposure for most service providers for routing in particular, but also for most types of system caching, generally should be small. The particular pathway traveled by a given message is somewhat random. Pursuant to TCP/IP protocols, information is broken into packets which may travel along separate routes before being reassembled at their ultimate destination. Moreover, the Internet dynamically reroutes traffic through the most efficient pathways available at a given time. Caching, like routing, is premised on considerations of efficiency and is undertaken without regard to the nature of the content temporarily copied. Even where an infringing copy is routed through a particular server as a result of a peering agreement—making the particular route traveled arguably less random—it may be difficult for a plaintiff to show causation; that a service provider’s mere act of providing access to the Internet constituted the type of volitional conduct or direct action typically required by courts as a prerequisite for imposing direct copyright liability on an ISP. See *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1370 (N.D. Cal. 1995) (Usenet postings; in order to find direct liability, “there should still be some element of volition or causation which is lacking where a defendant’s system is merely used to create a copy by a third party.”); see also, e.g., *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 131 (2d Cir. 2008) (holding that a cable service provider could not be held directly liable for its provision of a DVR service because “the operator . . . , the person who actually presses the button to make the recording, supplies the necessary element of volition, not the person who manufactures, maintains, or, if distinct from the operator, owns the machine.”), *cert. denied*, 557 U.S. 946 (2009); *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544 (4th Cir. 2004) (holding an ISP not liable for direct infringement where it was “simply the owner and manager of a system used by others who [we]re violating [plaintiffs] copyrights and [wa]s not an actual duplicator itself.”); *BWP Media USA, Inc. v. T&S Software Associates, Inc.*, 852 F.3d 436, 438-44 (5th Cir.) (affirming summary judgment for T & S Software Associates, an internet service provider, holding that it was not directly liable for hosting an internet forum on which third-party users posted images that allegedly

The Act also allows service providers to limit their liability for information location tools, including links. Absent DMCA protection, search engines and others potentially could be held liable under limited circumstances for links that they themselves provide. Service providers also could have exposure for links created by users on sites or services they host. A link generally does not involve the creation of a *copy*

infringed copyrights owned by plaintiffs), *cert. denied*, 138 S. Ct. 236 (2017); *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 666–67 (9th Cir. 2017) (affirming dismissal and summary judgment for defendants on plaintiff's direct infringement claims brought against ISPs that provided access to the USENET and a software program to be able to view USENET content, which, among many other things, plaintiffs claimed included infringing copies of its photos); *Fox Broadcasting Co. v. Dish Network LLC*, 747 F.3d 1060, 1066–68 (9th Cir. 2014) (following *Cartoon Network* in holding that a cable company that provided technology to its subscribers that they could use to make copies was not likely to be held directly liable because Dish itself did not make the copies; direct liability requires a showing of “copying by the defendant”); *Parker v. Google, Inc.*, 422 F. Supp. 2d 492, 497 (E.D. Pa. 2006) (“Google’s automatic archiving of USENET postings and excerpting of websites in its results to users’ search queries do not include the necessary volitional element to constitute direct copyright infringement.”), *aff’d*, 242 F. App’x 833 (3d Cir. 2007), *cert. denied*, 552 U.S. 1156 (2008); *Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923, 932 (N.D. Cal. 1996) (no evidence that BBS operator caused infringing copies to be made merely by operating a BBS where third parties posted infringing software); *Marobie-FL, Inc. v. National Ass’n of Fire Equipment Distributors*, 983 F. Supp. 1167 (N.D. Ill. 1997) (company which hosted a website on which infringing material was posted held not liable for direct infringement because, even though it “provide[d] a service somewhat broader than the . . . Internet access provider in *Religious* . . . [it] only provided the means to copy, distribute or display plaintiff’s works, much like the owner of a public copy machine used by a third party to copy protected material.”); *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503, 513 (N.D. Ohio 1997) (some element of direct action is required); *see generally supra* § 4.11[2]. Moreover, a strong argument could be made that routing and system caching amounts to fair use “intermediate” copying. *See supra* § 4.10[1]. As a practical matter, because no circuit court had applied the volitional conduct requirement articulated by Judge Whyte in the *Netcom* case by 1998 when the DMCA was enacted, some service providers were concerned that the issue of their potential liability for routing or caching was unclear.

Since the DMCA merely limits the liability of service providers for routing or system caching—without creating an exemption—a service provider’s act of routing or caching could serve as the underlying act of infringement on which a claim of contributory, vicarious or inducing infringement could be asserted against other parties (such as the people who initiated or received the communication) whose liability would not necessarily be limited by the Act—at least outside of the Second Circuit to the extent courts follow *MAI* but not *Cartoon Network*.

under the Copyright Act and therefore exposure for linking usually is premised on theories of secondary liability.¹⁵ Li-

¹⁵A link is merely an instruction to a browser to go from one location to another and does not involve the reproduction or distribution of content. *See, e.g., Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1156, 1162 (9th Cir. 2007) (applying the server test in holding that Google could not be held directly liable for violating the display or distribution rights of the plaintiff by creating links to photographs on third-party locations on the Internet because the content that was linked to was not located on Google's own servers; "Google simply provides HTML instructions directing a user's browser to access a third-party website. . . . [I]t is the website publisher's computer, rather than Google's computer, that stores and displays the infringing image."); *Microsoft Corp. v. Softicle.com*, Civil Action No. 16-2762, 2017 WL 5517379, at *2 (D.N.J. Sept. 29, 2017) (dismissing a claim for direct copyright infringement based on a link to infringing material; "Providing a link to a website containing infringing material does not, as a matter of law, constitute direct copyright infringement."); *Pearson Education, Inc. v. Ishayev*, 963 F. Supp. 2d 239, 251 (S.D.N.Y. 2013) (holding that the defendant was not liable for distributing infringing content by merely linking to it on a different site; "A hyperlink does not itself contain any substantive content; in that important sense, a hyperlink differs from a zip file. Because hyperlinks do not themselves contain the copyrighted or protected derivative works, forwarding them does not infringe on any of a copyright owner's five exclusive rights under § 106."); *MyPlayCity, Inc. v. Conduit Ltd.*, No. 10 Civ. 1615(CM), 2012 WL 1107648, at *12-14 (S.D.N.Y. Mar. 30, 2012) (granting summary judgment for the defendant on plaintiff's claim for direct copyright infringement for distribution of plaintiff's videogames by including a link on a toolbar it distributed following the termination of a license; "Because the actual transfer of a file between computers must occur, merely providing a 'link' to a site containing copyrighted material does not constitute direct infringement of a holder's distribution right."); *Batesville Services, Inc. v. Funeral Depot, Inc.*, 01 011-DFH-TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004) (hyperlinking "does not itself involve a violation of the Copyright Act (whatever it may do for other claims) since no copying is involved."); *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1202 n.12 (N.D. Cal. 2004) (finding hyperlinking does not involve copying).

Some district courts have held that a link may lead to direct liability for creating a public display or public performance in cases involving embedded or inline links or frames. *See Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *3-5 (S.D.N.Y. 2021) (denying defendant's motion to dismiss plaintiff's copyright infringement claim, holding that plaintiff stated a claim that Sinclair's placement of an embedded link to plaintiff's video of a starving polar bear (which plaintiff had uploaded to Instagram and Facebook), in an article describing how the video "went 'viral,'" constituted an unauthorized public display, and that Sinclair's fair use defense could not be resolved on a motion to dismiss); *Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585 (S.D.N.Y. 2018) (holding that that an image displayed via embedded links in various publications, from the Twitter feed where it had been posted, constituted a public display under the Copyright Act; granting partial

ability for linking has been most often imposed where link-

summary judgment to the plaintiff); *The Leader's Institute, LLC v. Jackson*, Civil Action No. 3:14-CV-3572-B, 2017 WL 5629514, at *10 (N.D. Tex. Nov. 22, 2017) (denying plaintiff's motion for summary judgment on defendant's counterclaim for copyright infringement, holding that plaintiff publicly displayed copyrighted content from defendant's website by framing it on its own website; distinguishing framing from ordinary linking); *Live Nation Motor Sports, Inc. v. Davis*, 81 U.S.P.Q.2d 1826, 2007 WL 79311 (N.D. Tex. Jan. 9, 2007) (holding that a link to a stream of a live webcast of motor races that were shown in real time created a public performance or display because those terms encompass "each step in the process by which a protected work wends its way to the audience").

Other courts, including two circuits courts, however, take a different view. *See, e.g., Flava Works, Inc. v. Gunter*, 689 F.3d 754, 761 (7th Cir. 2012) (holding that creating an in-line link to videos via frames from the defendant's website did not amount to a public performance); *see generally supra* § 4.03 (analyzing these cases and what constitutes a public performance); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1156, 1162 (9th Cir. 2007) (applying the server test in holding that Google could not be held directly liable for violating the public display rights of the plaintiff by creating links to photographs on third-party locations on the Internet because the content that was linked to was not located on Google's own servers; "Google simply provides HTML instructions directing a user's browser to access a third-party website. . . . [I]t is the website publisher's computer, rather than Google's computer, that stores and displays the infringing image."); *Hunley v. Instagram, LLC*, Case No. 21-cv-03778-CRB, 2021 WL 4243385 (N.D. Cal. Sept. 17, 2021) (dismissing plaintiff's claim against Instagram for secondary copyright infringement, which alleged that Instagram's embedding tool enabled third party websites to display copyrighted photos or videos posted to an Instagram account, because, under the server test, embedding a link does not publicly display a linked photograph or video, and therefore plaintiff could not plausibly allege an underlying act of direct infringement); *Flava Works, Inc. v. Gunter*, Case No. 17 C 1171, 2018 WL 620035, at *2, 4 (N.D. Ill. Jan. 30, 2018) (dismissing plaintiff's claim for direct infringement for offering a video bookmarking service because the defendant could not be held directly liable where it was the user, not the service, that clicked on a thumbnail link to access embedded content, and dismissing claims for secondary infringement because the plaintiff could not plausibly identify any myVidster users that in fact infringed one of plaintiff's works—to serve as an underlying act of direct infringement—merely by reference to DMCA notices reproducing alleged links); *see generally infra* §§ 9.03, 9.04 (analyzing links, in-line links, frames and embedded links in greater detail).

Direct liability was imposed in one case where the defendant did not merely link to infringing content, but also was responsible for the infringing content being at the linked locations and had started using links after being warned to stop displaying the photos on his own website. *See Batesville Services, Inc. v. Funeral Depot, Inc.*, No. 1:02-CV-01011-DFH-TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004) (holding that a triable issue of fact existed on the issue of defendant's potential direct or contributory liability for creating links to unauthorized photographs of

plaintiff's products, reproducing thumbnails of the photographs, and designing, creating and paying for the pages that it linked to, after having been warned to stop displaying the pictures itself on its own website.).

In *Free Speech Systems, LLC v. Menzel*, 390 F. Supp. 3d 1162, 1172 (N.D. Cal. 2019), the court—in denying the motion of the owner and operator of InfoWars to dismiss counterclaims brought against it—cited *Goldman v. Breitbart* and *The Leader's Institute v. Jackson* for the proposition that the server test might be inapplicable to a case where in-line links to defendant's copyrighted photographs were created by InfoWars, where the defendant could not cite to a case applying the server test in the Ninth Circuit “outside the search engine context.” This opinion, which involved only a cursory analysis of the issue, should be best understood in the context of a ruling on a motion to dismiss where InfoWars had sought unsuccessfully to have the court take judicial notice of an array of facts. Whether a work is displayed by creating a link to a third party website is not a function of whether the party creating the link is a search engine or a controversial political conspiracy news site. What constitutes a *display* is a matter of copyright law, not a function of a given business model.

Judge Breyer subsequently disagreed with Judge Orrick's *dicta* in *Menzel* that *Perfect 10* applied only in the context of search engines, writing that *Perfect 10* “addressed technology remarkably similar to the technology at issue” in a case involving embedded links. *Hunley v. Instagram, LLC*, Case No. 21-cv-03778-CRB, 2021 WL 4243385, at *2 n.1 (N.D. Cal. Sept. 17, 2021).

The Ninth Circuit also subsequently applied the server test to find a public display of a photograph on a server, where the image was not indexed on the site but could be accessed via a Google reverse image search or if someone had the exact URL, putting to rest the argument that the test was only applicable to search engines. *See Bell v. Wilmott Storage Services, LLC*, 12 F.4th 1065, 1072-74 (9th Cir. 2021) (“By displaying the Indianapolis photo on a server that was publicly accessible to anyone with an Internet connection . . . Wilmott publicly displayed the photo, *see* 17 U.S.C. § 106(5), regardless of whether or not any particular person actually found and viewed it.”).

In *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007), the in which Ninth Circuit adopted the server test to evaluate whether a given online use violates a copyright holder's display right, the appellate court considered linking and caching undertaken by Google and Amazon.com in connection with visual search engines that indexed the Internet. Google cached small thumbnail images on its servers and created links to full size copies of images located on third-party websites.

Under the server test, “a computer owner that stores an image as electronic information and serves that electronic information directly to the user . . . is displaying the electronic information in violation of a copyright holder's exclusive display right. Conversely, the owner of a computer that does not store and serve the electronic information to a user is not displaying that information, even if such owner in-line links to or frames the electronic information.” *Id.* at 1159.

Applying the server test, the court held that Google could not be held directly liable for creating links to third-party locations on the

ing occurs in connection with other misconduct that induces or materially contributes to the infringing activity of others.¹⁶

Internet because the content that was linked to was not located on Google's own servers. In the words of the court, "Google transmits or communicates only an address which directs a user's browser to the location where a copy of the full-size image is displayed. Google does not communicate a display of the work itself." *Id.* at 1161 n.7. Stated differently, "it is the website publisher's computer, rather than Google's computer, that stores and displays the infringing image." *Id.* at 1162.

With respect to thumbnail images stored on Google's own servers (which were displayed in its search results page to help users determine where responsive material was located), the court held that Google could be held directly liable for storing those images on its servers, under the server test. The court, however, found that Google's use, undertaken to index the Internet, was highly transformative and likely to be found a fair use. *See supra* § 4.10[1].

The court nevertheless remanded the case for further consideration of whether Google could be held contributorily liable for creating links to images stored on third-party servers (which created unauthorized copies on the computer screens of users) to determine if Google "had knowledge that infringing Perfect 10 images were available using its search engine, could take simple measures to prevent further damage to Perfect 10's copyrighted works, and failed to take such steps." *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1172 (9th Cir. 2007). *But see Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012) (vacating a preliminary injunction against a social bookmarking site based on the finding that creating links to infringing videos submitted by users was not sufficiently material to amount to contributory infringement; applying a different test for contributory infringement than the Ninth Circuit had in *Perfect 10*); *see generally infra* §§ 9.03[1], 9.04[1] (analyzing these cases and linking and framing generally in greater detail).

¹⁶*See, e.g., Microsoft Corp. v. Softicle.com*, Civil Action No. 16–2762, 2017 WL 5517379, at *3 (D.N.J. Sept. 29, 2017) (denying defendant's motion to dismiss plaintiff's claim for contributory copyright infringement, where the defendant provided a link to third party websites where infringing software could be obtained, where the plaintiff alleged third party infringement, defendant's knowledge of the infringement, and "Defendants' material contribution to the infringement by providing links to the website from which unauthorized copies were made."); *Arista Records, Inc. v. MP3Board, Inc.*, No. 00 CIV. 4660(SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002) (denying cross motions for summary judgment, holding that there were disputed material facts over whether the operator of a website that hosted only links to music files located on third party sites could be held liable for contributory and vicarious copyright infringement); *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp. 2d 1290 (D. Utah 1999) (holding the plaintiff likely to prevail on its claim for contributory copyright infringement and enjoining defendants from creating links to material that they had previously been ordered to remove from their own website). *But see Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012) (vacating a preliminary injunction against a social bookmarking

On the other hand, links generated in connection with indexing the Internet may be found to be a fair use.¹⁷ The liability limitation for information location tools nonetheless has been effective (and rarely challenged) because it allows copyright owners to obtain quick relief that might otherwise be difficult or impossible to obtain in court, and effectively saves service providers the time and expense of having to litigate where they are willing to simply disable a link in response to a notification.¹⁸

By contrast, sites and services that host or store user generated content or allow users to transmit it, potentially face a greater risk of third-party liability in the absence of the DMCA safe harbor.¹⁹ Perhaps not surprisingly, most of the litigation under the DMCA has involved the liability limitation for material stored at the direction of user.²⁰ For service providers with interactive sites or services where users may post, store or transmit their own material—which encompasses a wide array of services from traditional ISPs to social network operators and cloud service providers—the user storage limitation is potentially very important.

To limit its liability under any of the DMCA safe harbors, a service provider, as noted above, must meet specific thresh-

site based on the finding that creating links to infringing videos submitted by users was not sufficiently material to amount to contributory infringement); *Hunley v. Instagram, LLC*, Case No. 21-cv-03778-CRB, 2021 WL 4243385 (N.D. Cal. Sept. 17, 2021) (dismissing plaintiff's claim against Instagram for secondary copyright infringement, which alleged that Instagram's embedding tool enabled third party websites to display copyrighted photos or videos posted to an Instagram account, because, under the server test, embedding a link does not publicly display a linked photograph or video, and therefore plaintiff could not plausibly allege an underlying act of direct infringement); see generally *infra* §§ 4.12[7], 9.03 to 9.06.

¹⁷See, e.g., *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007); *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 820 (9th Cir. 2003); see generally *supra* § 4.10[1].

¹⁸The Digital Millennium Copyright Act does not limit liability for linking based on other theories of recovery, including the Lanham Act or state unfair competition laws (see *infra* chapter 6) or under federal securities or consumer protection laws. See *infra* §§ 25.04 (warranty information or disclaimers made available on a linked page), 28.12 (advertising), §§ 32.01, 32.04 (securities). Linking is analyzed under these and other theories of law (including copyright law) in chapter 9.

¹⁹See *supra* §§ 4.11[1] to 4.11[6].

²⁰See 17 U.S.C.A. § 512(c).

old requirements.²¹ It must adopt, reasonably implement and inform subscribers and account holders²² of a policy of terminating the accounts or subscriptions of repeat infringers, in appropriate circumstances, and accommodate and not interfere with “standard technical measures.”²³ If a service provider fails to meet these threshold requirements it will be ineligible for any of the safe harbors. Further, the DMCA only limits a service provider’s liability as of the date the service provider began complying with the statute.²⁴

For the user storage and information location tools²⁵ safe harbors (and in limited circumstances the caching²⁶ safe harbor), a service provider also must designate an agent to receive a special type of statutory demand letter called a *notification of claimed infringement* (referred to in this section of the treatise as a *notification*, or more colloquially as a *DMCA notice*) and expeditiously disable access to or remove material or activity (or links) identified as infringing in substantially complying notifications.²⁷ Failing to respond to a substantially complying notification may make a service

²¹See *infra* § 4.12[3].

²²Not every type of service will have subscribers or account holders.

²³See *infra* § 4.12[3].

²⁴See *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1092 (C.D. Cal. 2004) (holding that defendant Internet Key was ineligible for the DMCA liability limitations for acts of infringement that occurred prior to Aug. 21, 2002, when it first implemented and distributed to clients its policy of terminating repeat infringers), *aff’d in part on other grounds*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007); see also, e.g., *Oppenheimer v. Allvoices, Inc.*, No. C 14–00499 LB, 2014 WL 2604033, at *6 (N.D. Cal. June 10, 2014) (holding the DMCA inapplicable to conduct that pre-dated the defendant’s registration of its DMCA agent with the U.S. Copyright Office, in ruling on a motion to dismiss); *BWP Media USA Inc. v. Hollywood Fan Sites LLC*, 115 F. Supp. 397, 400-01 (S.D.N.Y. 2015) (citing *Oppenheimer* approvingly for the proposition that “[a] service provider cannot retroactively qualify for the safe harbor for infringements occurring before the proper designation of an agent under the statute” and holding that “§ 512(c) makes clear that it contemplates two parallel sources—the provider’s website and the USCO directory—where each service provider’s DMCA agent information is readily available to the public. For a service provider to fulfill only one of these two requirements is insufficient.”); *infra* § 4.12[9][A] (collecting cases on registration as the start time for DMCA protection and criticizing the rule).

²⁵See *infra* § 4.12[7] (analyzing whether a DMCA agent must be designated to qualify for the information location tools liability limitation).

²⁶See *infra* § 4.12[5].

²⁷See *infra* § 4.12[9].

provider ineligible for the safe harbor for the material identified in the notification.²⁸

To take advantage of the user storage safe harbor, a service provider further must disable access to or remove material, even in the absence of a DMCA notice, if it has actual knowledge of infringing activity or is “aware of facts or circumstances from which infringing activity is apparent . . . ,” which in the legislative history is explained as material that raises a “red flag.”²⁹ The DMCA was not intended to protect service providers that facilitate infringement or turn a blind eye to it. The liability limitations are “not presumptive, but granted only to ‘innocent’ service providers who can show that they do not have a defined level of knowledge.”³⁰

The Second and Ninth Circuits have held that actual knowledge denotes subjective belief, whereas red flag awareness is judged by an objective reasonableness standard.³¹

Both Circuits have also clarified that copyright owners, not service providers, have the obligation to investigate whether material on a site or service is infringing.³²

²⁸See, e.g., *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004) (finding a triable issue of fact on the question of whether AOL satisfied the requirements of section 512(i) and therefore was entitled to limit its liability under the DMCA in a case where it failed to receive a notification, and therefore took no action, due to its own error).

²⁹See *infra* § 4.12[6].

³⁰*In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634 (N.D. Ill. 2002), *aff’d on other grounds*, 334 F.3d 643 (7th Cir. 2003).

³¹See *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-98 (2d Cir. 2016); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1025 (9th Cir. 2013) (quoting *Viacom v. YouTube*); *infra* § 4.12[6].

³²See 17 U.S.C.A. § 512(m); *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 89 (2d Cir. 2016) (“the DMCA explicitly relieves service providers from having to affirmatively monitor their users for infringement”); *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 94, 98 (2d Cir. 2016) (“§ 512(m) makes clear that the service provider’s personnel are under no duty to ‘affirmatively seek[]’ indications of infringement.”); “§ 512(m) relieves the service provider of the obligation to monitor for infringements posted by users on its website.”; *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) (“Section 512(m) is explicit: DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider. For that reason, § 512(m) is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that infringement may be occurring.”); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 603

While a service provider has no obligation to take down material in response to a defective notification sent by a copyright owner, and knowledge or awareness may not be inferred from a notification that does not substantially comply with the requirements of section 512(c)(3),³³ the Ninth Circuit suggested in *dicta* that an unverified notice sent by a third party (as opposed to the copyright owner who filed suit against the service provider) potentially could provide red flag awareness.³⁴ A service provider also may be deemed to have knowledge or awareness where willful blindness³⁵ or evidence of inducement³⁶ is shown.

(9th Cir. 2018) (“The Digital Millennium Copyright Act places the burden of policing infringement on the copyright owner, not on the person or firm storing and hosting the material.”); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1022 (9th Cir. 2013) (holding that the burden of policing for infringement is on the copyright owner; “Copyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers like Veoh, who cannot readily ascertain what material is copyrighted and what is not.”); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir.) (“The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright.”), *cert. denied*, 522 U.S. 1062 (2007).

³³See 17 U.S.C.A. § 512(c)(3)(B)(i); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1020–21 n.12 (9th Cir. 2013).

³⁴See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1024–25 (9th Cir. 2013); *infra* § 4.12[6][A].

³⁵See, e.g., *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 92–94 (2d Cir. 2016) (reversing the district court’s order vacating a jury verdict of willful blindness and red flag awareness); *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 98–99 (2d Cir. 2016) (finding no willful blindness in that case); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) (holding that knowledge or awareness may be established by evidence of willful blindness, which the court characterized as a deliberate effort to avoid guilty knowledge); *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043 (9th Cir. 2013) (explaining that “inducing actions”—or measures deemed to induce copyright infringement—were relevant to the court’s determination that the defendant had red flag awareness); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1023 (9th Cir. 2013) (citing *Viacom v. YouTube* for the proposition that “a service provider cannot willfully bury its head in the sand to avoid obtaining . . . specific knowledge.”); see also *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) (holding that a service provider was not willfully blind to infringement); *infra* § 4.12[6][C].

³⁶See *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043 (9th Cir. 2013) (explaining that “inducing actions”—or measures deemed

Eligibility for the user storage liability limitation also requires showing that a defendant not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.³⁷ To lose safe harbor protection a service provider must have both a financial interest *and* right and ability to control the infringing activity.³⁸

The Second,³⁹ Fourth⁴⁰ and Ninth⁴¹ Circuits have held that the degree of control required to disqualify a service provider from eligibility for the DMCA safe harbor is higher than what would be required to prove right and ability to control to establish common law vicarious liability (which is analyzed in section 4.11[4]). In the Second and Ninth Circuits, what is required is “something more than merely the ability to remove or block access to materials posted on a service provider’s website.”⁴² That “something more” involves exerting “substantial influence” on the activities of users, which may include high levels of control over user activities or purposeful conduct.⁴³

The financial interest prong has been construed in the Ninth Circuit as requiring a showing that “the infringing activity constitutes a draw for subscribers, not just an added

to induce copyright infringement—were relevant to the court’s determination that the defendant had red flag awareness).

³⁷See *infra* § 4.12[6][D].

³⁸See *infra* § 4.12[6][D].

³⁹See *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37–38 (2d Cir. 2012).

⁴⁰See *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004).

⁴¹See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026–31 (9th Cir. 2013).

⁴²*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012), quoting *Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011); see also *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 603 (9th Cir. 2018); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013) (following the Second Circuit on this point).

⁴³See *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 603 (9th Cir. 2018); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013).

benefit.’”⁴⁴ Right and ability to control and financial interest are analyzed in section 4.12[6][D].

For purposes of the user storage limitation (and presumably for the information location tools safe harbor, to the extent applicable service providers have account holders and subscribers), the Ninth Circuit has held that in evaluating a service provider’s compliance with the threshold requirement that a service provider adopt, notify subscribers about and implement a policy of terminating “repeat infringers” in “appropriate circumstances,” a court must also consider the service provider’s compliance with third-party notifications and response to other instances where it had actual knowledge or red flag awareness of infringement (not merely how it acted in responding to the plaintiff’s own works), on the theory that a service provider may not be reasonably implementing a policy of terminating repeat infringers in appropriate circumstances if it is not, in the first instance, adequately keeping track of who is an infringer.⁴⁵ Thus, ignoring red flag material—or failing to disable access to or remove material when a service provider is aware of facts and circumstances from which infringing activity is apparent⁴⁶—could disqualify a service provider from safe harbor protection not only with respect to the red flag material that remained online but overall for any acts of user infringement (to the extent the failure to disable access to or remove

⁴⁴*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1044-45 (9th Cir. 2013) (finding a financial interest where the defendant earned advertising revenue from ads marketed based on the popularity of infringing material on his sites, where approximately 90-96 percent (or perhaps slightly less) of the content on his sites was infringing and where the defendant actively induced infringement by users of his sites); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117-18 (9th Cir.) (finding that evidence that the service provider hosted, for a fee, websites that contained infringing material inadequate to establish the requisite financial benefit based on the literal language of the legislative history), *cert. denied*, 522 U.S. 1062 (2007); *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004) (quoting legislative history) (holding that “financial interest” under the DMCA should be found where “there is a causal relationship between the infringing activity and any financial benefit a defendant reaps . . . ;” affirming the finding that there was no financial interest based on inadequate proof that “customers either subscribed because of the available infringing material or cancelled subscriptions because it was no longer available.”); *see generally infra* § 4.12[6][D].

⁴⁵*See Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1110-13 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007); *infra* § 4.12[3][B][iv].

⁴⁶17 U.S.C.A. § 512(c)(1)(A)(ii).

red flag material evidenced a failure to reasonably implement a repeat infringer policy, which is a threshold requirement for DMCA eligibility), at least in the Ninth Circuit. This ruling also potentially opens up a service provider to broad discovery (beyond the works at issue in a given case).⁴⁷

Whether and to what extent a service provider can lose safe harbor protection for its employees' failure to respond in the face of knowledge or awareness or for their own misconduct has been the focus of a number of disputes. The Second Circuit held in one case that the mere fact that an employee saw a video on his employer's site that included substantially all of a recording of recognizable copyrighted music (or posted a comment, added it to a channel or "liked" the video), was insufficient to sustain a copyright owner's burden of proving that the service provider had either actual knowledge or red flag awareness of the infringement because that fact alone did not account for whether the music was in fact recognized by the employee as infringing.⁴⁸ The Tenth Circuit has held that a service provider does not automatically lose DMCA protection for the infringing activity of employees where the employees were merely acting as users of the service.⁴⁹ The Ninth Circuit looks to agency law for both employees and unpaid moderators to determine actual or apparent authority, with the further wrinkle that beyond knowledge or red flag awareness potentially attributable to a service provider, the Ninth Circuit has suggested that material may not even qualify as "stored at the direction of a user" if it is reviewed prior to upload, leaving potentially a factual question in some cases whether the material was stored by the employee or moderator or at the direction of the user.⁵⁰ In other cases, whether employee knowledge or misconduct could be attributed to the service provider would likely turn on traditional principles of *respondeat superior*,⁵¹ and whether the employee's acts or omissions were undertaken within the scope of

⁴⁷See *infra* § 4.12[18] (discovery issues in DMCA litigation).

⁴⁸*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 96-97 (2d Cir. 2016).

⁴⁹*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1181 (10th Cir. 2016).

⁵⁰See *Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045 (9th Cir. 2017). This analysis is criticized elsewhere in section 4.12 because the focus of the statute is on material stored *at the direction* of a user, not on who mechanically effectuates the storage.

⁵¹In *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79

his or her employment.

With the user storage safe harbor, Congress “intended to balance the need for rapid response to potential infringement with the end-users['] legitimate interests in not having material removed without recourse.”⁵² The statute thus creates “strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital network environment.”⁵³

To benefit from the related exemption from liability for removing material stored by subscribers, service providers must also respond to counter notifications which may be directed to their agents by subscribers whose content was removed (or access disabled) in response to a notification.⁵⁴ When a substantially complying counter notification is received, a service provider must pay close attention to statutory time periods and either restore access to or re-post content that originally had been removed (if a copyright owner fails to timely respond to a counter notification), or

(2d Cir. 2016), the Second Circuit held that a reasonable jury could infer that a service provider consciously avoided knowing about specific repeat infringers using its service, which would amount to a failure to reasonably implement its repeat infringer policy, where company executives were encouraged to and did personally use a service to link to or download infringing music for their personal use. *See id.* at 90. Elsewhere in the opinion, the court held that a reasonable jury could infer that the company was liable for employee infringement under principles of respondeat superior, where, among other things, evidence was presented at trial that an executive wrote an email asserting that MP3tunes employees “would see[d] the [sideload.com] index with higher quality tracks,” an employee testified that she and other MP3tunes employees “specifically sought out websites on the Internet to locate files and sideload them into the Sideload index,” and that they all did so “as employees of MP3tunes,” and where the CEO directed that same employee to provide other MP3tunes employees a “list of some sites featuring free MP3s . . . for sideloading purposes.” *Id.* at 97. The panel elaborated that “[t]here was also ample evidence from which a juror could reasonably have inferred that these executive sideloads were performed from MP3tunes’s offices. And it was clearly in MP3tunes’s interest to increase the number of quality songs on sideload.com by using its employees to expand the index.” *Id.*

⁵²*Rossi v. Motion Picture Ass’n of America Inc.*, 391 F.3d 1000, 1003 (9th Cir. 2004) (quoting legislative history), *cert. denied*, 544 U.S. 1018 (2005).

⁵³*Rossi v. Motion Picture Ass’n of America Inc.*, 391 F.3d 1000, 1003 (9th Cir. 2004) (quoting legislative history), *cert. denied*, 544 U.S. 1018 (2005).

⁵⁴*See infra* § 4.12[13].

take no further action, and leave the material offline (if the copyright owner timely provides evidence to the service provider that it has filed suit against the subscriber or account holder).⁵⁵ Needless to say, liability to subscribers for taking down material in response to a DMCA notification already may be limited by the service provider's Terms of Use agreement, EULA or other service contract with its subscribers and account holders⁵⁶ and in some circumstances potentially by the Good Samaritan Exemption to the Telecommunications Act of 1996 (also known as the Communications Decency Act, or CDA).⁵⁷

Compliance with the DMCA is optional. If a service provider chooses not to comply or fails to meet the statute's technical requirements, its liability will be determined under existing provisions of copyright law, including the standards for third-party liability (premised on direct, contributory, vicarious or inducement liability), fair use, injunctive relief and damages outlined in, respectively, sections 4.11, 4.10, 4.13 and 4.14. The fact that a company chooses not to or fails to meet the requirements for any of the specific limitations created by the Act may not itself be cited as evidence of infringement.⁵⁸

Early on, some service providers were disinclined to comply with the DMCA based on concerns about the costs and burdens associated with compliance and the adverse impact that a notice and takedown system could have on Internet speech. The increased volume of complaints brought about through the designation of an agent, the time and manpower needed to evaluate whether notifications and counter notifications are substantially complying, and the obligation to adhere to multiple additional technical requirements (including strict time limitations) may impose significant costs on service providers that choose to comply with the Act (which may be especially challenging for new or smaller companies).

⁵⁵See *infra* § 4.12[9][C].

⁵⁶See *infra* chapters 21 (click through and other unilateral contracts), 22 (Terms of Use) and 23 (ISP contracts). Whether and to what extent service provider agreements will be deemed enforceable is analyzed in sections 21.03 and 21.04. DMCA compliance is separately addressed in section 22.05[2][A].

⁵⁷See 47 U.S.C.A. § 230(c); see generally *infra* §§ 4.12[8], 37.05.

⁵⁸17 U.S.C.A. § 512(l).

On the other hand, the costs associated with implementing a DMCA program may be small compared with the cost of litigating a copyright dispute (particularly one where the service provider may not be able to rely on the DMCA defense).

Today, compliance with the liability limitations of the DMCA is widely seen as almost essential for service providers to better insulate themselves from liability for the conduct of their users. DMCA compliance also is required by many insurers of interactive sites or services.⁵⁹

To reduce the costs and burdens of compliance, some service providers honor notifications, but not counter notifications. A service provider may seek to benefit from the user storage safe harbor—to limit liability to copyright owners—but choose not to comply with the procedures for counter notifications (as discussed in section 4.12[13]), which merely provides an exemption against liability to subscribers for disabling access to or removing material, based on a calculation that the risk of liability to subscribers for wrongfully removing material is likely to be limited and may be capped in the provider's contract with its customers. Failing to comply with procedures governing counter notification should not impact a service provider's entitlement to the safe harbors provided for transitory digital network communications, system caching, information stored at the direction of users or information location tools, because counter notification procedures merely provide a remedy for users accused of infringement. Offering users the opportunity to submit counter notifications, however, may help deflect user complaints about takedown notices and therefore may amount to a good business practice for some service providers. Complying with procedures for counter notifications also allows a site that is philosophically uncomfortable with disabling access to or removing material that potentially could be protected by the fair use doctrine or otherwise reflect a permitted use, to provide users with a mechanism to allow them to restore the material without exposing the service provider to liability.

If a service provider fails to comply with the technical requirements for one or more of the safe harbors set forth in sections 512(a), 512(b), 512(c) or 512(d) (as opposed to provi-

⁵⁹Whether and to what extent a given site should comply with the DMCA is separately considered in section 49.05 and chapter 50.

sions governing counter notification), the service provider could lose DMCA protection for a specific file, or overall for its entire service. The failure to take down material in response to a notification or based on knowledge or red flag awareness generally should only put at risk that material.⁶⁰ However, a service provider's failure to reasonably implement its repeat infringer policy,⁶¹ accommodate standard

⁶⁰See 17 U.S.C.A. § 512(c); *see generally infra* §§ 4.12[6][B], 4.12[6][C]. The Ninth Circuit raised but declined to decide the issue of whether the failure to remove material based on actual knowledge or red flag awareness would only implicate protection for that material or whether it could jeopardize a service provider's overall entitlement to safe harbor protection under section 512(c) for material stored at the direction of a user. *See Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1043 n.20 (9th Cir. 2013). Its holding in *Perfect 10, Inc. v. CCBill LLC*, 488 F.2d 1102, 1110-13 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007) that a service provider's compliance with third party notifications and response to other instances where it may have had red flag awareness should be considered in evaluating reasonable implementation of a repeat infringer program suggests that, in some cases, failing to remove red flag material could put at risk a company's entitlement to the DMCA safe harbor generally, and not just with respect to the material left online, at least in the Ninth Circuit, although no court has actually gone as far as *CCBill* suggests. In fact, the statute distinguishes between omissions applicable to specific content (such as knowledge or awareness) and threshold requirements for DMCA eligibility. *See, e.g., EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 94 n.9 (2d Cir. 2016) (noting that if, on remand, it was found that the defendant did not reasonably implement a repeat infringer policy it would be "ineligible for DMCA safe harbor protection at all . . .," making irrelevant questions such as red flag awareness or willful blindness). A service provider's failure to remove material in response to knowledge or awareness, however, if widespread, could support a finding that the service provider failed to properly implement its repeat infringer policy, which in turn could deprive the service provider of DMCA protection even for those files removed by the service provider in response to timely notice, actual knowledge or red flag awareness.

At the same time, although no court has yet considered this precise issue, even the failure to meet a threshold requirement potentially should not be disabling if the failure was not material. For example, failure to designate an agent in a filing with the Copyright Office due to mistake or inadvertence should not disqualify a service provider from protection where the agent and his or her contact information is posted on the service provider's website, in a lawsuit where the copyright owner was aware of this fact and was not prejudiced by the lack of technical compliance.

⁶¹See 17 U.S.C.A. § 512(i)(1)(A); *Atlantic Recording Corp. v. Spinrilla, LLC*, 506 F. Supp. 3d 1294, 1320 (N.D. Ga. 2020) (holding that Spinrilla could not invoke the DMCA safe harbor prior to the time it adopted a repeat infringer policy); *see generally infra* § 4.12[3][B].

technical measures,⁶² or designate an agent,⁶³ could result in a service provider losing DMCA protection under section 512(c) for all material on its site or service (even for material that was taken down or to which access was disabled)—at least during any time period when the service provider is not in compliance with these threshold requirements. While, as previously noted, losing DMCA protection will not automatically result in a finding of liability—the DMCA merely provides a defense to infringement, which a copyright owner otherwise must prove—it can be more expensive and complex for a service provider to defend claims based on user misconduct in cases where the DMCA does not apply.⁶⁴

For copyright owners, the Digital Millennium Copyright Act potentially provides valuable extra-judicial remedies. In lieu of spending tens of thousands of dollars or more to obtain injunctive relief, a copyright owner may be able to quickly and inexpensively have infringing content removed where a service provider complies with the DMCA. Even where a user challenges a notification by serving a counter notification—forcing the copyright owner to file suit if it wants to keep the material offline—any ensuing litigation would require the accused infringer to obtain injunctive relief to have the material placed back online (rather than compelling the copyright owner to obtain an injunction to have the material removed, as is usually the case in copyright in-

⁶²See 17 U.S.C.A. § 512(i)(1)(B); *see generally infra* § 4.12[3][C]. As noted in section 4.12[3][C], there likely are no standard technical measures in effect today.

⁶³See 17 U.S.C.A. § 512(c)(2); *see generally infra* § 4.12[9].

⁶⁴See, e.g., *BMG Rights Management (US) LLC v. Cox Communications, Inc.*, 881 F.3d 294, 303-05 (4th Cir. 2018) (affirming the lower court's holding that a service provider was ineligible for DMCA safe harbor protection where it failed to reasonably implement its repeat infringer policy, in a case that subsequently resulted in a \$25 million jury verdict for the copyright owner, which was reversed on appeal and remanded based on a faulty jury instruction); *BMG Rights Management (US) LLC v. Cox Communications, Inc.*, No. 1:14-cv-1611(LO/JFA), 2015 WL 9999710 (E.D. Va. Jury Verdict Form Dec. 17, 2015) (awarding plaintiff \$25,000,000). The case ultimately settled.

In a subsequent suit, a jury awarded \$99,830.29 for each work infringed (for a total of \$1 Billion). *See Sony Music Entertainment v. Cox Communications, Inc.*, 464 F. Supp. 3d 795 (E.D. Va. 2020); *see also Sony Music Entertainment v. Cox Communications, Inc.*, Civil Action No. 1:18-cv-00950, 2021 WL 1254683 (E.D. Va. Jan. 12, 2021) (affirming the jury award, in response to post-trial motions, holding that Cox's failure to present evidence of its own calculation to the jury at trial is determinative).

fringement litigation).⁶⁵ If the accused infringer does not seek injunctive relief, the material will automatically remain offline unless and until the court orders otherwise.

The compliance requirements imposed by the DMCA have ensured that, at least as of November 1, 2018, no pirate site has ever been found entitled to the DMCA safe harbor. Peer-to-peer networks and pirate sites that promote infringement operate outside the protection of the safe harbor because these sites and services typically have knowledge or awareness of infringing files based on willful blindness, inducement or at the very least red flag awareness of facts and circumstances from which infringing activity is apparent (and consequently fail to reasonably implement repeat infringer policies), because, by inducing infringement, they have the right and ability to control infringement and a financial interest in it, or, for peer-to-peer networks, because the operators do not qualify as service providers under the statute based on the technology on which they operate.⁶⁶ In short, courts apply section 512 in a way that sites and services

⁶⁵See *infra* § 4.12[9][C] (counter notifications), 4.13[1] (injunctive relief in copyright infringement suits).

⁶⁶See, e.g., *Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1039-47 (9th Cir. 2013) (holding that various providers of BitTorrent trackers that used a hybrid peer-to-peer file sharing protocol were ineligible for the DMCA's safe harbors because, among other things: (i) BitTorrent trackers are not "service providers" for purposes of section 512(a), (ii) they had actual knowledge and red flag awareness of infringement, and (iii) by inducing infringement they had both the right and ability to control infringement and a financial interest in it); *Capitol Records, LLC v. Escape Media Group, Inc.*, No. 12-cv-6646-AJN, 2015 WL 1402049, at *6-13, 44-58 (S.D.N.Y. Mar. 25, 2015) (entering summary judgment against Grooveshark where the court found that Grooveshark had not reasonably implemented its repeat infringer policy); *Disney Enterprises, Inc. v. Hotfile Corp.*, Case No. 11-cv-20427, 2013 WL 6336286 (S.D. Fla. Sept. 20, 2013) (holding Hotfile ineligible for the DMCA safe harbor for material stored at the direction of a user where it failed to reasonably implement its repeat infringer policy); *Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 153-54 (S.D.N.Y. 2009) (granting terminating sanctions and summary judgment against a Usenet hosting service and its owner where the court found defendants knew or should have known that their site was being used for infringement based on employee communications and where the defendants had tools available which they used to block certain content and users but did not employ those tools to block infringement); *In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634 (N.D. Ill. 2002), *aff'd on other grounds*, 334 F.3d 643 (7th Cir. 2003) (holding that a peer-to-peer service could not benefit from the DMCA safe harbors in part because it had failed to reasonably implement its repeat infringer policy and because material passed between users was not transmitted "through" the system

that encourage or turn a blind eye to infringement are deprived of DMCA safe harbor protection, while businesses that adhere to its technical requirements—including an ever growing list of new and innovative businesses such as social networks, UGC sites and sites that allow artists and entrepreneurs to develop new works and new business models—flourish, much in the way that Congress intended when it enacted the DMCA in 1998.

Of course, the DMCA alone cannot stop alleged infringers or their supporters from repeatedly posting unauthorized material on multiple locations online, both domestically and internationally. Where a user engages in ongoing or widespread infringement, litigation may be required. While suits against individual users serve a deterrent purpose, they are unlikely to stop viral distribution of an infringing file once it has been released on the Internet. The speed with which material may be posted, or reposted (either by the same user or others) following removal, is much faster than the time limits contemplated by the DMCA. Termination of a repeat infringer may prevent that infringer from reposting a work to a given site, but it does not stop the same user from posting the same file on another site or service.⁶⁷ Indeed, the DMCA cannot prevent the same user, or other users who

within the meaning of 17 U.S.C.A. § 512(b)(1)(B)); *A&M Records, Inc. v. Napster, Inc.*, No. 99-cv-05183-MHP, 2000 WL 573136, at *18 (N.D. Cal. May 12, 2000) (holding that Napster, a peer-to-peer network, was not eligible for the safe harbor created by section 512(a) for transitory digital network communications because users exchanged infringing files directly—not through Napster’s servers); see generally, e.g., *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) (holding that knowledge or awareness, which would deprive a site or service of DMCA protection, may be imputed to a defendant through evidence of willful blindness, which the court characterized as a deliberate effort to avoid guilty knowledge); *Fung*, 710 F.3d at 1043 (explaining that “inducing actions”—or measures deemed to induce copyright infringement—were relevant to the court’s determination that the defendant had red flag awareness and therefore was not entitled to DMCA safe harbor protection).

⁶⁷Case law to date has held that service providers do not lose DMCA protection because of the mere possibility that a user terminated as a repeat infringer could regain access to the service by falsely posing as a different person. See, e.g., *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 516 (S.D.N.Y. 2013) (holding that it was reasonable for Vimeo to block the email address, but not the IP address, of users terminated as repeat infringers, despite the possibility that a rogue user might reappear under a different name; following *Io Group*), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1144 (N.D. Cal. 2008) (holding that

copied a file after it was initially posted, from reposting the same file after it has been taken down. The viral nature of material posted on Internet sites and services means that copyright owners must look beyond the DMCA to filtering and other content recognition technologies—to adequately protect their works from infringement⁶⁸—and to more effective enforcement measures, especially overseas. The DMCA is a statutory regime that protects legitimate service providers and affords copyright owners fast, inexpensive remedies, to deal with infringement by individuals. It is not a tool to fight domestic or international pirate sites—nor does it provide safe harbor protection for them.

The DMCA “represents a legislative determination that copyright owners must themselves bear the burden of policing for infringing activity—service providers are under no such duty.”⁶⁹ The number of copyright notices sent to service providers each year is large. For example, as of mid-August, 2012, Google had processed takedown notices for 4.3 million URLs in the preceding 30 day period.⁷⁰ In November 2013,

the “hypothetical possibility that a rogue user might reappear under a different user name and identity does not raise a genuine fact issue as to the implementation of Veoh’s policy.”); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1103 (W.D. Wash. 2004) (writing that “[a]lthough this type of behavior is understandably vexing for a copyright holder like Corbis, it is not clear how Posternow’s efforts to sidestep Amazon’s policies amount to a failure of implementation.”).

Except where a site has already been enjoined based on a court’s determination that the plaintiff is likely to prevail on the merits and prove copyright infringement (as was the case in the Napster and Grokster lawsuits; *supra* § 4.11), courts have not required service providers to take extraordinary measures to prevent repeat infringers from anonymously gaining access to the site—largely out of recognition that an individual today can easily pose as someone else by assuming a different identity or using a different computer or ISP.

⁶⁸See *infra* § 17.05[3][C] (filtering technologies and the DMCA).

⁶⁹*In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634, 657–58 (N.D. Ill. 2002), *aff’d*, 334 F.3d 643 (7th Cir. 2003). The House Report accompanying the law makes clear, however, that the DMCA was “not intended to discourage the service provider from monitoring its service for infringing material.” See *infra* § 4.12[4]. Moreover, as already noted, service providers have an obligation to disable access to or remove material, even absent a notification, if they have actual knowledge or “red flag” awareness.

⁷⁰Google Inside Search (The Official Google Blog), “An Update to Our Search Algorithms,” Aug. 10, 2012, <http://insidesearch.blogspot.com/2012/08/an-update-to-our-search-algorithms.html>.

Google was asked to block access to 24,545,299 URLs.⁷¹ As of October 2015, Google had been asked to remove 50,639,990 URLs and block 71,649 domains by 5,690 copyright owners and 2,469 reporting organizations in the preceding month.⁷² In May 2016, Google received takedown requests for 91,595,236 URLs and 81,274 domains, which had been sent on behalf of 6,890 copyright owners and 3,088 reporting organizations.⁷³

By comparison, during the last six months of 2015, Microsoft received 976,134 DMCA takedown requests for links to 59,473,002 URLs posted on its Bing search engine (98% of which were taken down, while 985,090 were rejected).⁷⁴ During the same time period, Twitter received 35,004 DMCA notices.⁷⁵ By contrast, Snapchat received just seven DMCA notices (and no counter notifications) in the same time frame.⁷⁶

The DMCA does not apply some kind of “gotcha” test where every time an employee makes a mistake or fails to recognize material as potentially infringing, his or her employer suddenly loses safe harbor protection. As Judge Leval of the Second Circuit has explained, section 512(m) “makes clear that the service provider’s personnel are under no duty to ‘affirmatively seek[]’ indications of infringement.”⁷⁷ Further, in evaluating actual knowledge or red flag awareness, Judge Leval explained that “The hypothetical “reasonable person” to whom infringement must be obvious is an ordinary person—not endowed with specialized knowledge or expertise concerning music or the laws of copyright.”⁷⁸

Where they do not otherwise have actual knowledge or

⁷¹See <http://www.google.com/transparencyreport/removals/copyright/?hl=en> (visited Dec. 8, 2013).

⁷²See <https://www.google.com/transparencyreport/removals/copyright/> (visited October 12, 2015).

⁷³See <https://www.google.com/transparencyreport/removals/copyright/> (visited June 25, 2016).

⁷⁴See <https://www.microsoft.com/about/csr/transparencyhub/crrr/> (visited June 25, 2016).

⁷⁵See <https://transparency.twitter.com/copyright-notice/2015/jul-dec> (visited June 25, 2016).

⁷⁶See <https://www.snapchat.com/transparency> (visited June 25, 2016).

⁷⁷*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 94 (2d Cir. 2016).

⁷⁸*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-94 (2d Cir. 2016).

“red flag” awareness, service providers have no obligation to act unless they receive a substantially complying notification (and neither knowledge nor awareness may be inferred from a notification that is not substantially complying).⁷⁹ Thus, a service provider that otherwise meets the statutory requirements to qualify for the user storage safe harbor may not be held liable for copyright infringement if it does not have knowledge or red flag awareness and was not first provided the opportunity to respond to a substantially complying notification.

For example, the district court in *Perfect 10, Inc. v. CCBill, LLC*⁸⁰ ruled that a blanket statement that infringing copies of plaintiff’s works were found within 22,000 pages of documents, without specific identification of the infringing pages, did not provide sufficient notice to the service provider under the DMCA. Similarly, in *UMG Recordings, Inc. v. Veoh Networks, Inc.*,⁸¹ the court held that a notice that listed only a record company’s artists, rather than a representative list of works, and omitted any reference to the files on a service provider’s site alleged to be infringing, was deficient. Likewise, in *Hendrickson v. eBay, Inc.*,⁸² a copyright owner’s failure to authenticate a notification by including a written statement under penalty of perjury substantiating the accuracy of the notification (as required by section 512(c)(3)(A)(vi)) or certifying that he had “a good faith belief that use of the material in the manner complained of” was not authorized (as required by section 512(c)(3)(A)(v)) rendered the notice defective, justifying summary judgment for the defendant-service provider. Subsequently, in *Hen-*

⁷⁹See 17 U.S.C.A. § 512(c)(3)(B)(i). Where a notification is deficient but nonetheless substantially complies with the requirements for identifying the infringed work and the infringing material and includes sufficient contact information to allow the service provider to contact the complainant, however, the service provider must attempt to do so or “tak[e] other reasonable steps to assist” in obtaining a substantially complying notification before it may benefit from this provision. See 17 U.S.C.A. § 512(c)(3)(B)(ii); see generally *infra* §§ 4.12[6][C], 4.12[9][B].

⁸⁰*Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1096 (C.D. Cal. 2004), *aff’d in part on other grounds*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

⁸¹*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009), *aff’d on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁸²*Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

drickson v. Amazon.com, Inc.,⁸³ a court clarified that even a substantially complying notification will only be effective with respect to material online at the time it is sent, and cannot impose a continuing obligation on the service provider to monitor its service on an ongoing basis. In another district court case, where notice had been sent to the wrong entity, a court held in an unreported decision that a DMCA notice sent to a parent corporation was not effective in giving notice to the subsidiary.⁸⁴

Copyright owners, service providers, and users potentially may recover damages and attorneys' fees for misrepresentations made by copyright owners (in notifications) or users (in counter notifications), as analyzed more fully in section 4.12[9][D].⁸⁵ The Ninth Circuit has further held that a copyright owner faces liability under 17 U.S.C.A. § 512(f) if it knowingly misrepresents in a takedown notification that it has formed a good faith belief that the material identified in a DMCA notification was not authorized by law because the copyright owner failed to consider a user's potential fair use to the material before sending the DMCA notification.⁸⁶ This provision also potentially may be used to sue for declaratory relief or to seek an injunction prohibiting a competitor from sending unmeritorious DMCA notices for the purpose of having material removed from the Internet.⁸⁷ In lieu of litigation, claims under section 512(f) (but not the ancillary claims

⁸³*Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914 (C.D. Cal. 2003).

⁸⁴*See Perfect 10, Inc. v. Amazon.com, Inc.*, No. CV 05-4753 AHM (SHx), 2009 WL 1334364 (C.D. Cal. May 12, 2009). In that case, the court also held that DMCA notices sent after litigation was commenced were legally irrelevant in evaluating whether a service provider had notice of infringement.

⁸⁵*See infra* §§ 4.12[9][B], 4.12[9][C], 4.12[9][D], 4.12[9][F].

⁸⁶*See Lenz v. Universal Music Corp.*, 815 F.3d 1145 (9th Cir. 2016) (holding that a copyright owner must have a subjective good faith belief that allegedly infringing material does not constitute fair use before sending a DMCA takedown notice and that failing to form such a subjective good faith belief or being willfully blind would justify the imposition of sanctions under section 512(f)); *see also Lenz v. Universal Music Corp.*, 94 U.S.P.Q.2d 1344, 2010 WL 702466 (N.D. Cal. Feb. 25, 2010) (narrowly construing damages and fees potentially recoverable under section 512(f) in an earlier ruling in the case that was not addressed expressly by the Ninth Circuit in its opinion); *see generally infra* §§ 4.12[9][D], 4.12[9][F] (discussing the case at greater length), 4.10[1] (analyzing fair use).

⁸⁷*See infra* §§ 4.12[9][D] (section 512(f) sanctions, declaratory and injunctive relief), 4.12[9][F] (suits against copyright owners).

addressed in section 4.12[9][F]) may be brought before the Copyright Claims Board pursuant to the Copyright Alternative in Small-Claims Enforcement Act of 2020—or CASE Act⁸⁸—which is analyzed in section 4.08[8]. As set forth in that section, recovery under the CASE Act is capped at \$30,000 per proceeding (exclusive of attorneys’ fees and costs, which are also capped).

Wrongfully sending a DMCA notice potentially may also subject the complaining party to personal jurisdiction in the home state of the affected user because a substantially complying DMCA notice, unlike a simple cease and desist letter, will result in a service provider that complies with the DMCA expeditiously disabling access to or removing the offending material.⁸⁹

Some service providers, including Google, will forward DMCA notifications to *chillingeffects.org* (now *lumendatabase.org*), which catalogs and publicizes DMCA notifications, cease and desist letters and other legal notices, or otherwise post them online.

DMCA notices, if sent by email, generally are exempt from the requirements of the federal CAN-SPAM Act.⁹⁰

The DMCA, by its terms, applies to claims of copyright infringement, not other theories of liability.⁹¹ The statutory safe harbors, however, potentially apply to any claim of copyright infringement, not to specific theories of third-party liability. The DMCA therefore theoretically could apply to claims against service providers for third-party acts of infringement based on direct liability, contributory infringement, vicarious liability or inducing copyright infringement⁹² (even though the latter theory of recovery was judicially adopted approximately six-and-a-half years after the DMCA

⁸⁸See 17 U.S.C.A. §§ 1501 to 1511.

⁸⁹See *Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 333, 339–40 (D. Mass. 2013); see generally *infra* § 53.04[5][F] (analyzing jurisdiction based on DMCA and other takedown notices).

⁹⁰15 U.S.C.A. §§ 7701 to 7713. Efforts to negotiate licenses incident to resolving a dispute, however, must comply with the Act, if communicated by email. See *infra* § 29.04[2][B][iv].

⁹¹See generally *infra* chapter 49 (summarizing different theories of secondary liability that typically are asserted against service providers under various laws, subject to certain federal liability limitations and statutory exemptions).

⁹²See generally *supra* § 4.11 (analyzing secondary liability).

was enacted into law).⁹³ In practice, however, where liability could be established for inducing infringement (or for contributory infringement, if based on actual knowledge or intent) a service provider may have difficulty qualifying for the user storage liability limitation, which is inapplicable where a service provider has knowledge or awareness of the underlying acts of infringement and fails to act expeditiously in response to remove or disable access to the material or is willfully blind to infringing activity.⁹⁴ Of course, knowledge

⁹³The statute itself makes it clear that it applies to *all* potential claims for copyright infringement that fit within the specific exemptions set forth in sections 4.12[4] to 4.12[7]—not just those claims that existed in November 1998 when the DMCA was signed into law. *See* 17 U.S.C.A. § 512; *see also* *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 41 (2d Cir. 2012) (holding that “a finding of safe harbor application necessarily protects a defendant from all affirmative claims for monetary relief.”); *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1039–40 (9th Cir. 2013) (holding that the DMCA safe harbors potentially may be applied to a claim of inducement, but finding the transitory digital network communications, user storage and information location tools safe harbors inapplicable in that case); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1158 n.4, 1175 (9th Cir. 2007) (writing that the DMCA may apply if a service provider is found liable for “direct, contributory or vicarious copyright infringement” and that “the limitations on liability contained in 17 U.S.C. § 512 protect secondary infringers as well as direct infringers.”); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117 (9th Cir.) (“Section 512(c) ‘limits the liability of qualifying service providers for claims of direct, vicarious, and contributory infringement for storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider’”; *quoting* H.R. Rep. No. 105-551, Pt. II, at 53 (1998)), *cert. denied*, 522 U.S. 1062 (2007).

⁹⁴*See infra* § 4.12[6][C]. This is not to say that the DMCA does not protect service providers from liability for contributory infringement or inducement; merely that if there is evidence sufficient to prove inducement (and in some cases contributory infringement, if the theory of liability is based on knowledge) it is unlikely that a service provider could make the required showing for entitlement to the DMCA safe harbor. Inducement presupposes a level of intent that generally is inconsistent with lacking knowledge or awareness or reasonably implementing a policy of terminating repeat infringers in appropriate circumstances (and, depending on the facts of the case, may also evidence right and ability to control). *See generally supra* § 4.11[6] (analyzing inducement); *infra* §§ 4.12[3][B] (repeat infringer), 4.12[6][C] (knowledge or awareness), 4.12[6][D] (right and ability to control). Contributory infringement in some cases presupposes knowledge and substantial participation, although knowledge potentially may be imputed and substantial participation could be based on a failure to act (neither of which would imply knowledge or red flag awareness within the meaning of the DMCA). *See generally supra* § 4.11[3] (analyzing contributory infringement). While the DMCA should

or awareness are fact questions that would have to be proven in court if disputed.⁹⁵

The DMCA liability limitations constitute affirmative defenses that, in litigation, should be separately considered from liability.⁹⁶ At trial, this generally will mean that the defendant should be required to prove its entitlement to one or more of the liability limitations after the plaintiff rests its case (although, as one court noted, having to prove entitlement to the DMCA safe harbor at trial could “largely destroy the benefit of the safe harbor Congress intended to create.”).⁹⁷ In motion practice, the applicability of the DMCA liability limitations may be separately considered first, since a service provider’s entitlement to benefit from section 512 would moot potentially more complex (or fact-specific) liability questions.⁹⁸ As an affirmative defense, entitlement to the DMCA may be difficult to raise in a declaratory judgment action unless the complaint is specifically directed to particular works or “existing or foreseeable disputes about specific

insulate legitimate service providers that comply with its provisions from claims of inducement or contributory infringement, it should not shield pirate sites that induce or actively encourage (or turn a blind eye toward) infringement.

As discussed later in this subsection, DMCA issues frequently are addressed by summary judgment motion, obviating the need to evaluate liability on the merits if the service provider prevails on its motion.

⁹⁵Knowledge and intent may be resolved on motion for summary judgment or, if disputed, on a material point by admissible evidence, at trial.

⁹⁶The defendant bears the burden of proving its entitlement to one or more of the DMCA safe harbors. *See, e.g., ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 625 (4th Cir. 2001); *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1039 (9th Cir. 2013) (“Because the DMCA safe harbors are affirmative defenses, Fung has the burden of establishing that he meets the statutory requirements.”).

Where a service provider meets its burden to demonstrate entitlement to the DMCA safe harbor, the burden shifts to the copyright owner to prove that the service provider is not entitled to safe harbor protection based on knowledge or red flag awareness and failed to remove infringing files in the face of this knowledge or awareness. *See Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-95 (2d Cir. 2016).

⁹⁷*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 94 (2d Cir. 2016).

⁹⁸*See, e.g., Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 41–42 (2d Cir. 2012) (affirming in part and vacating and remanding in part, the lower court’s summary judgment order on the applicability of the DMCA user storage safe harbor “without expressing a view on the merits of the plaintiffs’ affirmative claims.”).

copyrights and instances of infringement.”⁹⁹ DMCA cases to date frequently have been decided (or largely decided) on summary judgment motions.¹⁰⁰ Unless timely raised, a service provider’s potential entitlement to the DMCA safe

⁹⁹*Windstream Services, LLC v. BMG Rights Management (US) LLC*, 16 Civ. 5015 (KMW) (RLE), 2017 WL 1386357 (S.D.N.Y. Apr. 17, 2017) (dismissing Windstream’s suit for a declaratory judgment that Windstream was entitled to the safe harbors created by sections 512(a) and 512(c), for lack of subject matter jurisdiction), *appeal dismissed*, Docket No. 17–1515, 2017 WL 5329346 (2d Cir. Sept. 25, 2017); *see also Veoh Networks, Inc. v. UMG Recordings, Inc.*, 522 F. Supp. 2d 1265, 1271 (S.D. Cal. 2007) (dismissing a declaratory judgment action premised on the plaintiff’s entitlement to the user storage safe harbor where plaintiff did not reference any specific copyright).

¹⁰⁰*See, e.g., Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78 (2d Cir. 2016) (holding the service provider entitled to DMCA protection); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012) (affirming in part, vacating and remanding in part, the lower court’s order granting summary judgment for YouTube); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597 (9th Cir. 2018) (affirming summary judgment for the service provider, holding that it was entitled to DMCA safe harbor protection); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013) (affirming summary judgment for the defendant-operator of a user submitted video site); *Kinsley v. Udemy, Inc.*, Case No. 19-cv-04334-JSC, 2021 WL 1222489 (N.D. Cal. Mar. 31, 2021) (granting summary judgment for Udemy on its DMCA defense); *Dona’t v. Amazon.com / Kindle*, 482 F. Supp. 3d 1137, 1140-41 (D. Colo. 2020) (granting summary judgment for Amazon.com, where plaintiff failed to present evidence that it sent a DMCA notification to Amazon.com for the material at issue, or to refute Amazon.com’s evidence that Amazon.com was entitled to the DMCA safe harbor); *Werner v. Evolve Media, LLC*, 2:18-cv-7188-VAP-SKx, 2020 WL 3213808, at *8 (C.D. Cal. Apr. 28, 2020) (granting summary judgment for the copyright owner on Evolve’s DMCA defense where Evolve, not a third-party user, posted all but one of the images at issue and, with respect to the last one, the image had been uploaded before Evolve had registered its DMCA agent); *Hempton v. Pond5, Inc.*, Case No. 3:15-cv-05696-BJR, 2016 WL 6217113 (W.D. Wash. Oct. 25, 2016) (granting summary judgment for Pond5, the operator of a website through which media producers may license and distribute content to third parties); *Milo & Gabby, LLC v. Amazon.com, Inc.*, No. C13-1932 RSM, 2015 WL 4394673, at *6-9 (W.D. Wash. July 16, 2015) (granting summary judgment in favor of Amazon.com on its DMCA defense), *aff’d on other grounds*, 693 F. App’x 879 (Fed. Cir.), *cert. denied*, 138 S. Ct. 335 (2017); *Avdeef v. Google, Inc.*, No. 4:14-CV-788-A, 2015 WL 5076877, at *1, 3-4 (N.D. Tex. Aug. 26, 2015) (granting summary judgment for Google on its DMCA defense, holding 14 days expeditious), *aff’d*, 678 F. App’x 239 (5th Cir. 2017); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (granting summary judgment for eBay).

harbors may be deemed waived.¹⁰¹

To a surprising extent, case law construing the DMCA for the first decade after its enactment was drawn disproportionately from district courts and appellate panels in one circuit—the Ninth Circuit. Even today, case law from outside the Ninth Circuit has been shaped and influenced by Ninth Circuit law, including influential district court cases from California applying Ninth Circuit precedent, because of the dearth of case law from other circuits. With the exception of two Fourth Circuit opinions and district court cases analyzing sanctions for misrepresentations in DMCA notices,¹⁰² all of the major cases construing the requirements of the DMCA for the first 11 1/2 years after the statute was signed into law in 1998 were decided by the Ninth Circuit or district courts within that circuit. The first Second Circuit opinion, *Viacom Int'l, Inc. v. YouTube, Inc.*,¹⁰³ was decided approximately 13 1/2 years after the DMCA was signed into law, even though the Second Circuit is one of the most important circuits for copyright law decisions. Even as of August 2016, there was not much DMCA safe harbor case law to speak of outside the Second, Fourth, Ninth and Tenth Circuits.

Blogs, social networks, cloud service providers, and other sites that host user generated content (UGC) all are potentially eligible for the DMCA safe harbors, if they meet the specific requirements of the statute.¹⁰⁴ Although these sites are technically more sophisticated and substantially

¹⁰¹See *Society of Holy Transfiguration Monastery, Inc. v. Gregory*, 689 F.3d 29, 58–59 (1st Cir. 2012) (holding that the defendant waived its right to argue that it was insulated from liability by the DMCA by not pleading the affirmative defense in its answer to plaintiff's complaint).

¹⁰²Sanctions for misrepresentations in DMCA notifications and counter notifications are authorized by 17 U.S.C.A. § 512(f) and analyzed in section 4.12[9][D].

¹⁰³*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 41–42 (2d Cir. 2012) (affirming in part, vacating and remanding in part a 2010 Southern District of New York order).

¹⁰⁴See, e.g., *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38–40 (2d Cir. 2012) (holding that transcoding and displaying user videos, among other things, were insulated from liability by the DMCA's user storage safe harbor); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1020–31 (9th Cir. 2013) (affirming summary judgment for a user submitted video site, holding that transcoding, streaming and allowing downloading of user videos did not undermine safe harbor protection); *infra* § 4.12[6] (analyzing the user storage liability limitation); see generally *infra* § 4.12[17] (discussing the UGC principles).

different sociologically from the Internet sites and services that were popular in 1998 when the DMCA was enacted, Congress understood that it could not fully anticipate future technological developments and therefore broadly defined “service provider” to encompass future sites and services. Nevertheless, the sites and services that Congress plainly had in mind when the DMCA was passed are not materially different from a legal perspective than today’s blogs, social networks and UGC sites. In 1998, Yahoo!, with its search features and links to other sites (or “information location tools”) and AOL, which allowed its users to post, store and transmit content (“material stored at the direction of users”) on personal homepages, websites and other interactive locations, collectively raised the same copyright law issues as today’s UGC sites.

Best practices frequently supplement the legal framework created by the DMCA. For example, Google, in 2012, announced that it would take into account in its site rankings the number of legitimate DMCA takedown notices that a site received.¹⁰⁵

A number of cross-industry accords have also been reached involving service providers and content owners. For example, a coalition of copyright owners and UGC sites promulgated the Principles for User Generated Content Services in October 2007 as a series of “best practices” for UGC sites to further protect copyright owners, beyond what the DMCA requires.¹⁰⁶ The UGC principles also create a quasi-contractual safe harbor for service providers that choose to comply with them, at least with respect to potential suits that otherwise could be brought by signatories to the UGC principles.

Similarly, in July 2011 a Memorandum of Understanding was reached between the Motion Picture Association of America (MPAA) and Recording Industry Association of America (RIAA) with major service providers, including Verizon, Comcast, Time Warner, SBC Internet Services and CSC Holdings on protocols to educate users about infringement and put in place a series of mitigation measures lead-

¹⁰⁵Google Inside Search (The Official Google Blog), “An Update to Our Search Algorithms,” Aug. 10, 2012, <http://insidesearch.blogspot.com/2012/08/an-update-to-our-search-algorithms.html>.

¹⁰⁶A copy of the Principles for User Generated Content Services is reproduced in § 4.12[17][B].

ing to sanctions such as reduced upload and download speeds. The MoU also led to the creation of the Center for Copyright Information (CCI) to help implement the MoU and combat online infringement.¹⁰⁷

In 2013, the White House's Office of the U.S. Intellectual Property Enforcement Coordinator, the Interactive Advertising Bureau (IAB), and Google, Yahoo!, Microsoft, and AOL, agreed to voluntary best practice guidelines for advertising networks to avoid promotion of pirate sites.¹⁰⁸ Participating ad networks agreed to maintain policies prohibiting websites that are principally dedicated to selling counterfeit goods or engaging in copyright piracy and have no substantial non-infringing uses from participating in advertising programs. Among other things, participants also agreed to accept and process "valid, reasonable, and sufficiently detailed notices from rights holders or their designated agents regarding websites participating in the Ad Network alleged to be principally dedicated to selling counterfeit goods or engaging in copyright piracy and to have no substantial non-infringing uses."¹⁰⁹ These voluntary agreements supplement that cooperation between copyright owners and service providers anticipated by Congress in its enactment of the DMCA.

Additional issues involving the DMCA and user generated content may be found in chapters 17 (licensing UGC content), 28 (advertising), 49 (liability for user generated content under multiple state and federal laws), 50 (strategies for managing the risks associated with third-party liability) and 51 (storage lockers, cloud facilities, mobile and Web 2.0 applications: social networks, blogs, wiki and UGC sites). DMCA forms that may be used by both copyright owners and service providers (as well as sample cover communications that may be used by service providers in administering DMCA programs) may be found in the appendix to this chapter.

While the DMCA safe harbors largely have worked for most copyright owners and service providers, the DMCA's liability scheme is not well suited to the needs of network service providers (NSP) or other entities that re-sell access to ISPs. For example, to benefit from the user storage limita-

¹⁰⁷See <http://www.copyrightinformation.org/>

¹⁰⁸See <http://2013ippractices.com/>

¹⁰⁹See <http://2013ippractices.com/>

tion, an NSP conceivably could be required to cut off access to a downstream service provider (affecting countless individual subscribers), merely as a result of the actions of one of the downstream provider's subscribers. Indeed, as predicted in the first edition of this treatise, the broad statutory language of the DMCA has even been interpreted to compel service providers in particular instances to disable access to or block third-party content originating on other services or elsewhere on the Internet.¹¹⁰ For these reasons, some NSPs have chosen to comply with some, but not all, of the specific limitations available under the statute, to impose compliance obligations by contract on downstream providers, or to disregard the statute entirely.

The DMCA is an imperfect law. The statute and its legislative history are not a model of clarity (in part because of the complexity of carving out specific, targeted liability limitations for a medium that is multifaceted and constantly evolving). On the other hand, the DMCA has proven flexible enough to adapt to changing technologies. Congress used broad terms—such as “information location tool,” rather than “link,” or “material stored at the direction of a user,” rather than “email account” or “website”—to expressly encompass future technologies.¹¹¹

The DMCA has brought clarity to the law of secondary

¹¹⁰In *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001), for example, the Fourth Circuit held that a service provider was not entitled to DMCA liability limitations because it refused to block two Usenet groups in response to substantially complying notifications relating to infringing materials accessible on these groups. Usenet groups, unlike websites, do not reside on a single server (or servers) accessed by users. Rather, the Usenet

is an international collection of organizations and individuals (known as ‘peers’) whose computers connect to each other and exchange messages posted by Usenet users. Messages are organized into “newsgroups,” which are topic-based discussion forums where individuals exchange ideas and information Peers in Usenet enter into peer agreements, whereby one peer’s servers automatically transmit and receive newsgroup messages from another peer’s servers. As most peers are parties to a large number of peer agreements, messages posted on one . . . peer’s server are quickly transmitted around the world. The result is a huge informational exchange system whereby millions of users can exchange millions of messages every day.

Ellison v. Robertson, 189 F. Supp. 2d 1051, 1053–54 (C.D. Cal. 2002) (footnotes omitted), *aff’d in part and rev’d in part*, 357 F.3d 1072 (9th Cir. 2004).

¹¹¹One of the reasons that there have not been as many cases construing the DMCA as other statutes that address service provider liability and user misconduct (*infra* §§ 37.05 (the Communications Decency Act), 49.03

copyright liability, allowed copyright owners to largely avoid having to sue legitimate Internet sites and services to have user material taken down, and enabled Internet industries to thrive without the fear of horrific liability for conduct that they cannot fully control. It also has enshrined a notice and takedown culture on the Internet that has largely been emulated internationally¹¹² and even applied in other areas of law.¹¹³

While the DMCA service provider safe harbors have been construed to date exclusively through case law, the U.S. Copyright Office announced its intention to study the effectiveness of the DMCA on December 31, 2015 and subsequently received submissions and held hearings in New York and San Francisco to address a series of questions posed by the U.S. Copyright Office.¹¹⁴ In its report, released in May 2020, the Copyright Office ultimately chose not to recommend any legislative amendments.¹¹⁵ may issue regulations or propose legislation to modify the DMCA.

& chapter 49 (statutes governing service provider liability more generally)) is that pirate sites generally are ruled ineligible for the statute's safe harbors and copyright owners have largely sought to work with, rather than sue, legitimate service providers under the DMCA (subject to some notable exceptions such as Perfect 10 (an adult magazine) and Universal Music Group). Unlike other Internet liability statutes, the DMCA also is potentially beneficial to both rights owners and service providers by affording service providers a safe harbor from liability and copyright owners the ability to have material removed without having to file suit. In addition, the line between copyright owner and service provider increasingly has blurred, as content owners have established their own user generated content sites and service providers have recognized the benefit of licensing, rather than merely disabling access to or removing, copyrighted works.

¹¹²See *infra* § 4.21 (analyzing the EU's E-Commerce Directive).

¹¹³See, e.g., *Tiffany (NJ) Inc. v. eBay Inc.*, 600 F.3d 93 (2d Cir.) (approving notice and takedown and a policy of terminating repeat infringers in holding a service provider not liable for secondary trademark infringement), *cert. denied*, 562 U.S. 1082 (2010); *infra* § 6.10 & chapter 49 (analyzing service provider liability and exemptions under multiple different legal theories).

¹¹⁴See <http://www.copyright.gov/policy/section512/> (detailing the Copyright Office's Section 512 Study). The author was an invited participant in the California Public Roundtable, which was held at the U.S. Court of Appeals for the Ninth Circuit in May 2016.

¹¹⁵See U.S. Copyright Office, Section 512 of Title 17 (May 2020), *available at* <https://www.copyright.gov/policy/section512/section-512-full-report.pdf>.

4.12[2] Definition of a Service Provider

The limitations and exemption created by the safe harbor provisions of the DMCA apply only to *service providers*, which is a term defined to include entities that offer the transmission, routing, or provision of connections “for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material sent or received”; or (except for the transitory digital network communications limitation¹) that provide “online services or network access,” or operate facilities therefor.² The definition applicable to the transitory digital network communications liability limitation is much narrower than for the other safe harbors.³

Except in connection with transitory digital network communications, *service provider*, on its face, is broad enough to extend well beyond ISPs and other services traditionally thought of as service providers to encompass the owners and operators of corporate intranets, university networks, website hosts or co-locators, cloud service providers, plat-

[Section 4.12[2]]

¹17 U.S.C.A. § 512(a); *infra* § 4.12[4].

²17 U.S.C.A. § 512(k).

³*Compare* 17 U.S.C.A. § 512(k)(1)(A) (narrowly defining the term *service provider* for purposes only of the transitory digital network communications safe harbor created by section 512(a)) *with* 17 U.S.C.A. § 512(k)(1)(B) (broadly defining the same term for purposes of the user storage, information location tools and caching safe harbors); *see generally infra* § 4.12[4] (discussing the definition in connection with the transitory digital network communications safe harbor).

In *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1041–42 (9th Cir. 2013), the Ninth Circuit held that the operator of a BitTorrent tracker did not qualify as a service provider for purposes of the narrower definition applicable to the transitory digital network communications safe harbor because trackers select the “points” to which a user’s client will connect in order to download a file using the BitTorrent protocol and a *service provider* for the transitory digital network communications safe harbor must provide “connections . . . between or among points specified by a user.” 17 U.S.C.A. § 512(k)(1)(A) (emphasis added).

The court in *A&M Records, Inc. v. Napster, Inc.*, No. C 99–05183 MHP, 2000 WL 573136, at *3 n.5 (N.D. Cal. May 12, 2000) expressed skepticism that Napster qualified for the narrower definition of *service provider* set forth in section 512(k)(1)(B) but since the plaintiffs had not challenged its eligibility the court proceeded to rule that Napster was ineligible for the liability limitation for transmitting, routing or providing connections on other grounds (because users exchanged infringing files directly—not through Napster’s servers).

forms used for third-party sales,⁴ social networks, blogs, and other interactive websites and services where third-party material (including user generate content) may be stored or cached or where links to such material may be established.⁵ As one court commented in *dicta*, a “plain reading of both definitions reveals that ‘service provider’ is defined so broadly that we have trouble imagining the existence of an online service that would not fall under the definitions, particularly the second.”⁶

As a consequence, any business with an interactive presence in cyberspace where third parties could post, store or transmit infringing material or engage in infringing activity

⁴*See, e.g., Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001) (operator of a website for the purchase and sale of consumer goods); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1100 (W.D. Wash. 2004) (“Amazon operates websites, provides retail and third-party selling services to Internet users, and maintains computers to govern access to its websites.”).

⁵*See, e.g., Kinsley v. Udemy, Inc.*, Case No. 19-cv-04334-JSC, 2021 WL 1222489, at *2 (N.D. Cal. Mar. 31, 2021) (granting summary judgment for Udemy on its DMCA defense; “Every reasonable trier of fact would find that Udemy is a service provider as defined under § 512(k)(1). It provides online services to its users in the form of its courses”); *Lenz v. Universal Music Corp.*, No. 5:07-cv-03783-JF, 2013 WL 271673, at *4 (N.D. Cal. Jan. 24, 2013) (holding in a section 512(f) dispute between a user and a content owner that “YouTube qualifies for protection under the DMCA safe harbor”), *aff’d on other grounds*, 815 F.3d 1145 (9th Cir. 2016); *Obodai v. Demand Media, Inc.*, Case No. 11 Civ. 2503 (PKC), 2012 WL 2189740, at *4 (S.D.N.Y. June 12, 2012) (holding Demand Media, the operator of Cracked.com and other websites, to constitute a service provider; “Because the defendant operates a website that permits users to post and share materials, it falls within the broad definition of a service provider under 512(k)(1)(B).”), *aff’d mem. on other grounds*, 522 F. App’x 41 (2d Cir. 2013); *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 744 (S.D.N.Y. 2012) (holding that “[b]ecause Photobucket offers a site that hosts and allows online sharing of photos and videos at the direction of users, Photobucket, like YouTube.com or Veoh.com, qualifies as a ‘service provider’ under § 512(k)(1)(B)” for purposes of the user storage safe harbor), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014); *Viacom Int’l Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 518 (S.D.N.Y. 2010) (holding YouTube to be a service provider), *aff’d in relevant part on other grounds*, 676 F.3d 19 (2d Cir. 2012).

⁶*In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634, 658 (N.D. Ill. 2002), *aff’d on other grounds*, 334 F.3d 643 (7th Cir. 2003). The Seventh Circuit reiterated in its subsequent opinion in the same case that, “[a]lthough the Act was not passed with Napster-type services in mind, the definition of Internet service provider is broad . . . , and, as the district judge ruled, Aimster fits it.” 334 F.3d at 655 (statutory citation omitted).

potentially could qualify as a service provider and should consider whether it would benefit by complying with the provisions of the statute discussed in the following subsections so that it can qualify for safe harbor protection.

Even where a service provider's activities are not limited to the provision of online services, "courts have consistently found that websites that provide services over and above the mere storage of uploaded user content are service providers pursuant to . . . § 512(k)(1)(B)'s expansive definition."⁷

Notwithstanding the broad construction given the term service provider under section 512(k)(1)(B), in *Agence France Presse v. Morel*,⁸ a district court in New York held that there was a material factual dispute precluding summary judgment on the issue of whether Getty Images constituted a service provider for purposes of the user storage safe harbor because it made available for license user uploaded images. That opinion, however, was wrongly decided.

In *Morel*, Judge Nathan conceded that the term *service provider* in section 512(k)(1)(B) has been construed broadly by courts, but nonetheless chose to read it narrowly by relying on dictionary definitions of *service* for the proposition that a service provider must "do something useful," and then concluding, somewhat inexplicably, that "licensing copyrighted material online more closely resembles the mere sale of goods (albeit, in this case, intellectual property) than facilitating users' activities online"⁹ even though there is no basis for excluding sites that license content or sell products from the statutory definition of *service provider* applicable to the user storage safe harbor.

The court in *Morel* seemed to draw a distinction between platforms where users may buy and sell products, such as

⁷*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 511 (S.D.N.Y. 2013) (citing earlier cases and holding that Vimeo, "a provider of online services that hosts and distributes user material by permitting its users to upload, share and view videos . . .," qualified as a service provider "[e]ven though Vimeo's activities are not limited to such . . ."), *aff'd in part on other grounds*, 826 F.3d 78 (2d Cir. 2016); *Obodai v. Demand Media, Inc.*, Case No. 11 Civ. 2503 (PKC), 2012 WL 2189740, at *3 (S.D.N.Y. June 12, 2012) (holding that a website that published its own content in addition to hosting and sharing users' content was a service provider), *aff'd mem.*, 522 F. App'x 41 (2d Cir. 2013).

⁸*Agence France Presse v. Morel*, 934 F. Supp. 2d 547 (S.D.N.Y. 2013).

⁹*Agence France Presse v. Morel*, 934 F. Supp. 2d 547, 565-68 (S.D.N.Y. 2013).

eBay and Amazon.com, and those that sell or license material directly, such as Getty, even if the material offered for sale or license was stored at the direction of a user. The court did not adequately explain why providing a venue for consumers to purchase products from third parties was “useful” but directly selling third-party products to the public would not be so. More importantly, the court’s novel focus on “usefulness,” and its own assumptions about whether sites that sell or license goods or services are more or less useful, is divorced from the language of the statute and, in the context of the safe harbor potentially claimed by Getty, the DMCA’s focus on material stored at the direction of a user, which has been broadly and inclusively defined by both the Second and Ninth Circuits.¹⁰ The court’s cramped definition of *service provider* is inconsistent with the broad construction of the statute given by appellate courts. It is also at odds with the plain terms of the statute and all prior court opinions construing the term.

This analysis is consistent with the way the court in *Greg Young Publishing, Inc. v. Zazzle, Inc.*¹¹ subsequently construed *Morel*. In *Greg Young Publishing*, Judge Stephen Wilson of the Central District of California characterized *Morel* as an “outlier” in treating the definition of *service provider* as a meaningful restriction on eligibility for safe harbor protection, whose analysis he found unpersuasive. He explained:

Morel is an outlier for a reason: its analysis is not persuasive. The court in *Morel* reasoned that Congress must have intended its definition of service provider “to impose some limitation on the availability of the § 512(c) safe harbors,” or it would not have provided such a definition at all. *Morel*, 934 F. Supp. 2d at 565. That premise is faulty. Congress will often define a term because it wants the term to carry a *broader* meaning than it would in ordinary parlance, or because it wants to emphasize that it is rejecting an implied limitation that might otherwise be imported from another area of law. Nothing about the definition of “service provider” in § 512(k)(1)(B) supports

¹⁰See *infra* § 4.12[6][A] (broadly defining the scope of protection under the user storage safe harbor as applying in any instance where liability is premised on material stored at the direction of a user and but for the user’s stored material liability would not be asserted against a service provider).

¹¹*Greg Young Publishing, Inc. v. Zazzle, Inc.*, Case No. 2:16-CV-05487, 2017 WL 2729584, at *6 (C.D. Cal. May 1, 2017).

the notion that it was intended as a limitation on § 512(c)'s safe harbor.¹²

Although the definition of a *service provider* is quite broad, it appears to exclude individuals. The DMCA defines a service provider as an “entity,” which presumably precludes a person from qualifying as a service provider. This may be significant for smaller Internet businesses operated by individuals or those considering whether to begin operations as a business entity or sole proprietorship.

4.12[3] Threshold Prerequisites

4.12[3][A] In General

A service provider's liability may only be limited under the Act if, in addition to meeting the requirements of one of the four specific safe harbors set forth in sections 512(a), 512(b), 512(c) or 512(d), it first satisfies four threshold requirements set forth in 17 U.S.C.A. § 512(i).¹ First, the service provider must have adopted a policy providing that it will terminate,

¹²*Greg Young Publishing, Inc. v. Zazzle, Inc.*, Case No. 2:16-CV-05487, 2017 WL 2729584, at *6 (C.D. Cal. May 1, 2017) (footnote omitted). The *Zazzle* court also criticized *Gardner v. CafePress Inc.*, No. 3:13-cv-1108-GPC-JMA, 2014 WL 794216 (S.D. Cal. Feb. 26, 2014), as unpersuasive in holding, in connection with a motion for summary judgment, that a company might not qualify as a service provider if it also offered offline services such as “facilitating the sale of products between internet users by directly selling products to online shoppers.” 2014 WL 794216, at *5. In *Greg Young Publishing*, Judge Wilson explained that “[t]he problem with this argument is that, as a logical matter, a company does not cease to be ‘a provider of online services’ because it offers offline services as well. There is nothing in the statutory text or in Ninth Circuit precedent that suggests an entity must be *primarily* engaged in providing online services to benefit from § 512(c)'s safe harbor.” 2017 WL 2729584, at *7. Although *Gardner* does not cite *Morel*, the court in *Gardner* plainly had read *Morel* and applied it in narrowly construing what constitutes a service provider based on whether a defendant was primarily engaged in providing online services. There is no statutory basis for evaluating a company's primary function in determining whether it qualifies as a service provider.

[Section 4.12[3][A]]

¹Subsection (i) provides that “[t]he limitations on liability established by this section” apply where the threshold requirements have been met, without specifically identifying the individual subsections of section 512 that are affected. The House Report accompanying the bill clarifies that the requirements of subsection (i) must be met in order to qualify for the limitations set forth in subsections (a) through (d) or the exemption created by subsection (g) (which the legislative history also refers to as a limitation).

“in appropriate circumstances,” the accounts or subscriptions of “repeat infringers.” Second, it must have informed its subscribers and account holders of its policy. Third, it must have “*reasonably* implemented” the policy. Fourth, it must accommodate and not interfere with “standard technical measures.”² These requirements are addressed in turn in the following subsections. A sample DMCA policy that includes a repeat infringer policy notice is reproduced in the Appendix to this chapter.

4.12[3][B] Adoption, Reasonable Implementation and Notice of the Policy

4.12[3][B][i] Adoption, Reasonable Implementation and Notice of the Policy—In General

Neither the statute nor its legislative history shed light on what type of policy is required, what constitutes “*appropriate* circumstances” or “*reasonable* implementation” of the policy, or at what point a person or entity might be deemed to constitute a “*repeat infringer*.” “The fact that Congress chose not to adopt . . . specific provisions when defining a user policy indicates its intent to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined.”¹

A service provider’s policy literally must “provid[e] for the termination in appropriate circumstances of subscribers and account holders of the service provider’s system or network who are repeat infringers”² While service providers may adopt and publicize more detailed practices and procedures, as a practical matter they need only track this statutory language to effectively inform their subscribers and account holders of their policy and comply with the statute. The policy details need not even be in writing (at least for a small company), so long as the site informs subscribers “of ‘a policy’ of terminating repeat infringers in

²17 U.S.C.A. § 512(i)(1) (emphasis added).

[Section 4.12[3][B][i]]

¹*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1101 (W.D. Wash. 2004).

²17 U.S.C.A. § 512(i)(1).

appropriate circumstances.”³ To provide notice, service providers should include this language or (if they choose) post more detailed policies in their Terms of Use or on their websites (or, if an internal service, on their corporate intranets).⁴

4.12[3][B][ii] Operational Considerations and the Obligation to Inform Subscribers and Account Holders

Service providers that have “account holders” and “subscribers,” such as ISPs or cable or phone companies, should reference the policy in their respective service or access agreements or Terms of Use.¹ Employers likewise may choose to include their DMCA policy in employee manuals or policy books.² As a practical matter, who is a *subscriber* or *account holder* has not been explored in litigation and is not defined in the statute or explained in its legislative history.

Service providers that do not have *subscribers* or *account holders* (such as search engines that do not offer free email or other services or the owners of corporate websites) pre-

³*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 615-16 (9th Cir. 2018). In *Motherless*, the court held that for a company run by its owners “and a few independent contractors” it was sufficient to inform subscribers that there was a policy, but have no written guidelines, where the owner alone made termination decisions. *Id.* at 616. The court opined, in *dicta*, that:

A company might need a written policy to tell its employees or independent contractors what to do if there were a significant number of them, but *Motherless* is not such a firm. Small operations in many industries often do not have written policies because the owners who would formulate the policies are also the ones who execute it. There might not have been a need for anything in writing. So the lack of a detailed written policy is not by itself fatal to safe harbor eligibility. Neither is the fact that *Motherless* did not publicize its internal criteria.

Id. (footnote omitted). By contrast, posting a policy and stating publicly that a service provider has one will be insufficient where the service in fact has no internal policies or procedures for terminating repeat infringers and in fact does not do so. *See UMG Recordings, Inc. v. Grande Communications Networks*, 384 F. Supp. 3d 743, 754-55 (W.D. Tex. 2019) (holding the defendant ineligible for DMCA safe harbor protection).

⁴For a discussion of how to structure, and where to post, website Terms and Conditions, *see infra* chapter 22.

[Section 4.12[3][B][ii]]

¹*See infra* §§ 22.05[2][A], 23.03[4].

²Employer policies and related issues are addressed in sections 58.09, 58.11 and 58.12.

sumably do not need to adopt or implement termination policies. There does not appear to be any basis for construing either the term “subscribers” or “account holders” so broadly that they could extend to mere users of a service or visitors to a website (in the absence of some type of contractual or employment³ relationship with the service provider). Nevertheless, it is advisable as a best practice—in view of the mandatory language of section 512(i)—for the owners of any Internet site or service with an interactive component that allows users to post, store or transmit material on or through their servers to adopt and publicize a policy of restricting the access rights of “repeat infringers” if it is technologically feasible for them to do so.

The requirement for notifying subscribers and account holders, imposes a relatively low burden on service providers. The statute “require[s] that the service provider ‘put users on notice that they face exclusion from the service if they repeatedly violate copyright laws’ . . . [but] does not ‘suggest what criteria should be considered by a service provider, much less require the service provider to reveal its decision-making criteria to the user.’ ”⁴ Section 512(i) “does not require that a service provider reveal its decision-making criteria to users . . . [or] provide its users with a detailed version of its policy, including all of the criteria it uses to determine whether an account will be suspended.”⁵

Courts have found the notice requirement met where Terms and Conditions or another policy state that a user may be terminated for repeat infringement.⁶ One court further rejected the argument that a service provider failed to

³An employee presumably could be characterized as an account holder if she is given a password that grants her access to a network. Anyone with an email address also may be viewed by a court as an account holder.

⁴*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1102 (W.D. Wash. 2004).

⁵*Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *8-9 (C.D. Cal. Jan. 16, 2015).

⁶*See, e.g., Hempton v. Pond5, Inc.*, Case No. 3:15-cv-05696-BJR, 2016 WL 6217113, at *4-6 (W.D. Wash. Oct. 25, 2016) (granting summary judgment for the service provider on plaintiff’s claim for copyright infringement where Pond5 required its users to accept its Terms of Use and Contributor Agreement before being allowed to upload any media to the website, which “clearly and unambiguously” prohibited contributors from uploading material to which they did not hold the copyright, over objections that under the policy Pond5 retained the right to terminate a user’s

provide adequate notice where it did not post a formal “repeat infringer” policy on its website until 2011, but had, since it began operations in 2004, included in its Terms of Service “a more general policy—threatening account termination upon any violation of the Terms of Service including single or repeated instances of infringement”⁷

A service provider should be deemed to satisfy its obligations to inform its subscribers and account holders of its policy merely by posting a notice on its website. A better practice, however, is to require users to affirmatively assent to or at least acknowledge the policy. Many service providers include reference to the policy in their Terms of Use. Service providers of course may choose to formally notify existing customers and subscribers by email or other means. If a site has pre-existing subscribers or account holders at the time it implements its DMCA policy, or if it changes its policy, it should consider providing notice to existing subscribers and account holders by email or at the time they first log on to the site after the new policy has taken effect, or by other means.⁸ For example, service providers that host blogs, social networks, chat rooms or other locations where user generated content may be posted may find it advisable to provide notice via a pop-up box that could appear the first time a visitor enters after a new DMCA policy goes into effect (through use of cookies or other means to identify when a user has not yet been notice of the new policy) or via a link, although courts have not required that this kind of notice be provided. Indeed, some user generated video sites and social

access to the website in the event of a breach Pond5’s Terms of Use, rather than expressly for repeat infringement; “The fact that Pond5 allows for such banishment for *any* violation of its terms, rather than specifically limiting banishment to repeat infringers, is immaterial. Pond5 goes beyond the threshold requirement of DMCA by communicating a policy to its users that allows for termination for any infringement.”); *Obodai v. Demand Media, Inc.*, Case No. 11 Civ. 2503 (PKC), 2012 WL 2189740, at *4 (S.D.N.Y. June 12, 2012) (holding that Demand Media, the operator of Cracked.com, met this requirement where its policy provided that it could terminate “any Account or user for repeated infringement . . . and . . . reserved[d] the right to terminate an Account or user for even one infringement.”), *aff’d mem. on other grounds*, 522 F. App’x 41 (2d Cir. 2013).

⁷*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 514 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁸Suggestions about operational “best practices” are not meant to imply that such practices are necessarily required to benefit from the DMCA safe harbors.

networks provide a link to their copyright policies on all pages where material may be uploaded, downloaded or reviewed.⁹

Service providers also may opt to draft template responses such as a specific warning to send to first time offenders. Such a warning should advise an offender that its account or network access will be terminated if a second complaint is received (or whatever the service provider's policy in fact provides).

4.12[3][B][iii] Adopting a Policy and Defining "Repeat Infringer"

The fact "that Congress chose not to adopt . . . specific provisions when defining a user policy indicates its intent to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined."¹ Many stated policies do little more than track the statutory language, stating that the service provider has a policy of terminating repeat infringers in appropriate circumstances.²

For the policy to have meaning, it is advisable that a service provider explicitly prohibit copyright infringement and not merely state that it has a policy of terminating repeat infringers in appropriate circumstances. Many sites require an affirmative undertaking by users that material they upload to or otherwise store on a site or service is not infringing which, while not mandated by the DMCA, is certainly a

⁹For a discussion of "best practices" for user generated video sites, see *infra* § 4.12[17].

[Section 4.12[3][B][iii]]

¹*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1101 (W.D. Wash. 2004).

²See 17 U.S.C.A. § 512(i)(1)(A). Needless to say, posting a policy and stating publicly that a service provider has one will be insufficient to establish adoption of a policy where the service in fact has no internal policies or procedures for terminating repeat infringers and in fact does not do so. See *UMG Recordings, Inc. v. Grande Communications Networks*, 384 F. Supp. 3d 743, 754-55 (W.D. Tex. 2019) (holding the defendant ineligible for DMCA safe harbor protection, noting that although Grande had a public-facing policy since 2012 and "apparently stated publicly that its policy was to terminate infringing customers, Grande's corporate representative testified that from 2010 through 2016, Grande did not have any specific policies or procedures providing for how it would actually go about terminating any such infringing customers. . . . In internal emails, one Grande employee even stated that 'we have users who are racking up DMCA take down requests and no process for remedy in place.'").

good practice.

In adopting a repeat infringer policy, a service provider must determine how it will identify a user as a repeat infringer, although it need not spell that out in the policy communicated to its subscribers and account holders.

A *repeat infringer*, by definition, is someone who has engaged in infringing conduct on more than one occasion.³ Yet, neither the statute nor the legislative history define *repeat infringer*.

In discussing the provisions applicable to nonprofit educational institutions,⁴ the House Report refers to more than two notifications within a three-year period as “a pattern of infringing conduct” This reference arguably suggests that a person would be deemed to be a *repeat infringer* once a second notification was received (assuming that the notifications were not based on material misrepresentations or otherwise invalid).

Treating a repeat infringer as someone who has been the subject of a second notification is a prudent approach and one that has been upheld as reasonable by at least one court.⁵ On the other hand, district courts in the Central District of California and Southern District of New York have approved of repeat infringer policies premised on termination upon receipt of a third DMCA notice, rather than a second one.⁶ One court also expressly approved of a service provider’s policy of treating notifications received within a three-day

³See *BMG Rights Management (US) LLC v. Cox Communications, Inc.*, 881 F.3d 294, 301 (4th Cir. 2018) (“A repeat infringer . . . is one who infringes a copyright more than once.”).

⁴See 17 U.S.C.A. § 512(e).

⁵See *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

⁶See *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 511-17 (S.D.N.Y. 2013), *aff’d in part, rev’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016); *Viacom Int’l Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *aff’d in relevant part on other grounds*, 676 F.3d 19, 40–41 (2d Cir. 2012); *UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009), *aff’d on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013); *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1094 n.12 (C.D. Cal. 2004), *aff’d in part on other grounds*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007); see also *BMG Rights Management (US) LLC v. Cox Communications, Inc.*, 881 F.3d 294, 301 (4th Cir. 2018) (stating in *dicta* that “[a] repeat infringer . . . is one who infringes a copyright more than once.”).

period as a single strike.⁷ While there is nothing in the statute or legislative history specifically to suggest that someone who has been the subject of two notices may be treated as not being a repeat infringer, Americans love baseball and it is difficult to imagine a judge or jury finding that a three strikes policy is unreasonable.

Perhaps more importantly, it is clear from the fact that Congress modified the requirement that service providers terminate repeat infringers by the caveat that termination need only occur in *appropriate circumstances*, that the statute is intended to be flexible and allow service providers to implement policies that they deem appropriate for their services or based on the type of infringing activity involved. Moreover, as discussed more extensively in section 4.12[3][B][iv], Congress further modified the requirement by providing that a policy of terminating repeat infringers in appropriate circumstances be *reasonably implemented*, which suggests both that the policy in fact must be implemented, but also that it may be *reasonably*, rather than strictly implemented.

In the words of the Ninth Circuit, “[t]he statute permits providers to implement a variety of procedures.”⁸ Indeed, no single policy is mandated beyond what is literally set forth in the language of the statute—a policy of terminating repeat infringers in appropriate circumstances.⁹

Nevertheless, what constitutes an infringer should not be

In *YouTube*, the district court also rejected Viacom’s argument that YouTube did not reasonably implement its repeat infringer policy because it treated as only one strike: (1) a single DMCA takedown notice identifying multiple videos, and (2) multiple takedown notices identifying videos uploaded by a user received by YouTube within a two-hour period.

The district court likewise discounted Viacom’s argument that YouTube’s repeat infringer policy was not reasonably implemented because YouTube only counted DMCA notices; it did not account for videos automatically removed by Audible Magic content filters. These aspects of the district court’s ruling were not addressed in the Second Circuit’s opinion, which focused narrowly on the issue of whether YouTube’s provision of a search tool only to business partners, and not plaintiffs, meant that it had failed to reasonably implement its repeat infringer policy (which the appellate court concluded it had not).

⁷*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 516 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁸*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1109 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

⁹*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1101 (W.D.

defined too narrowly. The Second Circuit has held that a policy that treated uploaders as infringers for purposes of a DMCA repeat infringer policy, but did not consider downloads of infringing material intended for personal use to be infringing, was unreasonable.¹⁰ In that case, *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*,¹¹ the defendant defined a repeat infringer as a user who posted or uploaded infringing content “to the internet for the world to experience or copy” knowing that it infringed another’s copyright. The court held that this policy also was too narrow in limiting its focus to acts of willful infringement given that liability under the Copyright Act may be imposed even on a party who did not “know of the infringing nature of its online activities”¹²

While a policy that provides blanket protection for personal links and downloads of infringing material and does not treat as infringement anything less than conduct that was willful will not pass muster in the Second Circuit in light of this case, the proviso that a service provider *reasonably implement* its policy¹³ means that in individual cases a service provider potentially could choose to not terminate a subscriber or account holder for innocent infringement, but any variation from a service provider’s policy would have to be justified as reasonable in the event of litigation (and widespread variances could support a finding that the policy was not reasonably implemented, depriving the service provider of any safe harbor protection).

The Second Circuit panel also elaborated that a company could be found to have not reasonably implemented its repeat infringer policy if it consciously avoided knowing about specific repeat infringers on its service, and therefore was willfully blind.¹⁴

In an amended opinion, the panel clarified that it was not

Wash. 2004).

¹⁰See *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 88-89 (2d Cir. 2016).

¹¹*EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79 (2d Cir. 2016).

¹²*EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 90 n.6 (2d Cir. 2016).

¹³See *infra* § 4.12[3][B][iv].

¹⁴See *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 91 (2d Cir. 2016). Willful blindness is discussed extensively in connec-

addressing the question of “whether MP3tunes would be required to terminate a user who visited sideload.com only to stream files rather than sideload them into an MP3tunes locker.”¹⁵

In *Capitol Records, LLC v. Vimeo, LLC*,¹⁶ Judge Ronnie Abrams of the Southern District of New York held that the video sharing site Vimeo met the requirement for adopting a policy of terminating repeat infringers in appropriate circumstances where, since the time it began operations in 2004, it required users to assent to Terms of Service that informed them that Vimeo reserved the right to remove videos and terminate user accounts for violation of its Terms, Vimeo had implemented a three strikes policy and evidence showed that it in fact had terminated users as early as 2007, including in some instances upon receipt of a single takedown notice. In so ruling, the court rejected the plaintiffs’ argument that Vimeo had not adopted a policy early on its existence. Judge Abrams explained that “Vimeo’s policy became more structured and refined as Vimeo’s employee roster and user base grew, but the evidence establishes that Vimeo had a policy in place that provided for the termination of service for repeat (or even first-time) infringers from the company’s inception. The DMCA requires nothing more . . .” to meet this threshold requirement.¹⁷

Some have argued that an infringer, by definition, is a person who has been adjudicated as such, and thus a repeat infringer policy would only apply to those who have been successfully sued for copyright infringement. This analysis, however, is unsupported by the statute or its legislative history and has been expressly rejected by the Fourth Circuit.¹⁸ As noted above, the House Report’s reference to two notifications as evidencing a “pattern of infringement” belies the argument that an *infringer* for purposes of the DMCA is

tion with knowledge and red flag awareness under the DMCA (in section 4.12[6][C]) and contributory infringement (in section 4.11[3]) and inducement (in section 4.11[6]).

¹⁵See *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 90 n.6 (2d Cir. 2016).

¹⁶*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 511-13 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

¹⁷*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 513 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

¹⁸See *BMG Rights Management (US) LLC v. Cox Communications, Inc.*, 881 F.3d 294, 301-03 (4th Cir. 2018).

someone who has been found liable by a judge or jury for copyright infringement. Moreover, the notice and takedown system created by the DMCA was intended, among other things, to allow copyright owners to obtain protection through cooperation with service providers, rather than litigation. Requiring a copyright owner to successfully sue a user repeatedly before a service provider would have an obligation to terminate access to an account holder or subscriber is simply inconsistent with the legislative scheme established by the DMCA.

On the other hand, at least in the Ninth Circuit, consideration only of DMCA notifications in determining whether an account holder or subscriber is a repeat infringer may be insufficient in certain circumstances under *Perfect 10, Inc. v. CCBill, LLC*,¹⁹ in which the court held that whether a service provider has reasonably implemented its policy of terminating repeat infringers in appropriate circumstances requires evaluation of how the service provider responded both to notifications *and* instances where it had actual knowledge or “red flag” awareness of infringement.²⁰ In other words, in the Ninth Circuit, failing to track red flag material theoretically could put at risk not just safe harbor protection for that material, but for the entire service, based on whether the omission evidences that the service provider is not reasonably implementing a policy of terminating repeat infringers in appropriate circumstances.

Since a service provider’s obligation to remove material in response to actual knowledge or red flag awareness only arises in connection with the user storage liability limitation, it may be hard to argue that these additional factors should be considered in evaluating a repeat infringer policy for purposes of the other three safe harbors or the exemption from liability for removing user material. Moreover, while a service provider may err on the side of caution in removing material of its own volition based on red flag awareness, it may not be appropriate to terminate an account holder or

¹⁹*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir. 2007), cert. denied, 522 U.S. 1062 (2007).

²⁰*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113-14 (9th Cir.), cert. denied, 522 U.S. 1062 (2007). Knowledge and “red flag” awareness are analyzed below in section 4.12[6][C]. The *Perfect 10* case is also discussed more extensively in the following subsection in connection with reasonable implementation of a repeat infringer policy in section 4.12[3][B][iv].

subscriber as a repeat infringer based solely on the intuition of a service provider. Hence, a policy that defines a repeat infringer in terms of actual notifications received from copyright owners (who after all are in the best position to know whether their works in fact have been infringed, and whose notifications of infringement are submitted under penalty of perjury and subject to sanctions under section 512(f)²¹) may in fact be reasonable, although a safer approach for risk averse service providers would be to terminate users as repeat infringers based on actual knowledge or reasonable awareness as well as notifications submitted by copyright owners. At least in the Ninth Circuit, if not elsewhere,²² a plaintiff may be allowed discovery of a service provider's response to material and activity where it had actual knowledge or red flag awareness, to evaluate reasonable implementation of that policy in connection with a case where the service provider is relying on the user storage safe harbor.

As a practical matter, in the event of litigation, service providers would be better poised to defend themselves if they have mechanically applied their repeat infringer policies and erred on the side of termination, rather than opening themselves up to discovery and motion practice (or even trial) on the question of whether the service provider *reasonably* implemented its policy of terminating repeat infringers *in appropriate circumstances*. Those that terminate accounts upon receipt of a second or possibly third DMCA notification (and at least in the Ninth Circuit, for purposes of the user storage liability limitation, a second instance of infringement based on a notification or removal for actual knowledge or red flag awareness) will be better able to establish their compliance with the requirements of the statute, and potentially obtain summary judgment, than service providers that make exceptions for given users and do not apply their policies uniformly, whose compliance may be so fact-dependent that their entitlement to the safe harbor cannot easily be determined except at trial (which is riskier and more expensive than if the issue is resolved through motion practice). Whereas termination of all potential repeat infring-

²¹See *infra* § 4.12[9][D].

²²The *Perfect 10* standard was cited approvingly in *Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 139–42 (S.D.N.Y. 2009), a case where sanctions for spoliation of evidence were imposed on defendants that had failed to retain evidence relevant to their compliance with red flag material under *Perfect 10*.

ers may be shown by undisputed facts in connection with a motion for summary judgment, whether the failure to terminate a user was “appropriate” or suggests a failure to reasonably implement a repeat infringer policy may, in some circumstances, raise disputed factual questions that preclude summary judgment.

This is not to say that a mechanical approach is required by the statute, because it is not. As noted above, the obligation to terminate repeat infringers only arises in appropriate circumstances. Indeed, simply because a DMCA notice has been sent does not mean that the user whose content is at issue is necessarily even an infringer. In some instances a copyright owner could be mistaken and material identified in a notification could be licensed or permitted as a fair use. A service provider that receives two or three notifications from a copyright owner that are shown to be invalid, either based on mistake or misrepresentation or an account holder’s submission of a counter notification that goes unanswered by the copyright owner, would have no obligation to terminate the affected user as a repeat infringer. A service provider that keeps good records and is prepared to defend its termination decisions in appropriate circumstances will not be denied the benefits of the DMCA safe harbor. Nevertheless, for companies that do not have the resources or appetite to justify their conduct in such a labor-intensive manner in litigation, a stricter interpretation may be the safer approach.

The DMCA creates incentives for service providers to err on the side of removing material and terminating users.²³ Although the statute merely mandates termination of repeat infringers in appropriate circumstances, where it is apparent that a subscriber or account holder is flagrantly violating the Copyright Act—such as where a person is using a site exclusively or primarily to upload infringing images from a magazine, protected software or pirated music, films or

²³Except where a notification is received from a copyright owner, a service provider that otherwise complies with the threshold requirements of the Act will be exempt from liability for terminating service to someone who it believes in good faith is engaged in acts of infringement. 17 U.S.C.A. § 512(g); *see generally infra* § 4.12[8]. Conversely, if a service provider fails to act when it has reason to believe that infringing content may be online, it may be denied the benefit of the user storage and information location tools limitations if a court determines that it had red flag awareness or actual knowledge. 17 U.S.C.A. § 512(c)(1)(A), 512(d)(1)(A).

videogames—it may be prudent for a service provider (regardless of its policy) to simply terminate service at the time the infringement is first discovered. That is not to say that an account holder or subscriber could be deemed a repeat infringer based on an initial notification (or discovery creating knowledge or awareness) of infringement involving multiple works. Congress used the term “repeat infringer,” which is focused on repetitive conduct, rather than “multiple infringements” or other terminology that would suggest that the volume of infringement, rather than repeated bad behavior, is the relevant consideration. Although it seems unlikely that someone whose first violation involved multiple works could actually be considered a repeat infringer, it nonetheless may be prudent for service providers, in appropriate circumstances, to take action against subscribers or account holders whose sites or services contain multiple infringing works. In practice, service providers that appear to be compliance oriented and that do more than the statute requires are less likely to be sued and more likely to be given the benefit of the doubt by judges and juries than those that do the bare minimum.

4.12[3][B][iv] Reasonable Implementation of A Service’s Repeat Infringer Policy

The requirement that a service provider’s policy of terminating repeat infringers in appropriate circumstances be *reasonably implemented*, like the DMCA itself, reflects an attempt to balance the needs and interests of both copyright owners and service providers. On the one hand, a service provider must in fact implement its repeat infringer policy,¹ and must do so reasonably. On the other hand, Congress

[Section 4.12[3][B][iv]]

¹Although it should go without saying, identifying but failing to actually terminate any repeat infringers without some explanation to justify *reasonable implementation or appropriate circumstances* would disqualify a service provider from the safe harbor. See, e.g., *UMG Recordings, Inc. v. Grande Communications Networks*, 384 F. Supp. 3d 743, 754-58 (W.D. Tex. 2019) (holding the defendant ineligible for DMCA safe harbor protection where Grande ended its policy of “turning off” subscribers and requiring them to contact Grande to discuss the issue in response to copyright violation notices in 2010, and, although it posted a repeat infringer policy in 2012 and publicly stated that it had a policy of terminating repeat infringers, Grande in fact did not terminate any users as repeat infringers from October 2010 to May 2017 even though it received over a million copyright notices between 2011 and 2016 and internal emails

could have required strict adherence to termination policies, but instead merely required *reasonable* implementation, recognizing that service providers are not a monolithic group and that in a medium that is constantly evolving where user infringement may occur willfully or inadvertently, it is beneficial to allow service providers flexibility in how a policy is crafted, what constitutes appropriate circumstances for termination and how the policy in fact is implemented.² “Safe harbor eligibility does not require perfection, just ‘reasonable’ implementation of the policy ‘in appropriate circumstances.’”³ Failing to reasonably implement a repeat infringer policy will preclude safe harbor protection (at least until the compliance defect is cured).⁴

Reasonable implementation of a repeat infringer policy presupposes that the policy itself is reasonable.⁵ Where the policy is unreasonable, reasonable implementation is not possible. Similarly, where a company’s executives were encouraged to and did personally use a service to link to or download infringing music for their personal use, the Second Circuit held that a reasonable jury could infer that the

showed that it was tracking user complaints and had over 9,000 customers on its “Excessive Violations Report” by late 2016, and had some users who had received up to 54 notices); *Datatech Enterprises LLC v. FF Magnat Ltd.*, No. C 12-04500 CRB, 2013 WL 1007360, at *5–6 (N.D. Cal. Mar. 13, 2013) (declining to dissolve a preliminary injunction against an offshore cloud file storage site accused of copyright infringement where the court found that the defendant was unlikely to prevail on its DMCA defense based on evidence that it had ignored copyright holders’ requests to remove specifically identified repeat infringers, including one individual who uploaded 1,600 separate copies of an infringing work).

²Adoption of a repeat infringer policy is separately addressed in section 4.12[3][B][iii].

³*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 618 (9th Cir. 2018). In *Motherless*, the court found that Motherless had reasonably implemented its repeat infringer policy as a matter of law where it had terminated between 1,320 and 1,980 users for alleged infringement and only nine had been able to rejoin. *Id.* at 619. The court reiterated that “[e]ligibility for the safe harbor is not lost just because some repeat infringers may have slipped through the provider’s net for screening them out and terminating their access.” *Id.*

⁴*See, e.g., Atlantic Recording Corp. v. Spinrilla, LLC*, 506 F. Supp. 3d 1294, 1320 (N.D. Ga. 2020) (holding that Spinrilla could not invoke the DMCA safe harbor for infringement on its service that took place prior to the time it adopted a repeat infringer policy).

⁵*See generally supra* § 4.12[3][B][iii] (analyzing what constitutes a permissible repeat infringer policy).

company consciously avoided knowing about specific repeat infringers using its service, which would amount to a failure to reasonably implement its repeat infringer policy.⁶

“At a minimum,” the Fourth Circuit explained, “an ISP has not ‘reasonably implemented’ a repeat infringer policy if the ISP fails to enforce the terms of its policy in any meaningful fashion”⁷ or, stated alternatively, “in any consis-

⁶See *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 91 (2d Cir. 2016). In that case, the court found that the defendant’s policy itself was unreasonable. See *id.*; see generally *supra* § 4.12[3][B][iii] (analyzing this aspect of the case).

⁷*BMG Rights Management (US) LLC v. Cox Communications, Inc.*, 881 F.3d 294, 303 (4th Cir. 2018), citing *In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634, 659 (N.D. Ill. 2002), *aff’d*, 334 F.3d 643 (7th Cir. 2003) (“Adopting a repeat infringer policy and then purposely eviscerating any hope that such a policy could ever be carried out is not an ‘implementation’ as required by § 512(i).”). In *BMG v. Cox*, the service provider had adopted a 13 strike policy, which itself could have been challenged as unreasonable. In addressing *reasonable implementation*, however, the court concluded that “Cox very clearly determined *not* to terminate subscribers who in fact repeatedly violated the policy.” 881 F.2d at 303 (emphasis in original). Prior to September 2012, Cox had an unofficial policy of allowing repeat infringers to sign back on the service and reset their strike count to zero, as reflected in internal employee emails. The court characterized the evidence from this time period as showing that “Cox *always* reactivated subscribers after termination, regardless of its knowledge of the subscriber’s infringement.” *Id.* at 304 (emphasis in original). In September 2012, Cox abandoned “its practice of routine reactivation”—as evidenced by an employee email stating that “we now terminate, for real”—but the court found that “Cox simply stopped terminating them in the first place. Before September 2012, Cox was terminating (and reactivating) 15.5 subscribers per month on average; after September 2012, Cox abruptly began terminating *less than one* subscriber per month on average.” *Id.* at 304 (emphasis in original). Indeed, between September 2012 and the end of October 2014—the month before BMG filed suit—Cox issued only 21 terminations in total, 17 of which were to subscribers who had either failed to pay their bills on time or used excessive bandwidth. *Id.* The court noted that Cox did not provide evidence that the remaining four terminations were for repeat copyright infringement but stated that “even assuming they were, they stand in stark contrast to the over 500,000 email warnings and temporary suspensions Cox issued to alleged infringers during the same time period.” *Id.* Cox also had dispensed with terminating subscribers who infringed BMG’s copyrights by deleting automatically all infringement notices sent on BMG’s behalf by Rightscorp., an agency that sent notices and demanded payment for unauthorized material. The court further noted that “Cox failed to terminate subscribers whom Cox employees regarded as repeat infringers.” *Id.* The court concluded that Cox failed to meet its burden of proof on the DMCA defense on the issue of reasonable implementation. *Id.*

tent or meaningful way—leaving it essentially with no policy.”⁸

Indeed, what it means to *reasonably implement* a repeat infringer policy has often been defined by courts largely in negative terms based on what courts had found to be *unreasonable*,⁹ leaving open tougher questions about how much

at 305. It also “failed to provide evidence that a determination of ‘appropriate circumstances’ played *any* role in its decisions to terminate (or not to terminate).” *Id.* (emphasis in original).

⁸*BMG Rights Management (US) LLC v. Cox Communications, Inc.*, 881 F.3d 294, 305 (4th Cir. 2018).

⁹In *In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634 (N.D. Ill. 2002), *aff’d*, 334 F.3d 643 (7th Cir. 2003), the court ruled that a peer-to-peer service that encouraged users to exchange unauthorized copies of protected music files, made it easy for them to do so, and encrypted the files and their users’ identities (making detection of individual acts of infringement more difficult), was not entitled to benefit from the DMCA’s liability limitations where it had adopted a policy of terminating repeat infringers that amounted to “an absolute mirage” because it was never implemented. Defendants had argued that although plaintiffs may have identified copyrighted works residing on individual hard drives, plaintiffs could not demonstrate that any particular user actually transferred any of those files, and that they would terminate service to any user identified as a repeat infringer. The court noted that this assurance was “not nearly so helpful and agreeable as it seems . . . because, according to defendants themselves, such identification would be impossible” because Aimster files are encrypted.

The *Aimster* court also took issue with the requirement in Aimster’s termination policy that copyright owners identify the Internet protocol address of infringers using its system.

On both of these grounds, the court ruled that “[a]dopting a repeat infringer policy and then purposefully eviscerating any hope that such a policy could ever be carried out is not an ‘implementation’ as required by § 512(i).” 252 F. Supp. 2d at 657–58.

Although the Seventh Circuit did not address the issue as extensively as the district court in *Aimster*, Judge Posner, in affirming the district court on this point explained that:

The common element of its safe harbors is that the service provider must do what it can reasonably be asked to do to prevent the use of its service by “repeat infringers.” 17 U.S.C.A. § 512(i)(1)(A). Far from doing anything to discourage repeat infringers of the plaintiffs’ copyrights, Aimster invited them to do so, showed them how they could do so with ease using its system, and by teaching its users how to encrypt their unlawful distribution of copyrighted materials disabled itself from doing anything to prevent infringement.

334 F.3d at 655. Similarly, in *A&M Records, Inc. v. Napster, Inc.*, No. C 99–05183 MHP, 2000 WL 573136 (N.D. Cal. May 12, 2000), the lower court in the *Napster* case held that there was a genuine issue of fact precluding summary judgment on the issue of whether Napster had reasonably implemented a policy of terminating repeat infringers in appropri-

flexibility a service provider should have in particular cases.

ate circumstances where Napster only adopted its copyright compliance policy after the onset of litigation and plaintiffs had presented evidence that Napster could have kept terminated users from re-accessing the service by blocking their IP addresses, but did not do so and generally turned a blind eye to infringement. *A&M Records, Inc. v. Napster, Inc.*, No. C 99-05183 MHP, 2000 WL 573136, at *9-10 (N.D. Cal. May 12, 2000); see also *supra* § 4.12[4] (discussing the court's ruling that Napster did not qualify for the transitory digital network communications safe harbor).

Napster does not stand for the proposition that service providers are required to block IP addresses to reasonably implement a repeat infringer policy. See, e.g., *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1145 (N.D. Cal. 2008) (explaining *Napster* and holding that a service provider need not seek to block IP addresses to reasonably implement its repeat infringer policy), citing *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1109-10 (9th Cir.), cert. denied, 522 U.S. 1062 (2007); see also *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 516 (S.D.N.Y. 2013) (following *Io Group* in rejecting the argument that a service provider did not reasonably implement its repeat infringer policy because it did not block IP addresses, where it blocked the email addresses of repeat infringers; "The *Io* court concluded that without testimony describing a more feasible or effective alternative, the defendant's policy of blocking a terminated user's e-mail account was reasonable."), *aff'd in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

In *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004), the Ninth Circuit ruled that there was a triable issue of fact on the issue of whether AOL satisfied the requirements of § 512(i) where, as a result of an error, AOL did not receive plaintiff's notification, and therefore took no action in response to it. AOL had changed the email address to which notifications could be sent in late 1999, but failed to close the old account or forward messages from that account to the new address, and failed to notify the Copyright Office of the new address for several months. The Ninth Circuit wrote that there was sufficient evidence for a reasonable jury to conclude that AOL had not reasonably implemented its policy of terminating repeat infringers because "AOL allowed notices of potential copyright infringement to fall into a vacuum and to go unheeded" *Ellison v. Robertson*, 357 F.3d 1072, 1080 (9th Cir. 2004). This ruling, of course, does not mean that AOL today could be alleged to have not reasonably implemented its policy simply because of an error in implementation that may have occurred in late 1999 and early 2000. *Ellison*, however, underscores that even unintentional mistakes in implementing a policy potentially could result in a service provider being denied the protections of the DMCA liability limitations if the error was significant enough to call into question the reasonableness of its implementation.

In *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077 (C.D. Cal. 2004), *aff'd in part on other grounds*, 488 F.3d 1102 (9th Cir.), cert. denied, 522 U.S. 1062 (2007), the district court had written that a service provider that receives repeat notifications that substantially comply with the requirements of 17 U.S.C.A. § 512(c)(3)(A) "about one of its clients but does not terminate its relationship with the client, has not reasonably implemented a repeat infringer policy." 340 F. Supp. 2d at 1088.

A service provider that in fact terminates subscribers and account holders upon receipt of a second DMCA notice (or discovery that the same user has posted, stored or transmitted a second or third file identified or believed to be infringing) would be deemed to “reasonably implement” its policy. The qualification that access by repeat infringers be terminated “in appropriate circumstances” suggests that a more lenient implementation—for example, a case-by-case analysis—could also be justified. As discussed below, courts have approved “three strikes” policies (consistent with America’s love of baseball) as well as policies that count notifications (which are submitted by a copyright owner under penalty of perjury) but not material removed based on knowledge or red flag awareness. In practice, some service providers will terminate access for some users on a first strike (when it is apparent that the user is engaged in piracy) or be more lenient where users genuinely seem to have made a mistake (or where the problem is a user of a subscriber or account holder, not the actual subscriber or account holder itself). The exact contours of what constitutes *reasonable implementation*, however, is still an evolving question.

For many years, case law construing the DMCA’s repeat infringer provisions largely was based on the Ninth Circuit’s opinion in *Perfect 10, Inc. v. CCBill, LLC*.¹⁰ The Second Circuit briefly addressed section 512(i) in *Viacom Int’l, Inc. v. YouTube, Inc.*,¹¹ but decided the issue on very narrow grounds. In *Viacom v. YouTube*, the Second Circuit rejected a challenge to YouTube’s repeat infringer policy based on YouTube’s provision of content identification tools to business partners, which allowed these business partners to proactively search the site for particular content. Plaintiffs had alleged that YouTube had not reasonably implemented its repeat infringer policy because it did not use its identification tools to search for plaintiffs’ works—only those of its business partners—and therefore allegedly sought to avoid identifying plaintiffs’ works. The Second Circuit, however, held that pursuant to section 512(m), service providers had no obligation to deploy search technology except to the extent that such monitoring constituted a “standard technical mea-

¹⁰*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

¹¹*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).

sure” within the meaning of section 512(i)¹² (which plaintiffs had not alleged).¹³ While refusing to accommodate or implement a standard technical measure may deprive a service provider of the protection of the DMCA safe harbors, “refusing to provide access to mechanisms by which a service provider affirmatively monitors its own network has no such result.”¹⁴ The Second Circuit panel emphasized that YouTube could not “be excluded from the safe harbor by dint of a decision to restrict access to its proprietary search mechanisms.”¹⁵

Subsequently, the Second Circuit, in *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*,¹⁶ in vacating an order granting summary judgment for the defendant and remanding the case for further consideration, held that a jury could infer a failure to reasonably implement a policy of terminating repeat infringers from evidence that it failed to “connect known infringing activity. . . [identified in] takedown notices to users who repeatedly created links to that infringing content . . . or who copied files from those links.”¹⁷ The court also held that evidence of a failure to reasonably implement a policy could be inferred from evidence that company executives were encouraged to and did personally use the service to link to or make copies of infringing material for personal use.¹⁸ *MP3Tunes*, however, largely turned on the inadequacy of the company’s policy, rather than reasonable implementation, since by definition a company would not be entitled to DMCA protection if it reasonably implemented a policy that was unreasonable.

By contrast, in *Ventura Content, Ltd. v. Motherless, Inc.*,¹⁹ the Ninth Circuit affirmed summary judgment for a small

¹²See *infra* § 4.12[3][C] (analyzing the standard technical measures provision).

¹³*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 40–41 (2d Cir. 2012).

¹⁴*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 41 (2d Cir. 2012).

¹⁵*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 41 (2d Cir. 2012).

¹⁶*EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79 (2d Cir. 2016).

¹⁷*EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 90–91 (2d Cir. 2016).

¹⁸*EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 90 (2d Cir. 2016).

¹⁹*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 615–17 (9th Cir. 2018).

service provider, whose policy was implemented by the company's sole owner, where reasonable implementation was found based on the owner's deposition testimony and evidence that between 1,320 and 1,980 users had been terminated, only nine of whom had slipped back on (suggesting "that less than one repeat infringer in 100,000 was missed"), and there was a "a paucity of proven failures to terminate."²⁰ Senior Judge Kleinfeld, writing for the majority, conceded that it was "tempting" to assume that the policy was not reasonably implemented because it depended on "little more than Lange's multifactor judgment based largely on his recollection of DMCA notices" and did not include either "a database of users whose uploads . . . generated DMCA notices and some automated means of catching them if they [did] it again[.]" but he explained that the statute did not require these things; "It modifies the termination requirement with the phrase 'appropriate circumstances' in

²⁰The court explained the service provider's sole owner's reasonable implementation as follows:

He testified that he excludes infringing material by looking for an identifying watermark in the corner, the usual way owners identify their copyrighted material. If he receives a DMCA takedown notice (the form designated in subsection (c)(3)(A)), he also uses "hashing" software so that copies of the image or clip will be removed and will be screened out if anyone tries to post them again. Ordinarily, he will not terminate a user because of one takedown notice, but he will if there are two or more, which is to say, "repeated" instances of infringement. He might make a "gut decision" to terminate a user after the first DMCA notice (that is, a user who is not a repeat infringer) if there are multiple infringing pictures or videos identified in the notice, though that is not his usual practice. Motherless has received over 3,000 DMCA takedown notices. Lange does not keep a written list of subscribers whose submissions generated DMCA notices, but he saves each of the takedown notices and can track the number of times each user's content has been deleted in response, as well as the date of and reason (e.g., copyright infringement, child pornography) for each deletion. In deciding to terminate a user, he considers the account's history, as well as his memory and judgment. He is especially careful to look for and screen out material from one producer who threatened to sue him for infringement.

Before removing a user, Lange considers multiple factors, as detailed above, including the number of complaints arising from the user's uploads, the amount of infringing content in the complaint he received, and whether he thinks the user had maliciously or intentionally uploaded infringing content. Lange testified at one point that Motherless had an automated system for removing repeat infringers, but he subsequently admitted that Motherless did not have such a system and may have confused it with Motherless's automatic removal of content when two or more people report it for violating the Terms of Use within a 24-hour period. Lange uses his judgment, not a mechanical test, to terminate infringers based on the volume, history, severity, and intentions behind a user's infringing content uploads. Ventura does not dispute this.

Ventura Content, Ltd. v. Motherless, Inc., 885 F.3d 597, 616-17 (9th Cir. 2018) (footnote omitted).

addition to the word ‘reasonable.’”²¹ In the context of a sole proprietorship, the majority considered this approach reasonable. Judge Kleinfeld emphasized that “[d]oubt that Motherless really does have a ‘policy’ of terminating repeat infringers that is ‘reasonably implemented’ is unavoidable in light of unsystematic and casual implementation. But doubt is not evidence.”²² Because the service provider met its burden of presenting evidence of reasonable implementation based on “[t]he absence of any significant number of repeat infringers who escaped termination . . .,” and the copyright owner did not controvert it, the court affirmed summary judgment for the service provider.²³

Unlike the majority, the dissenting judge in *Motherless*, Judge Rawlinson, would have reversed the entry of summary judgment for the service provider on the issue of reasonable implementation because there was no written policy to instruct an independent contractor, who worked for the sole owner, regarding repeat infringers, and the owner failed to articulate a consistent approach to terminations. The dissent asked rhetorically, “[w]ho can say with a straight fact that a “gut decisionmaking process” constitutes a policy? I certainly can’t.”²⁴ Judge Rawlinson also took issue with the “less than stellar, unautomated recordkeeping system used by Motherless.”²⁵ The dissent further considered it material that one of the largest repeat infringers was not terminated until after a fourth notice had been received.²⁶

²¹*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 618-19 (9th Cir. 2018).

²²*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 619 (9th Cir. 2018).

²³*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 618-19 (9th Cir. 2018). Justice Rawlinson, in dissent, had noted that files could be uploaded anonymously, which made it impossible to determine with precision who was or was not a repeat infringer, but the majority noted that 85% of uploads came from members who were identified and, more importantly, none of the 33 clips at issue had been uploaded by anonymous users. *See id.*

²⁴*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 621 (9th Cir. 2018) (Rawlinson, J. dissenting).

²⁵*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 621 (9th Cir. 2018) (Rawlinson, J. dissenting).

²⁶*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 622 (9th Cir. 2018) (Rawlinson, J. dissenting).

In *Perfect 10, Inc. v. CCBill, LLC*,²⁷ the Ninth Circuit, summarizing earlier district court case law, held that a service provider reasonably implements a repeat infringer policy if it “has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications,”²⁸ and if it terminates users when “appropriate.”²⁹ A limitation of the *Perfect 10* test—like any test based on a summary of earlier court holdings—is that it potentially may be both over-inclusive or under-inclusive in its reach. The fact patterns that by happenstance were litigated first may not accurately represent the universe of circumstances that are either *reasonable* or *unreasonable*. Nevertheless, once a test has been announced by a circuit court, there is a temptation for courts in later cases to apply it mechanically, rather than focusing specifically on the language of the statute.

What constitutes *reasonable implementation* may not be the same in every case, given the statutory requirement that repeat infringers be terminated “*in appropriate circumstances*.” What is appropriate in one instance may or may not be in another. What is clear, however, is that *reasonable implementation* does not mean 100% accuracy. Nor does it mean that a service provider should be subjected to a strict liability standard or to that of an insurer.

In *CCBill*, the Ninth Circuit separately analyzed “implementation” and “reasonable implementation,” focusing on the importance of adequate record keeping.³⁰ It found that the defendants met the statutory requirement for implementing their repeat infringement policy by maintaining a system for keeping track of potential repeat infringers, such as a log identifying infringers. The court rejected Perfect 10’s argument that there was a triable issue of fact based on the defendants’ failure to adequately keep track of infringers (as

²⁷*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

²⁸*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1109 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

²⁹*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1111 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

³⁰As noted in earlier editions of this chapter, “service providers should document and maintain records of all attempts to reasonably implement their policies so that they are not denied the benefits of the Act’s liability limitations.”

evidenced by missing or blank data in its logs) because only “a *substantial* failure to record webmasters associated with allegedly infringing websites may raise a genuine issue of material fact as to the implementation of the service provider’s repeat infringement policy.”³¹ While its records were incomplete (missing the names of some of the Webmasters), CCBill had “recorded most webmasters” and its DMCA log “indicate[d] that the email address and/or name of the webmaster [wa]s routinely recorded.”³²

With respect to the *reasonableness* of implementation, according to the Ninth Circuit, a “policy is unreasonable *only* if the service provider failed to respond when it had knowledge of the infringement.”³³ The court explained that “[t]o identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement.”³⁴ Indeed, in so holding, the Ninth Circuit expressly rejected Perfect 10’s argument that CCBill had implemented its repeat infringer policy in an unreasonable manner because infringing material remained on the site even after non-complying DMCA notices had been submitted identifying the works.³⁵

The Ninth Circuit went further, however, in conflating the specific requirements for complying with the user storage liability limitation of section 512(c) with the requirement under section 512(i) that a service provider reasonably implement its repeat infringer policy. To evaluate reasonable implementation of a repeat infringer policy, the panel ruled that it was necessary to also assess whether a service provider in fact had taken down material in response to substantially complying DMCA notifications both from the plaintiff *and* unrelated third parties *and* whether the service provider responded to “red flags” (involving any material—not merely the plaintiffs’). In theory, a service provider that

³¹*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1110 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007) (emphasis added).

³²*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1110–11 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

³³*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007) (emphasis added).

³⁴*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1111 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

³⁵*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1111 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

fails to adequately respond to *all* DMCA notifications and *all* red flags would not have adequate records of which of its users were repeat infringers. In practice, this approach puts at issue in discovery a service provider's entire record of compliance every time it is sued for infringement, at least where the user storage liability limitation is at issue.

In *CCBill*, the Ninth Circuit found Perfect 10's own notifications deficient³⁶ and therefore did not consider them in evaluating reasonable implementation of the defendants' repeat infringer policy. "Since Perfect 10 did not provide effective notice, knowledge of infringement may not be imputed to CCBill or CWIE based on Perfect 10's communications."³⁷

With respect to non-party notices, the court ruled that the service providers' "actions toward copyright holders who are not a party to the litigation are relevant in determining whether CCBill and CWIE reasonably implemented their repeat infringer policy." The panel explained that section 512(i)(1)(A) "requires an assessment of the service provider's 'policy,' not how the service provider treated a particular copyright holder." Although the Ninth Circuit held that a "policy is unreasonable only if the service provider failed to respond when it had knowledge of the infringement" it nonetheless remanded the case for further consideration because the district court had deemed third-party notices to be irrelevant and therefore declined to consider evidence of notices provided by any party other than Perfect 10.³⁸

The court likewise concluded that the service providers' response to "red flag" material was relevant to an evaluation of its repeat infringer policy. The court explained that "[i]n importing the knowledge standards of § 512(c) to the analysis of whether a service provider reasonably implemented its § 512(i) repeat infringer policy, Congress also imported the

³⁶See *infra* § 4.12[9].

³⁷*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

³⁸*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007). In *Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *8 (C.D. Cal. Jan. 16, 2015), District Court Judge Michael Fitzgerald ruled that where a service provider presents evidence to establish that its policy is reasonably implemented, a court need only consider the service provider's response to third party notices if that evidence is presented to the court by the copyright owner in admissible form.

‘red flag’ test of § 512(c)(1)(A)(ii)” and therefore may lose the benefit of the safe harbor if it fails to take action with regard to infringing material when it is aware of facts or circumstances from which infringing activity is apparent.”³⁹

In *Io Group, Inc. v. Veoh Networks, Inc.*,⁴⁰ a district court in the Ninth Circuit applying *CCBill* to a UGC video site held that the defendant, Veoh, had reasonably implemented its repeat infringer policy where it had a working notification system, often responded to DMCA notices the same day they were received (or at most within a few days), upon receipt of a second DMCA notice it terminated the account of the affected user and disabled *all* content posted by that user (not just the material at issue in the DMCA notice) and blocked the user’s email address so that a new account could not be established using the same address and Veoh generated a hash file or digital fingerprint for each video and thereby prevented additional identical files from ever being uploaded to the site.⁴¹

In so ruling, Judge Howard R. Lloyd, following *Corbis Corp. v. Amazon.com*⁴² (which is discussed below), rejected the argument that Veoh’s policy was faulty because it did not prevent repeat infringers from reappearing on Veoh’s site under a pseudonym, using a different email address. He also clarified “[t]o identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringers.”⁴³ The “hypothetical possibility that a rogue user might reappear under a different user name and identity does not raise a genuine fact issue as to the implementation of Veoh’s policy.”⁴⁴ In that case, the plaintiff in fact had presented no evidence that any repeat

³⁹*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113–14 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007). The court concluded that the defendants in *CCBill* had not ignored red flag material. Knowledge and red flag awareness are separately addressed in section 4.12[6][C].

⁴⁰*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

⁴¹Veoh had asserted that it had terminated 1,096 users as repeat infringers since the time its site launched, which was not challenged by the plaintiff.

⁴²*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

⁴³*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1144 (N.D. Cal. 2008) (*italics in original*).

⁴⁴*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1144

infringers in fact had gotten back on to the service.

The court in *Io Group, Inc. v. Veoh Networks, Inc.*, also expressly rejected the notion that Veoh should have sought to block IP addresses associated with repeat infringers. Although the court noted that in an unreported decision in *A&M Records, Inc. v. Napster, Inc.*,⁴⁵ Chief Judge Marilyn Patel of the Northern District of California had found that Napster had not reasonably implemented its repeat infringer policy because it did not block the IP addresses associated with infringers, Judge Lloyd wrote that *Napster* was readily distinguishable. He explained that in *Napster*, there was evidence that the defendant was not only capable of blocking IP addresses but in fact had done so for certain users. Judge Lloyd noted that while it was undisputed that IP addresses identified particular *computers* there was no evidence that Veoh could identify particular *users*. “More to the point,” he wrote, “section 512(i) does not require service providers to track users in a particular way to or affirmatively police users for evidence of repeat infringement.”⁴⁶

The reasonableness of Veoh’s implementation of its repeat infringer policy was also considered in *UMG Recordings, Inc. v. Veoh Networks, Inc.*,⁴⁷ in which Judge Matz rejected UMG’s argument that Veoh had failed to reasonably implement its policy because Veoh did not automatically terminate users whose videos were blocked from being uploaded to its UGC site by Audible Magic filters.⁴⁸ The district court, however, concluded that Audible Magic filters do “not meet the standard of reliability and verifiability required by the

(N.D. Cal. 2008).

⁴⁵*A&M Records, Inc. v. Napster, Inc.*, No. C 99–05183 MHP, 2000 WL 573136 (N.D. Cal. May 12, 2000).

⁴⁶*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1145 (N.D. Cal. 2008), citing *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1109–10 (9th Cir.), cert. denied, 522 U.S. 1062 (2007); see also *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 516 (S.D.N.Y. 2013) (following *Io Group* on this same point in rejecting the argument that a service provider did not reasonably implement its repeat infringer policy because it did not block IP addresses), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁴⁷*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009), *aff’d on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁴⁸Audible Magic video filters—and filtering technologies in general—are discussed in section 17.05.

Ninth Circuit to justify terminating a user's account."⁴⁹ Judge Matz wrote that identification by the Audible Magic filter lacks the reliability of a sworn declaration. The court noted that there was no way for Veoh to verify the information provided or evaluate Audible Magic's process for compiling the database. Indeed, Veoh had asked Audible Magic for the contact information of claimants for works identified by its filter so that Veoh could implement a counter notification procedure but Audible Magic turned down that request.

Judge Matz also rejected the argument that Veoh had not reasonably implemented its policy because it did not necessarily terminate users who had uploaded multiple infringing works that were identified in a single DMCA notification. Veoh sent users a warning notice when it received a notification (or terminated users who had received two prior notifications) without regard to the number of allegedly infringing videos identified in a given notice. Judge Matz concluded that this approach was reasonable, noting that even a DMCA notice is "not the *sine qua non* of copyright liability . . . A copyright owner may have a good faith belief that her work is being infringed, but may still be wrong."⁵⁰

Finally, the court approved Veoh's policy of terminating repeat infringers who had been the subject of two prior notifications given that the term "repeat infringer" is not defined in the statute and the legislative history suggests an intent to leave the policy requirements and subsequent obligations of service providers loosely defined.⁵¹

Reasonable implementation of a repeat infringer policy was also considered in *Corbis Corp. v. Amazon.com, Inc.*,⁵² a district court opinion that pre-dated *CCBill* which was cited

⁴⁹*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1116 (C.D. Cal. 2009), *aff'd on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁵⁰*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1117 (C.D. Cal. 2009) (quoting *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1105 (W.D. Wash. 2004)), *aff'd on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁵¹*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009) (quoting *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1100–01 (W.D. Wash. 2004)), *aff'd on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁵²*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash.

approvingly by the Ninth Circuit in that case. In *Corbis Corp. v. Amazon.com*, Judge Robert Lasnik of the Western District of Washington ruled that Amazon.com was shielded from liability for damages for its zShops platform (which allowed individuals and retail vendors to showcase their own products and sell them directly to online consumers),⁵³ rejecting plaintiffs' argument that Amazon.com's policies were too vague to satisfy the requirements of the statute.

Corbis had argued that Amazon.com's user policies did not include the term "repeat infringer" or describe the methodology employed in determining which users would be terminated as repeat infringers. The court ruled, however, that the open-ended language used in section 512(i)—such as the absence of a definition of "repeat infringer"—when contrasted with the very specific requirements set forth elsewhere in section 512 (such as those in section 512(c) relating to notifications and takedown requirements to comply with the user storage liability limitation) underscores that a user policy need not be as specific as Corbis had argued. "Given the complexities inherent in identifying and defining online copyright infringement, section 512(i) does not require a service provider to decide, *ex ante*, the specific types of conduct that will merit restricting access to its services."⁵⁴ The fact that *Amazon.com* did not use the term "repeat infringer" or

2004).

⁵³Vendors sold their products on zShops by creating Web pages, known as "listings," and paying Amazon.com \$39.99 plus a percentage of all sales (ranging between 2.5% and 5%). If vendors chose to offer buyers the option to pay by credit card, Amazon.com required vendors to use its services for processing credit card transactions. If a product was paid for by another means, Amazon.com had no involvement in the transaction. Vendors entered into a Participation Agreement with Amazon.com, which prohibited the sale of infringing items and bound users to various policies including Community Rules, which further prohibited the sale of infringing items. Amazon.com further reserved the right, but did not undertake the obligation, to monitor any activity and content associated with the site. *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1094–95 (W.D. Wash. 2004). When Amazon.com received information that a vendor could be infringing another's copyrights, its practice had been to cancel the allegedly infringing listing and notify the vendor by email of the cancellation, providing a contact email address for the complaining party and reminding the vendor that "repeat violations of our Community Rules could result in permanent suspension from our Auction, zShops, and Amazon Marketplace sites." *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1095 (W.D. Wash. 2004).

⁵⁴*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1101 (W.D. Wash. 2004).

track the exact language of the statute was immaterial because its policies adequately conveyed the message to users that there was a realistic threat that those who repeatedly or flagrantly abused their access through disrespect for the intellectual property rights of others would lose their access.

Judge Lasnik also rejected Corbis's argument that *Amazon.com* had not adequately communicated its termination policy to users because, in addition to the policies set forth in its Participation Agreement and Community Rules, it had an internal policy that had not been communicated to users, which set forth the criteria for determining when to terminate a user's access to the site. He wrote that "section 512(i) . . . is not so exacting. Amazon need only inform users that, in appropriate circumstances, it may terminate the user's accounts for repeated copyright infringement."⁵⁵ The court held unequivocally that "[t]he statute does not suggest what criteria should be considered by a service provider, much less require the service provider to reveal its decision-making criteria to the user."⁵⁶

Corbis further had challenged *Amazon.com*'s reasonable implementation of its policy, arguing, among other things, that *Amazon.com*'s policy had not been able to prevent certain vendors from reappearing on the zShops platform under pseudonyms after being terminated as repeat infringers, even though *Amazon.com*'s policies prohibited vendors from opening new accounts after an account had been terminated. In rejecting this argument, with respect to a repeat infringer named Posternow, the court wrote that:

Although this type of behavior is understandably vexing for a copyright holder like Corbis, it is not clear how Posternow's efforts to sidestep Amazon's policies amount to a failure of implementation. Corbis has not alleged that Amazon intentionally allowed Posternow to open a zShops account or suggested that a more effective means of denying Posternow's access could have been implemented by Amazon.⁵⁷

Judge Lasnik held that "[a]n infringement policy need not

⁵⁵*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1102 (W.D. Wash. 2004).

⁵⁶*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1102 (W.D. Wash. 2004).

⁵⁷*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1103 (W.D. Wash. 2004).

be perfect; it need only be reasonably implemented.”⁵⁸

Corbis further argued that *Amazon.com* tolerated flagrant or blatant copyright infringement, based on its conduct with respect to two users. The court noted that because a service provider such as *Amazon.com* “does not have an affirmative duty to police its users, failure to properly implement an infringement policy requires a showing of instances where a service provider fails to terminate a user even though it has sufficient evidence to create actual knowledge of that user’s blatant repeat infringement of a willful and commercial nature.”⁵⁹ Corbis presented evidence that *Amazon.com* received three emails about one of the problem vendors and seven emails about the other, but the court ruled that these examples did not constitute evidence that *Amazon.com* had knowledge of blatant, repeat infringement, such that it would have been required to terminate access to the vendor’s zShops locations. In the words of the court, “[a]lthough the notices have brought the listings to Amazon’s attention, they did not, in themselves, provide evidence of blatant copyright infringement.”⁶⁰ Indeed, Judge Lasnik wrote that “even if Amazon acted unreasonably when it failed to terminate Posternow, that unreasonable act is not the equivalent of having actual knowledge that Posternow was engaged in blatant repeat infringement. Actual knowledge of repeat infringement cannot be imputed merely from the receipt of notices of infringement.”⁶¹ Stated differently, “[w]ithout some evidence from the site raising a red flag, Amazon would not know enough about the photography, the copyright owner, or the user to make a determination that the vendor was engaging in blatant copyright infringement.”⁶²

Summarizing *Corbis*, the court in *Rosen v. eBay, Inc.*⁶³ explained that section 512(i) “does not require that a service

⁵⁸*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1103 (W.D. Wash. 2004).

⁵⁹*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1104 (W.D. Wash. 2004).

⁶⁰*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1105 (W.D. Wash. 2004).

⁶¹*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1105 (W.D. Wash. 2004).

⁶²*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1106 (W.D. Wash. 2004).

⁶³*Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *8-9 (C.D. Cal. Jan. 16, 2015) (granting summary judgment for eBay on

provider reveal its decision-making criteria to its users . . . ,” that “implementation of the policy ‘need only put users on notice that they face exclusion from the service if they repeatedly violate copyright laws’ ” and that “the implementation of a policy need not be perfect to render it sufficient to qualify a service provider for protection under § 512(c).”⁶⁴

In *Capitol Records, LLC v. Vimeo, LLC*,⁶⁵ Judge Ronnie Abrams of the Southern District of New York declined to find that a video hosting site failed to reasonably implement its repeat infringer policy in the early years of its existence because its policy, and implementation, improved over time as the site grew and the size of its in-house staff expanded. Vimeo, a video sharing platform intended for original videos, began operations in 2004, at which time it required users to agree to its Terms of Service, which contained language stating that users would not use the website to infringe any copyright or other proprietary rights and warned users that it reserved the right to remove videos and terminate user accounts for violation of its Terms. As early as 2007, Vimeo actually disabled user accounts upon discovery of infringing activity. Since at least May 5, 2008, the Terms also warned expressly that Vimeo would “terminate rights of subscribers and account holders in appropriate circumstances if they are determined to be repeat infringers.” From around the time of its inception through mid-2008, Vimeo received approximately five or fewer takedown notices per month. At some point in time (the exact date was unclear), Vimeo adopted a “three strikes” policy, pursuant to which it would terminate a user’s account if the user became the subject of three separate, valid takedown notices and it would add the terminated user’s email address to a list of banned addresses that would be blocked from opening new accounts. Any video removed pursuant to a takedown notice was placed on a “blocked video” list, which prevented other Vimeo users from re-uploading the same video. In addition to removing material identified in a notice, when a notice was received Vimeo also reviewed the other videos in the same account of the user who uploaded the allegedly infringing item to look for other

its entitlement to the DMCA safe harbor).

⁶⁴*Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *8 (C.D. Cal. Jan. 16, 2015), quoting *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1102 (W.D. Wash. 2004).

⁶⁵*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

potential Terms of Use violations. Pursuant to its policy, notices received within three days of one another were treated as a single instance of infringement. In October 2008, Vimeo also began using a “Purgatory Tool,” which facilitated the tracking of repeat infringers by collecting and maintaining all videos and accounts removed from the website, including those removed due to DMCA notices. A video placed in “Purgatory” was no longer accessible to anyone other than Vimeo employees with “Moderator status.” When a user’s account was placed in purgatory, all videos uploaded by that same user are automatically placed in Purgatory.

The court found that Vimeo reasonably implemented its repeat infringer policy, rejecting the argument that its later practices evidenced that earlier on Vimeo had not reasonably implemented its policy. Judge Abrams explained that:

In its nascent years, Vimeo employees identified repeat infringers by reviewing e-mail records or recalling the names of users previously implicated in a takedown notice [U]ser accounts violating the Terms of Service “were often terminated upon the receipt of the first DMCA takedown notice,” . . . and as early as June 2007, Vimeo disabled user accounts upon discovery of infringing conduct This evidence establishes that Vimeo reasonably implemented its policy from the beginning.

The Court’s finding of reasonableness is also informed by the evidence of Vimeo’s business circumstances as they evolved during the relevant period. That is, the policies Vimeo implemented in the first several years of its operation, as described above, were reasonable ones in light of the fact that Vimeo was, at the time, a small service provider, the twenty full-time employees of which were tasked with processing only a trickle (zero to five) of takedown requests per month. The evidence reflects that as the flow of those requests increased, Vimeo’s policy became more robust—first in the form of a “three strikes” rule and a blocked video list, implemented at some point after Vimeo’s inception, and eventually in the form of the “Purgatory” tool, implemented later in October 2008. That Vimeo’s enforcement mechanisms advanced in step with the realities of its growing business further supports the reasonableness of its implementation system.⁶⁶

Summarizing earlier case law, the court in *Vimeo* explained that a substantial failure to record infringers may raise a genuine question of material fact on the issue of rea-

⁶⁶See *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 514–15 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

sonable implementation. In addition, implementation will be found unreasonable where notices of potential copyright infringement fall into a vacuum and go unheeded, where a site teaches users how to encrypt copyrighted works to avoid detection or where a site in fact fails to terminate users who repeatedly or blatantly infringe third-party copyrights,⁶⁷ among other things.

Potential defects in Vimeo's implementation of its repeat infringer policy were dismissed by Judge Abrams as either legally irrelevant under the DMCA or not rising to the level of a substantial failure. With respect to legal arguments, the court rejected plaintiff's contention that Vimeo failed to reasonably implement its repeat infringer policy because it only blocked the email addresses of repeat infringers, not their IP addresses.⁶⁸ The court also rejected the argument that Vimeo's implementation was inadequate because it treated all notices received within a three-day period as a single instance of infringement.⁶⁹

Plaintiffs further challenged Vimeo's reasonable implementation based on the deposition testimony of a Vimeo "Community Director" who expressed ignorance about Vimeo's list of banned users or "blocked video list" and who did not know who was responsible for identifying repeat infringers. The court characterized the testimony as reflecting a "troubling ignorance of Vimeo's tools for terminating infringing activity" but considered it to amount to no more than "isolated comments" rather than a "substantial failure" by Vimeo to reasonably implement its repeat infringer policy.⁷⁰ Like Judge Lasnik in *Amazon.com*, Judge Abrams emphasized

⁶⁷See *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 514 (S.D.N.Y. 2013), *aff'd in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁶⁸See *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 516 (S.D.N.Y. 2013) (following *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1143–45 (N.D. Cal. 2008)), *aff'd in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁶⁹See *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 516 (S.D.N.Y. 2013), *aff'd in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁷⁰See *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 515 (S.D.N.Y. 2013) ("even assuming one could infer from Verdugo's apparent ignorance of aspects of Vimeo's tools for terminating infringement that Vimeo's overall implementation of its policy was affected in some way, such isolated comments, while certainly unfortunate, do not reflect the sort of "substantial failure," see *CCBill*, 488 F.3d at 1110, that courts have held gives rise to a genuine dispute as to the reasonableness of a repeat infringer policy."), *aff'd in part on other grounds*, 826 F.3d 78 (2d Cir.

that “[i]mplementation . . . need not be perfect. Rather, by the terms of the statute, it need only be ‘reasonable.’”⁷¹

Reasonable implementation likewise was found by the district court in *Hempton v. Pond5, Inc.*,⁷² despite the fact that a user who was terminated as a repeat infringer signed up again under a different user name, using the same IP address and PayPal account as the previously-terminated user, because there was no evidence that the service provider in fact was aware of these details and the DMCA does not require a service provider to affirmatively investigate.

Reasonable implementation also has been found in other cases.⁷³

By contrast, in *Capitol Records, LLC v. Escape Media Group, Inc.*,⁷⁴ Southern District of New York Judge Allison Nathan, affirming the report and recommendation of Magistrate Judge Sarah Netburn, entered summary judgment in favor of Capitol Records and against Escape Media over the latter’s operation of the Grooveshark music service for both federal and common law copyright infringement based on the finding that Escape Media did not reasonably implement a repeat infringer policy and therefore did not meet the

2016).

⁷¹See *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 515 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁷²*Hempton v. Pond5, Inc.*, Case No. 3:15-cv-05696-BJR, 2016 WL 6217113, at *7-8 (W.D. Wash. Oct. 25, 2016).

⁷³See, e.g., *Kinsley v. Udemy, Inc.*, Case No. 19-cv-04334-JSC, 2021 WL 1222489, at *2 (N.D. Cal. Mar. 31, 2021) (granting summary judgment for Udemy on its DMCA defense; “Udemy satisfies this requirement. Its ‘Instructor Copyright Ban Policy’ bans instructor accounts where an instructor ‘represents a high risk of additional infringements,’ and presumes a ‘high risk of additional infringement . . . when there has either been a material violation [of the policy], cases of impersonation, and repeated non-material violations.’ . . . The policy lays out Udemy’s consequences for copyright infringement and its investigative processes regarding possible infringements and has been in place since 2015. . . . Udemy’s ‘Intellectual Property Policy’ also informs its users that any instructor deemed to be a ‘repeat infringer’ shall have their courses removed. . . . These documents clearly ‘inform subscribers of [Udemy’s] policy of terminating repeat infringers in appropriate circumstances.’ *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 615–16 (9th Cir. 2018) (internal quotation marks omitted). Furthermore, Udemy terminated the accounts of the instructors who posted the content infringing on Mr. Kinsley’s copyrights.”).

⁷⁴*Capitol Records, LLC v. Escape Media Group, Inc.*, No. 12-CV-6646 (AJN), 2015 WL 1402049, at *6-13, 44-58 (S.D.N.Y. Mar. 25, 2015).

requirements for the DMCA safe harbor. In *Escape Media*, the defendant claimed to have a one strike policy, to justify its failure to retain any records of terminating repeat infringers. Escape Media argued that there could be no repeat infringers given its policy. In fact, however, 1,609 users received DMCA takedown notices for an upload that occurred *after* the user had already received a prior DMCA takedown notice. Moreover, 21,044 Grooveshark users who had received multiple DMCA takedown notices accounted for 7,098,634 uploads, or nearly 35% of all uploads on the site. Further, Escape Media had adopted a “DMCA Lite” procedure pursuant to which it did not treat defective notices as justifying a strike pursuant to its one strike policy. The evidence showed, however, that since February 2013 94.2% of takedowns were pursuant to this procedure. Judge Nathan questioned whether all of those notices could be so defective that Escape Media was still able to identify and remove the material at issue. The more reasonable inference is that this procedure allowed Escape Media to avoid having to terminate repeat infringers.

In *Datatech Enterprises LLC v. FF Magnat Ltd.*,⁷⁵ Judge Charles Breyer of the Northern District of California ruled, in connection with declining to dissolve a preliminary injunction, that the defendant was unlikely to prevail on its DMCA defense based on evidence that it had ignored copyright holders’ requests to remove specifically identified repeat infringers, including one individual who uploaded 1,600 separate copies of an infringing work.

In *Perfect 10, Inc. v. Giganews, Inc.*,⁷⁶ the court denied summary judgment to the defendant on its entitlement to the DMCA defense because the fact that Giganews had terminated only 46 people as repeat infringers since 2008, despite having removed more than 531 million infringing messages just in the preceding year, created at least a possible inference that it had not reasonably implemented its repeat infringer policy (although the court made clear that this inference was not necessarily compelled by the

⁷⁵*Datatech Enterprises LLC v. FF Magnat Ltd.*, No. C 12-04500 CRB, 2013 WL 1007360, at *5–6 (N.D. Cal. Mar. 13, 2013).

⁷⁶*Perfect 10, Inc. v. Giganews, Inc.*, 993 F. Supp. 2d 1192 (C.D. Cal. 2014).

evidence).⁷⁷

In *Disney Enterprises, Inc. v. Hotfile Corp.*,⁷⁸ Judge Kathleen M. Williams of the Southern District of Florida held that Hotfile, a heavily trafficked offshore file storage site, was not entitled to the DMCA user storage safe harbor where it failed to reasonably implement its repeat infringer policy—and indeed, largely ignored it except in cases where Hotfile was directly threatened with litigation—at least prior to being sued by Disney and the other motion picture studio plaintiffs. In granting the plaintiffs’ motion for partial summary judgment on the issue of Hotfile’s entitlement to the DMCA affirmative defense, the court ruled that the number of notices of infringement sent to Hotfile “indicated to Hotfile that a substantial number of blatant repeat infringers made the system a conduit for infringing activity. Yet Hotfile did not act on receipt of DMCA notices and failed to devise any actual policy of dealing with those offenders, even if it publicly asserted otherwise.” Hotfile’s designated Rule 30(b)(6) corporate representative testified that Hotfile in fact did not keep track of who was or was not a repeat infringer, even though it would have been easy to do so. Despite receiving over eight million notices for five million users, Hotfile only terminated 43 users before being sued by Disney and the other studio plaintiffs—and of those, 33 were terminated in response to a TRO issued in another lawsuit and the others were terminated in response to express threats to take legal action. Most glaringly, the court wrote, there were 61 users who had accumulated more than 300 notices each. Indeed, by the time the lawsuit had been filed, 24,790 Hotfile users had accumulated more than three notices, “half of those had more than ten notices; half again had 25 notices; 1,217 had 100 notices; and 61 had more than 300 notices.” One single user, who had been suspended but then allowed back on after he contacted Hotfile, had uploaded nearly 30,000 files to Hotfile and accumulated 9,254 takedown notices.

⁷⁷*Perfect 10, Inc. v. Giganews, Inc.*, 993 F. Supp. 2d 1192, 1197 (C.D. Cal. 2014). Giganews ultimately prevailed on the merits on plaintiffs’ claims for direct infringement, contributory infringement, inducement, or vicarious liability, which was affirmed on appeal. *See Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657 (9th Cir. 2017).

⁷⁸*Disney Enterprises, Inc. v. Hotfile Corp.*, Case No. 11-20427-Civ, 2013 WL 6336286 (S.D. Fla. Order Granting in Part and Denying in Part Cross-Motions for Summary Judgment Sept. 20, 2013).

The potential importance of a repeat infringer policy to deterring infringement was illustrated by the fact that while those who were the subject of more than three infringement notices made up less than one percent of all Hotmail users, they were responsible for posting 50 million files (15.6 million of which were subsequently the subject of a takedown notice or removed for infringement), representing 44 percent of all files ever uploaded to Hotfile.

The court acknowledged that Hotfile had made many improvements since being sued, but declined to rule on Hotfile's cross-motion for partial summary judgment on its entitlement to the safe harbor for post-litigation conduct based on the plaintiffs' representation at oral argument that they only sought damages for infringement pre-dating the lawsuit. Judge Williams noted in *dicta*, however, that Hotfile's request had raised questions such as whether a party can ever regain the protections of the DMCA and whether the court could trust Hotfile not to revert to its prior offending conduct (as well as how the court would be able to determine an exact point at which Hotfile began implementing a DMCA-compliant policy).

Hotfile and *Escape Media* illustrate the potential importance of discovery to copyright owners in seeking to overcome a service provider's contention that it reasonably implemented its repeat infringer policy. Given the potentially broad scope of discovery that could be permitted on the issue of reasonable implementation based on the Ninth Circuit's conclusion in *CCBill* that treatment of "red flag" material is relevant to reasonable implementation (at least in cases involving the user storage safe harbor and, by extension, presumably the information location tools safe harbor), service providers must be careful to preserve relevant evidence of all material removed and all communications that arguably could evidence a failure to respond in response to knowledge, notice or red flag awareness.

In *Arista Records LLC v. Usenet.com, Inc.*,⁷⁹ Judge Harold Baer, Jr., of the Southern District of New York imposed an evidentiary sanction on a service provider and other defendants for bad faith spoliation of documents and other evasive

⁷⁹*Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124 (S.D.N.Y. 2009). Magistrate Judge Katz's earlier recommendation may be found at *Arista Records LLC v. Usenet.com, Inc.*, 608 F. Supp. 2d 409 (S.D.N.Y. 2009).

tactics that prevented the plaintiffs from conducting discovery on the defendants' compliance with the requirements of the DMCA. In precluding the defendants from raising the DMCA as a defense in plaintiffs' suit for copyright infringement, Judge Baer wrote that "if defendants were aware of such red flags, or worse yet, if they encouraged or fostered such infringement, they would be ineligible for the DMCA's safe harbor provisions."⁸⁰ Although evidentiary sanctions were imposed in *Usenet.com* for spoliation of evidence that effectively prevented the service provider from challenging plaintiffs' contention that it had notice, knowledge or red flag awareness of infringing activity, they could just as easily have been imposed for failing to preserve evidence relevant to reasonable implementation of the service provider's repeat infringement policy in the Ninth Circuit under *CCBill*, given the Ninth Circuit's analysis in that case that evidence of a service provider's response to red flag material is relevant to assessing its reasonable implementation of its repeat infringement policy. The issue of spoliation and the DMCA is addressed further in section 4.12[18].

4.12[3][C] Standard Technical Measures

Service providers, as a prerequisite to being eligible to benefit from one of the four safe harbors set forth in sections 512(a), 512(b), 512(c) and 512(d), must accommodate and not interfere with "standard technical measures," which are defined in the Act as technical measures used by copyright owners to identify or protect their works.¹ Service providers whose systems interfere with certain anti-piracy technologies therefore potentially could be unable to benefit from the liability limitations and exemption established by the DMCA.

Not all anti-piracy technologies will fall within the scope

⁸⁰633 F. Supp. 2d at 142. In that case, the defendants had wiped clean seven hard drives that belonged to employees without backing up the data to a central server, and failed to adequately preserve email communications. The defendants also sent potentially key witnesses to Europe during the height of discovery to "engineer their unavailability," encouraged witnesses to evade process, provided evasive or false sworn statements and violated two court orders requiring them to present information regarding the despoiled computer evidence, although Judge Baer concluded that while these abuses were not sufficient on their own to justify terminating sanctions they supported the finding that sanctions for discovery abuse were warranted.

[Section 4.12[3][C]]

¹17 U.S.C.A. § 512(i)(2).

of the Act. Indeed, it is unclear whether there are *any* technologies that presently constitute “standard technical measures.” To qualify as a “standard technical measure,” the technical measure must “have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process.”² In addition, the technical measure must be available to any person on reasonable and nondiscriminatory terms and must not impose substantial costs on service providers or substantially burden their systems or networks.³

In discussing analogous “industry standard communications protocols and technologies” in the context of the systems caching limitation, the House Report accompanying the final bill states that Congress expected “that the Internet industry standards setting organizations, such as the Internet Engineering Task Force and the World Wide Web Consortium, will act promptly and without delay to establish these protocols.” However, this never happened.⁴ As noted by one court, “[t]here is no indication that the ‘strong urging’ of both the House and Senate committees reporting on this bill has led to ‘all of the affected parties expeditiously [commencing] voluntary, interindustry discussions to agree upon and implement the best technological solutions available to achieve these goals.’”⁵

Although “standard technical measures,” by definition, must be accepted by a broad consensus of copyright owners and service providers—and not merely Internet standard setting bodies—paradoxically service providers are not given any apparent incentive under the Act to cooperate with content owners to achieve such a consensus.

In *Perfect 10, Inc. v. CCBill, LLC*,⁶ the Ninth Circuit found that the issue of a defendant’s compliance with standard technical measures constituted a disputed fact precluding

²17 U.S.C.A. § 512(i)(2)(A).

³17 U.S.C.A. §§ 512(i)(2)(B), 512(i)(2)(C).

⁴The Secure Digital Music Initiative (SDMI) represented an effort to develop a standard technical measure, but it was unsuccessful in achieving a broad consensus of copyright owners and service providers.

⁵*Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1174 (C.D. Cal. 2002), quoting H.R. Rep. 105-551(II), at 61; S. Rep. at 52 (1998).

⁶*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

summary judgment on the question of entitlement to the DMCA user storage safe harbor. In that case, the plaintiff had argued that one of the defendants interfered with “standard technical measures” by blocking plaintiff’s access to its affiliated websites to prevent it from discovering whether those sites infringed plaintiff’s copyrights. The defendant had argued that it merely blocked access because the plaintiff signed up for subscriptions that it then canceled, causing the defendant to incur credit card charge-back and other fees.

The Ninth Circuit panel directed the district court to determine whether accessing websites is a standard technical measure and if so whether CCBill interfered with that access. The court wrote that “[i]f CCBill is correct, Perfect 10’s method of identifying infringement—forcing CCBill to pay the fines and fees associated with chargebacks—may well impose a substantial cost on CCBill. If not, CCBill may well have interfered with Perfect 10’s efforts to police the websites in question for possible infringement.”⁷

While these points may be relevant to DMCA implementation in some way—and potentially go to the question of *reasonable implementation* of a repeat infringer policy under the Ninth Circuit test articulated in *CCBill* itself⁸—they do not relate to “a standard technical measure” which, by definition, is a technical standard (such as a filtering or a DRM standard) developed pursuant to a broad consensus of copyright owners and service providers, which did not exist in 1998. The Ninth Circuit’s analysis on this point is simply incorrect.

In *Capitol Records, LLC v. Vimeo, LLC*,⁹ plaintiffs had argued that a service provider’s privacy settings prevented copyright owners from collecting information needed to issue takedown notices. The court ruled, however, that privacy settings do not constitute interference with standard technical measures.

The Second Circuit subsequently ruled that metadata contained on photographs does not constitute a standard

⁷*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1115 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

⁸*See supra* § 4.12[3][B][iv].

⁹*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 517 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

technical measure, in a case where the copyright owner had argued that a service's practice of stripping out metadata when user images were uploaded to the site interfered impermissibly with standard technical measures and should have disqualified it from DMCA safe harbor protection.¹⁰

In *Ventura Content, Ltd. v. Motherless, Inc.*,¹¹ a Ninth Circuit panel explained, in *dicta*, that standard technical measures “enable copyright owners to establish some technical means so that service providers can spot and exclude infringing material without substantial expense. One can imagine a digital version of the old c in a circle (©) automati-

¹⁰See *BWP Media USA Inc. v. Polyvore, Inc.*, 922 F.3d 42, 44 (2d Cir. 2019) (“BWP has not shown that Polyvore’s stripping of metadata disqualifies it from safe harbor protection”); see also *id.* at 55-57 (Walker, J. concurring) (providing the rationale for the panel’s *per curiam* ruling). In so ruling, the court disagreed with *Gardner v. CafePress Inc.*, No. 3:13-cv-1108-GPC-JMA, 2014 WL 794216, at *6 (S.D. Cal. Feb. 26, 2014) (finding a factual dispute precluding summary judgment on the issue of whether stripping metadata containing copyright information from photographs interfered with a standard technical measure).

Judge Walker rejected the argument that because courts have considered metadata to qualify as copyright management information under the anti-circumvention provisions of the DMCA, 17 U.S.C.A. § 1202 (*infra* § 4.21), metadata should be considered a standard technical measure under 17 U.S.C.A. § 512(i)(2), because the term *standard technical measure* is expressly defined in section 512. 922 F.3d at 57 (Walker, J. concurring), quoting *Stenberg v. Carhart*, 530 U.S. 914, 942 (2000) (“When a statute includes an explicit definition, we must follow that definition”). Judge Walker explained that “there is no indication in § 512(i) that Congress intended that items that courts find to be ‘copyright management information’ for § 1202 purposes somehow count as ‘standard technical measures’ for § 512(i) purposes.” 922 F.3d at 57 (Walker, J. concurring), citing *Burgess v. United States*, 553 U.S. 124, 130 (2008).

Judge Walker reiterated that although Polyvore had the burden of proving its entitlement to the DCMA affirmative defense, BWP, as the party asserting that metadata was a standard technical measure, had the burden of proving it. See 922 F.3d at 56-57 n.9 (Walker, J. concurring). He also emphasized an important point made in this treatise for many years:

Congress did not leave it to the courts to simply pronounce out of thin air that a given technical measure has become a “standard” in the industry such that interfering with it prevents an ISP from claiming the protection of the § 512(c) safe harbors. It is plain from § 512(i) itself that such a pronouncement can only come from “a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process.” 17 U.S.C. § 512(i)(2)(A). I see nothing to show, to date, that such a consensus or such a process has developed.

922 F.3d at 57 (Walker, J. concurring).

¹¹*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 614-15 (9th Cir. 2018).

cally triggering the uploading software to exclude material so marked by the copyright owner.”¹² The service provider’s compliance with standard technical measures in fact was not at issue in *Motherless*. The court observed that it was undisputed “that Ventura did not in any way mark its material so that infringement could be spotted and the material excluded by some standard technical measure.”¹³

Other courts have fudged the issue and found that service providers have not interfered with standard technical measures without actually assessing whether a particular practice in fact could constitute a “standard technical measure” based on the high standard set by Congress for characterizing a technology as a standard technical measure. For example, in *Wolk v. Kodak Imaging Network, Inc.*,¹⁴ the court held that Photobucket’s provision of editing tools did not interfere with standard technical measures and therefore did not disqualify it from safe harbor eligibility. In that case, the plaintiff had argued that Photobucket editing tools could be used to remove watermarks. Without analyzing whether watermarks in fact constitute standard technical measures, the court held that the fact that watermarks appear suggested that Photobucket accommodates standard technical measures and the fact that users, not Photobucket, use editing tools to attempt to circumvent copy protection measures already on the site did not disqualify Photobucket.¹⁵

4.12[4] Transitory Digital Network Communications

A service provider that meets the threshold prerequisites for eligibility set forth in subsection 4.12[3] may, under certain circumstances, limit its liability for copyright infringement for “transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for . . . [it,] or by reason of the intermediate or transient storage of that material in the course of such

¹²*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 615 (9th Cir. 2018).

¹³*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 614-15 (9th Cir. 2018).

¹⁴*Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724 (S.D.N.Y. 2012), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014).

¹⁵*See Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 745 (S.D.N.Y. 2012), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014).

transmitting, routing, or providing connections.”¹ Section 512(a) was intended (when enacted in 1998) to protect ISPs from liability for routing, transmitting or providing connections to copyrighted material, but by its terms may also apply to certain modern day streaming services.

Although not discussed in the House Report accompanying the final version of the bill, the safe harbor created by section 512(a) is directed at the possibility that under *MAI Systems Corp. v. Peak Computer, Inc.*² and its progeny a copy within the meaning of the Copyright Act may be created at multiple points over the Internet simply because of the way information is transmitted under TCP/IP and related Internet protocols.³ In the words of the Ninth Circuit, “[t]he Internet as we know it simply cannot exist if th[e] intervening computers” through which information travels pursuant to TCP/IP protocols could not benefit from the DMCA safe harbor and had to “block indirectly infringing content.”⁴

To qualify for the limitation for “transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate or transient storage of that

[Section 4.12[4]]

¹17 U.S.C.A. § 512(a). “To fall within that safe harbor, . . . [a service provider] must show that it meets the threshold requirement[s], common to all § 512 safe harbors” *BMG Rights Management (US) LLC v. Cox Communications, Inc.*, 881 F.3d 294, 301 (4th Cir. 2018) (holding that Cox, although a “conduit ISP,” failed to meet its burden of proof to show eligibility for the safe harbor created by section 512(a) because it failed to reasonably implement its repeat infringer policy).

²*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994).

³*See Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995) (analyzing *MAI*’s impact on Internet communications); *see generally supra* § 4.03. Congress was plainly aware of the *MAI* case and its potential application to Internet liability, as evidenced by the fact that the very next sections (sections 301 and 302) of the Digital Millennium Copyright Act following the Online Copyright Infringement Liability Limitation Act modify the effects of *MAI* for independent service organizations, which are entities that provide post-warranty maintenance work on computers which they did not manufacture and who otherwise could be held liable for copyright infringement (like the defendant in *MAI*) simply by virtue of turning on a computer, which causes a temporary copy of the licensed operating system to be loaded into random access memory (RAM). *See supra* §§ 4.03, 4.04[5].

⁴*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1116 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

material in the course of such transmitting, routing, or providing connections”⁵ a defendant must meet the narrower requirements to be deemed a *service provider* applicable to section 512(a)⁶ and satisfy five conditions.

First, a transmission must have been initiated by or at the direction of a person other than the service provider.⁷

Second, the “transmission, routing, provision of connections, or storage” must have been carried out by “an automatic technical process without selection of the material

⁵17 U.S.C.A. § 512(a).

⁶*Service provider* for purposes of the transitory digital network communications safe harbor means “an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.” 17 U.S.C.A. § 512(k)(1)(A). The term *service provider* is defined more narrowly when used in connection with the liability limitation created by section 512(a) than for the other DMCA safe harbors. Compare 17 U.S.C.A. § 512(k)(1)(A) (narrowly defining the term *service provider* for purposes only of the transitory digital network communications safe harbor created by section 512(a)) with 17 U.S.C.A. § 512(k)(1)(B) (broadly defining the same term for purposes of the user storage, information location tools and caching safe harbors); see generally *supra* § 4.12[2] (analyzing the definition of *service provider* in different contexts under the DMCA).

In *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1041–42 (9th Cir. 2013), the Ninth Circuit held that the operator of a BitTorrent tracker did not qualify as a service provider for purposes of the transitory digital network communications safe harbor because trackers select the “points” to which a user’s client will connect in order to download a file using the BitTorrent protocol and a *service provider* for purposes of this safe harbor must provide “connections . . . between or among points specified by a user.” 17 U.S.C.A. § 512(k)(1)(A) (emphasis added).

The district court in *A&M Records, Inc. v. Napster, Inc.*, No. C 99–05183 MHP, 2000 WL 573136, at *3 n.5 (N.D. Cal. May 12, 2000) expressed skepticism in *dicta* that Napster, which provided a peer-to-peer software application that relied on an index located on a central server, qualified for the narrower definition of *service provider* set forth in section 512(k)(1)(B), but since the plaintiffs had not challenged Napster’s eligibility on this basis the court proceeded to deny Napster’s motion for summary adjudication on the issue of its entitlement to the DMCA defense on other grounds (ruling that to benefit from the safe harbor, transmitting, routing, or providing connections must occur “through” a service provider’s system or network and, because users exchanged infringing files directly—not through Napster’s servers—Napster did not “transmit, route, or provide connections through its system . . .”).

⁷17 U.S.C.A. § 512(a)(1).

by the service provider.”⁸

Third, the service provider may not select the recipients of the material except “as an automatic response to the request of another person.”⁹

Fourth, the service provider may not maintain any stored copy of the material made in the course of intermediate or transient storage on its system or network in a manner “ordinarily accessible to anyone other than anticipated recipients” or for longer than “reasonably necessary” to allow for the transmission, routing, or provision of connections.¹⁰

Fifth, the content of the material may not have been modified while it was transmitted through the service provider’s “system or network”¹¹

According to the legislative history, subsections “(a)(1) through (5) limit the range of activities that qualify under this subsection to ones in which a service provider plays the

⁸17 U.S.C.A. § 512(a)(2). According to a House Report accompanying an earlier version of the bill, *selection of the material* means “the editorial function of determining what material to send, or the specific sources of material to place on-line (e.g., a radio station), rather than ‘an automatic technical process’ of responding to a command or request, such as one from a user, an Internet location tool, or another network.” H.R. Conf. Rep. No. 551, 105th Cong., 2d Sess. 51 (1998). The term *automatic response to the request of another*, according to this same source, “is intended to encompass a service provider’s actions in responding to requests by a user or other networks, such as requests to forward e-mail traffic or to route messages to a mailing list agent (such as a ‘Listserv’) or other discussion group.” *Id.*

⁹17 U.S.C.A. § 512(a)(3).

¹⁰17 U.S.C.A. § 512(a)(4). A House Report accompanying an earlier version of the bill explained:

The Committee intends subsection (a)(4) to cover copies made of material while it is en route to its destination, such as copies made on a router or mail server, storage of a web page in the course of transmission to a specific user, store and forward functions, and other transient copies that occur en route. The term “ordinarily accessible” is intended to encompass stored material that is routinely accessible to third parties. For example, the fact that an illegal intruder might be able to obtain access to the material would not make it ordinarily accessible to third parties. Neither, for example, would occasional access in the course of maintenance by service provider personnel, nor access by law enforcement officials pursuant to subpoena make the material “ordinarily accessible.” However, the term does not include copies made by a service provider for the purpose of making the material available to other users. Such copying is addressed in subsection (b) [the caching safe harbor].

H.R. Conf. Rep. No. 551, 105th Cong., 2d Sess. 51 (1998).

¹¹17 U.S.C.A. § 512(a)(5).

role of a ‘conduit’ for the communications of others.”¹² Accordingly, some courts have referred to section 512(a) in *dicta* as creating a safe harbor for service providers that act as “conduits” for the transmission of information.¹³

The safe harbor created by section 512(a) is consistent with and was influenced by the court’s analysis in *Religious Technology Center. v. Netcom On-Line Communication Services, Inc.*,¹⁴ which was the leading Internet secondary liability case at the time the DMCA was crafted and which influenced the development of the statute. In that case, the court held that Netcom, an ISP that provided Internet access to a Usenet group where infringing material allegedly had been posted, was a passive participant in the infringement, and thus could not be held directly liable for copyright infringement in the absence of any evidence of “direct action” on its part to further the infringement. The court based its holding in part on the fact that Netcom did not “initiate” the transmissions and its acts of copying and transmitting infringing content were “automatic and indiscriminate.”¹⁵

¹²H.R. Conf. Rep. No. 551, 105th Cong., 2d Sess. 51 (1998).

¹³*See, e.g., In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 775–76 (8th Cir. 2005) (characterizing section 512(a) as limiting “the liability of ISPs when they do nothing more than transmit, route, or provide connections for copyrighted material—that is, when the ISP is a mere conduit for the transmission” and applying when a service provider “merely acts as a conduit for infringing material without storing, caching, or providing links to copyrighted material.”); *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1041 (9th Cir. 2013) (stating that section “512(a) applies to service providers who act only as ‘conduits’ for the transmission of information.”). *But see A&M Records, Inc. v. Napster, Inc.*, No. C 99–05183 MHP, 2000 WL 573136, at *6 (N.D. Cal. May 12, 2000) (“the words ‘conduit’ or ‘passive conduit’ appear nowhere in 512(a), but are found only in the legislative history and summaries of the DMCA. The court must look first to the plain language of the statute.”).

Among other services, “[g]enerally, ISPs . . . fit this definition.” *Windstream Services, LLC v. BMG Rights Management (US) LLC*, 16 Civ. 5015 (KMW) (RLE), 2017 WL 1386357, at *5 (S.D.N.Y. Apr. 17, 2017) (*dicta*) (dismissing Windstream’s suit for a declaratory judgment that Windstream was entitled to the safe harbors created by sections 512(a) and 512(c), for lack of subject matter jurisdiction), *appeal dismissed*, Docket No. 17–1515, 2017 WL 5329346 (2d Cir. Sept. 25, 2017).

¹⁴*Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995); *see generally supra* §§ 4.11[2], 4.11[8][B].

¹⁵*In Ellison v. Robertson*, 357 F.3d 1072, 1081 (9th Cir. 2004), the

There have been few court opinions that have analyzed the applicability of the safe harbor created by section 512(a) since it was signed into law in 1998. Courts have held that services where the defendant, rather than the user, specifies the point of connection (such as a BitTorrent tracker¹⁶) or where transmissions occur directly between users, rather than “through a system or network controlled or operated by or for” a service provider¹⁷ (such as a Peer-to-Peer network¹⁸), are ineligible for the safe harbor. On the other hand, the Ninth Circuit clarified that, where applicable, the safe harbor for transitory digital network communications applies to all transmissions and not merely for those that a service provider can show are directly infringing.¹⁹ Thus, if a service provider qualifies for the safe harbor created by section 512(a), it is entitled to safe harbor protection regardless of whether it could also qualify for another safe harbor under

Ninth Circuit ruled that AOL was entitled to benefit from this liability limitation for Usenet posts that, as in *Netcom*, originated on a different service and were only accessible for a limited time period (fourteen days, in comparison to eleven days in *Netcom*).

¹⁶See *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1041–42 (9th Cir. 2013).

¹⁷17 U.S.C.A. § 512(a).

¹⁸In *A&M Records, Inc. v. Napster, Inc.*, No. C 99–05183 MHP, 2000 WL 573136 (N.D. Cal. May 12, 2000), the court held that Napster was not eligible for the liability limitation for transmitting, routing or providing connections, because users exchanged infringing files directly—not through Napster’s servers. Napster was a service that facilitated infringement by providing software and an index on a central server that users could access to exchange files directly with each other. The court explained that to qualify for the safe harbor created by subsection 512(a), transmitting, routing, or providing connections must occur “through” a service provider’s system or network and Napster did not “transmit, route, or provide connections through its system” *Id.* at *8.

¹⁹See *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1115–16 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007). In *Perfect 10*, the Ninth Circuit remanded for consideration whether a Web hosting company that transmitted “digital online communications” in the form of credit card payments and proof of payments was entitled to this safe harbor. In so doing, the panel rejected the plaintiff’s argument that the defendant was not entitled to protection under section 512(a) because it did not itself transmit the allegedly infringing material. It also rejected as “perverse” the argument that while the safe harbor might extend to infringing material it would not insulate a service provider from liability for noninfringing content that could form the basis of a claim of contributory infringement. Eligible service providers “are immune for transmitting all digital online communications, not just those that directly infringe.” 488 F.3d at 1116.

section 512.²⁰

If a service provider initiates or modifies²¹ a transmission, stores it²² so that it becomes generally accessible or posts third-party content through a process involving some element of selection, presumably it would be unable to benefit from the liability limitation for transitory digital network communications.

In short, the statute's multipart test to evaluate whether a communication is genuinely transitory is directed specifically—and narrowly—at circumstances where liability could be imposed by virtue of *MAI Systems Corp. v. Peak Computer, Inc.*²³ and its extension to the Internet, where a service provider could not reasonably be expected to be able to monitor, control or prevent such communications. Moreover, because the DMCA should be broadly construed, and because transmission, routing and providing communications do not occur in a vacuum, a service should not be deemed to fall outside the safe harbor based on internal processes incident to transmission, routing or providing communications.

On the other hand, merely because a service provider monitors content that passes over its system or network should not provide sufficient grounds—absent additional facts—for concluding that the liability limitation is inapplicable. The House Report makes clear that the “legisla-

²⁰See, e.g., *Rosen v. PCCW Global, Inc.*, Case No. CV 10-2248 ODW (CWx), 2010 WL 11597955, at *5-6 (C.D. Cal. Dec. 29, 2010) (granting summary judgment for the defending, holding that it was entitled to the safe harbor created by section 512(a)).

²¹In *In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634 (N.D. Ill. 2002), *aff'd on other grounds*, 334 F.3d 643 (7th Cir. 2003), the court wrote in *dicta* that the Aimster peer-to-peer service “modified” content by encrypting all information transferred between users.

²²See *Rosen v. Global Net Access, LLC*, No. CV 10-2721-DMG (E), 2014 WL 2803752, at *4 (C.D. Cal. June 20, 2014) (holding that “[b]ecause GNAX stores clients’ data on its servers, its connection to its clients’ material is not transient, and thus GNAX’s affirmative defense under Section 512(a) fails.”).

²³*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994); see generally *supra* § 4.03. The temporary copies created by some transmissions may not be actionable if they are not fixed for a period of more than merely “a transitory duration.” See *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 129–30 (2d Cir. 2008), *cert. denied*, 557 U.S. 946 (2009); see generally *supra* § 4.03. What constitutes a *transitory duration* may be evaluated differently outside the Second Circuit. See generally *supra* § 4.03.

tion [wa]s not intended to discourage the service provider from monitoring its service for infringing material. Courts should not conclude that the service provider loses eligibility for limitations on liability . . . solely because it engaged in a monitoring program.”²⁴

Where a service provider qualifies for the safe harbor created by section 512(a) it may not be held liable for damages or attorneys’ fees and may only be subject to narrow injunctive relief.²⁵

It also may not be required to comply with DMCA subpoenas served pursuant to section 512(h).²⁶

²⁴H.R. Conf. Rep. No. 796, 105th Cong., 2d Sess. 73 (1998), *reprinted in* 1998 U.S.C.C.A.N. 639, 649.

²⁵Service providers that meet the requirements to qualify for the transitory digital network communications safe harbor may only be subject to the following injunctive relief:

- (i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider’s system or network who is using the provider’s service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.
- (ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

17 U.S.C.A. § 512(j)(1)(B). Broader relief may be obtained against service providers that qualify for the other three safe harbors. *See* 17 U.S.C.A. § 512(j)(1)(A). The considerations relevant to whether injunctive relief should issue and provisions for notice and *ex parte* relief are set forth in sections 512(j)(2) and 512(j)(3), respectively. At least in the Ninth Circuit, an injunction compelling a service provider to remove user content is deemed to be a mandatory injunction, which is disfavored. *Garcia v. Google, Inc.*, 786 F.3d 733, 740 & n.4 (9th Cir. 2015) (*en banc*); *see generally infra* § 4.13[1] (setting forth the standards for obtaining injunctive relief). It may also be viewed as an impermissible prior restraint. *See Garcia v. Google, Inc.*, 786 F.3d 733, 746-47 (9th Cir. 2015) (*en banc*) (dissolving a previously entered preliminary injunction compelling YouTube to take down copies of the film “Innocence of Muslims” and take all reasonable steps to prevent further uploads, which the *en banc* panel held had operated as a prior restraint), *citing Alexander v. United States*, 509 U.S. 544, 550 (1993) (“Temporary restraining orders and permanent injunctions—i.e., court orders that actually forbid speech activities—are classic examples of prior restraints.”); *infra* § 4.13[1].

²⁶*See, e.g., In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 781-82 (8th Cir. 2005); *Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229, 1237-38 (D.C. Cir. 2003), *cert denied*, 543 U.S. 924 (2004); *In re Subpoena To University of North Carolina at Chapel Hill*, 367 F. Supp. 2d 945, 948-56 (M.D.N.C. 2005); *see generally infra* § 4.12[9][E] (analyzing section

4.12[5] System Caching

4.12[5][A] System Caching—In General

The DMCA also potentially limits the liability of a service provider (which otherwise meets the four general threshold requirements set forth in section 4.12[3]) for the “intermediate and temporary storage of material on a system or network”—commonly referred to as caching.¹ This provision is a logical compliment to the liability limitation created for transitory digital network communications, which only applies to the temporary storage of copyrighted material that occurs during transmission, routing, or provision of connections. Both limitations address the potential liability which inadvertently could be imposed on a service provider by virtue of the *MAI Systems Corp. v. Peak Computer, Inc.* case.²

To limit liability for system caching, eight specific requirements must be satisfied (in addition to the four threshold prerequisites). The first four conditions are intended to limit the provision to system caching rather than other types of caching. The last four requirements are intended to ensure that copyright owners and third-party content providers are not disadvantaged by the caching safe harbor in circumstances such as where material is frequently updated and the cached copy could grow stale, where a rights owner implements content protection technology to deter infringement, where content is only made available for a fee or where access is password protected or otherwise restricted, or where the original material has been taken down as infringing but a cached copy remains online. While the first four conditions are generally applicable, the last four will apply only to particular types of services. The first three, which are set forth in section 512(b)(1), may be thought of as

512(h) subpoenas).

[Section 4.12[5][A]]

¹17 U.S.C.A. § 512(b)(1). The limitation applies both where a system or network is controlled by the service provider and where it is merely operated by or for the provider. *See id.*

²*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994); *see generally supra* §§ 4.03 (analyzing *MAI* and more recent case law), 4.12[4] (discussing why Congress was aware of the *MAI* case and intended to address potential exposure that could be created for temporary, cached copies by the liability limitations created in sections 512(a) and 512(b)).

eligibility requirements, whereas the last five, which are enumerated in section 512(b)(2), are characterized as “conditions.”

Section 512(b) provides that a service provider shall not be liable for monetary relief, or except as provided in subsection (j) for injunctive or equitable relief,³ “for infringement of

³With respect to the caching safe harbor, section 512(j) provides:

- (j) **Injunctions.**— The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) **Scope of relief.**—

- (A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

- (i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider’s system or network.
- (ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider’s system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.
- (iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose

- (2) **Considerations.**— The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider—

- (A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider’s system or network;
- (B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;
- (C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider” if the following requirements and conditions are met:

- (1) The allegedly infringing material at issue in a given suit must have been “made available online by a person other than the service provider.”⁴
- (2) The material must have been “transmitted from the person described in subparagraph (A)”—i.e., “a person other than the service provider”⁵—“through the [service provider’s] system or network⁶ to a person other than the person described in subparagraph (A) at the

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

- (3) **Notice and ex parte orders.**— Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider’s communications network.

17 U.S.C.A. § 512(j). At least in the Ninth Circuit, an injunction compelling a service provider to remove user content is deemed to be a mandatory injunction, which is disfavored. *Garcia v. Google, Inc.*, 786 F.3d 733, 740 & n.4 (9th Cir. 2015) (*en banc*); see generally *infra* § 4.13[1] (setting forth the standards for obtaining injunctive relief). It may also be viewed as an impermissible prior restraint. See *Garcia v. Google, Inc.*, 786 F.3d 733, 746-47 (9th Cir. 2015) (*en banc*) (dissolving a previously entered preliminary injunction compelling YouTube to take down copies of the film “Innocence of Muslims” and take all reasonable steps to prevent further uploads, which the *en banc* panel held had operated as a prior restraint), citing *Alexander v. United States*, 509 U.S. 544, 550 (1993) (“Temporary restraining orders and permanent injunctions—i.e., court orders that actually forbid speech activities—are classic examples of prior restraints.”); *infra* § 4.13[1].

⁴17 U.S.C.A. § 512(b)(1)(A).

⁵17 U.S.C.A. § 512(b)(1)(A).

⁶The statute does not define what constitutes *a system or network controlled or operated by or for the service provider*. The lower court in *In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634 (N.D. Ill. 2002), *aff’d on other grounds*, 334 F.3d 643 (7th Cir. 2003), wrote in *dicta* that a peer-to-peer service could not benefit from this limitation in part because material passed between users was not transmitted “through” the system within the meaning of 17 U.S.C.A. § 512(b)(1)(B); see also *A&M Records, Inc. v. Napster, Inc.*, No. C 99-05183 MHP, 2000 WL 573136 (N.D. Cal. May 12, 2000) (reaching a similar conclusion in analyzing the safe harbor created by section 512(a) for transitory digital network communications); see generally *supra* § 4.12[4].

- direction of that other person”⁷—such as when a user calls up a third-party website that is transmitted through the service provider’s system or network. This requirement is poorly drafted and is explained in greater detail below in section 4.12[5][B].
- (3) The storage is carried out “through an automatic technical process for the purpose of making the [cached] material available to users of the system or network” who requested it from the original location that was cached.⁸
 - (4) The material must have been transmitted (by the service provider) to subsequent users without modification “to its content from the manner in which the material was transmitted from the person . . .” (i.e., the content must not have been changed even if, from a technical standpoint, the form may have been modified as part of the process of caching).⁹

The legislative history does not provide much guidance other than emphasizing that material stored on *a system or network controlled or operated by or for the service provider* refers to the service provider’s own system or network. The House Report accompanying the DMCA states that “[t]he material in question is stored on the service provider’s system or network for some period of time to facilitate access by users subsequent to the one who previously sought access to it.” H.R. Rep. No. 105-551, 105th Cong., 2d Sess. (1998). The Senate Report also explains that “[t]he liability limitations apply to networks ‘operated by or for the service provider,’ thereby protecting both service providers who offer a service and subcontractors who may operate parts of, or an entire, system or network for another service provider.” S. Rep. No. 105-190, 105th Cong., 2d Sess. (1998).

⁷17 U.S.C.A. § 512(b)(1)(B).

⁸See 17 U.S.C.A. § 512(b)(1)(C). The exact statutory language is:

[T]he storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A) . . .

Id. In other words, the material must be stored automatically for the purpose of allowing users who subsequently request the original material to be given access to the cached copy.

⁹See 17 U.S.C.A. § 512(b)(2)(A) (stating that “the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A); . . .”). The terms *content* and *material* are not defined in the statute but *content* should be understood to mean the creative contents of a cached file (such as a photograph, motion picture or song, which could not be modified), as opposed to the file itself (the *material*, in

- (5) The service provider must have complied with “rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data com-

which the *content* is stored, which may be modified technically by a service provider in the process of caching). At the time the DMCA was enacted, *content* generally meant the “essential meaning; substance,” while *material* was defined as “what a thing is, or may be, made of.” Webster’s New World College Dictionary (3d ed. 1997).

The DMCA’s legislative history further supports the view that the focus is on the contents, and not the form of the cached material. *See* H.R. Rep. 105-551 (II) at 52. In explaining section 512(b), the Report states that “the material must be transmitted to subsequent users without modification to its content in comparison to the way it was originally transmitted from the originating site. The Committee intends that this restriction apply, for example, so that a service provider who caches material from another site does not change the advertising associated with the cached material on the originating site without authorization from the originating site.” *Id.* This suggests that modification to “content” refers to changes to the substance, but not the “form,” of the material.

In construing the same language under the safe harbor in section 512(a)(5) requiring that “the material is transmitted through the system or network without modification of its content . . .,” the court in *Perfect 10, Inc. v. Amazon.com, Inc.*, No. CV 05-4753 AHM (SHX), 2008 WL 11336890, at *7 (C.D. Cal. Nov. 4, 2008), ruled that this requirement does not, according to the legislative history, “pertain to modifications of the ‘form’ of the material, citing as an example an e-mail transmission that appears to the recipient without bolding or italics resulting from format codes contained in the sender’s message.” *Id.*, citing H.R. Rep. 105-551 (II) at 52. The court held that “differences in the appearance of URLs, such as the omission of ‘http://,’ . . . are in the format, not content, of the URLs,” and “[t]he same goes for differences in layout and fonts.” 2008 WL 11336890, at *7. By contrast, added text and differences in the number of search results that effectively displayed different search results created at least a triable issue of fact on whether content had been modified. *Id.* at *8.

In *In re Aimster Copyright Litig.*, 252 F. Supp. 2d 634 (N.D. Ill. 2002), *aff’d on other grounds*, 334 F.3d 643 (7th Cir. 2003), the court held that Aimster was not eligible for the caching safe harbor in part because Aimster encrypted all data transferred between users, including music files, and therefore could not satisfy the requirement that material be transmitted without modification. 252 F. Supp. 2d at 660-61 & nn.19, 21. The district court wrote in *dicta* that Aimster’s peer-to-peer service “modified” content by encrypting all information transferred between users. In light of the legislative history cited above, the district court’s analysis in *Aimster* appears to be incorrect. Merely encrypting files should not be understood to modify the content of material.

munications protocol¹⁰ for the system or network through which that person makes the material available”¹¹

- (6) The service provider must not “interfere with the ability of technology associated with the material” to return information to the party that originally posted or transmitted it that would have been available to the site owner if the material had been accessed directly, rather than from a cached copy (such as returning user statistics to a website owner when the cached copy of its site is accessed).¹² This sixth requirement only applies, however, when the technology: (a) does not significantly interfere with the performance of the service provider’s system or network or the intermediate storage of the material; (b) is consistent with generally accepted industry standard communications protocols; and (c) does not extract information from the service provider’s system or network other than information that would otherwise have been available to the person who originally posted or transmitted the material (*i.e.*, “the person described in paragraph (1)(A) . . . ,” which is defined

¹⁰The House Report accompanying the statute acknowledged that these protocols and related technologies were only in the early stages of development at the time the DMCA was under consideration. The Report clarifies that the House and Senate conferees expected that “the Internet industry standards setting organizations, such as the Internet Engineering Task Force and the World Wide Web Consortium, will act promptly and without delay to establish these protocols so that . . . [the subsection providing the system caching limitation] can operate as intended.”

¹¹17 U.S.C.A. § 512(b)(2)(B). This specific requirement is not applicable if the person who originally posted or transmitted the content (*i.e.*, “the person described in paragraph (1)(A)”) uses these rules “to prevent or unreasonably impair the intermediate storage” that is the subject of the caching limitation set forth in section 512(b). *See id.* In other words, if “the person described in paragraph (1)(A) . . . ,” which is defined to be “a person other than the service provider” (*id.* § 512(b)(1)(A)) and therefore typically refers to the owner or operator of a website or other online content that may be cached, uses rules concerning refreshing, reloading or other updating of material “to prevent or unreasonably impair” intermediate storage, the service provider will not lose safe harbor protection under the caching liability limitation created by section 512(b) if it fails to comply with those rules with respect to material from that owner or operator.

¹²17 U.S.C.A. § 512(b)(2)(C).

- to be “a person other than the service provider”¹³), had subsequent users gained access to the material directly from that person, rather than from the service provider’s cached copy.¹⁴
- (7) If the site owner (or other “person other than the service provider”) has in effect a condition that a person must meet prior to gaining access to the material—such as payment of a fee or provision of a password or other information—the service provider must permit access to the stored material “in significant part” only to users of its system or network that have met those conditions and only in accordance with those conditions.¹⁵ In other words, a service provider may not permit unrestricted access to cached content if the same material could not be accessed without restrictions, and must ensure that the same conditions imposed by a site owner or service provider are met (such as payment of a fee or provision of login credentials) before giving a user access to the cached version. Substantial compliance with this condition, not strict adherence, is required, as evidenced by the use of the qualifier “in significant part” in describing a service provider’s compliance obligation, likely out of recognition that systems can fail and software malfunction. A service provider therefore will not lose safe harbor protection so long as this condition is met “in significant part.”
- (8) Where a site or service (or other “person other than the service provider”) makes material available online without the authorization of the copyright owner, the service provider must respond *expeditiously* to remove, or disable access to, the material upon receipt of a notification pursuant to section 512(c)(3), which sets forth the requirement for responding to copyright owner notifications in compliance with the user storage safe harbor (which is discussed below in subsection 4.12[9][B]).¹⁶ This requirement only applies, however, if the material has previously been removed from the site where it originated from (or

¹³17 U.S.C.A. § 512(b)(1)(A).

¹⁴17 U.S.C.A. § 512(b)(2)(C).

¹⁵17 U.S.C.A. § 512(b)(2)(D).

¹⁶See 17 U.S.C.A. § 512(b)(2)(E).

access to that site has been disabled) or a court has ordered that the material be removed (or access be disabled) *and* the party giving notice includes a statement confirming these facts.¹⁷

There is very little case law construing the caching safe harbor. The most detailed analysis is found in *Field v Google, Inc.*¹⁸ In that case, a district court in Nevada held that Google was entitled to the safe harbor created by section 512(b) for caching websites incident to the operation of its search engine and granted summary judgment in Google's favor on that basis. At issue was Google's practice of caching almost the entire Internet to allow users to access material when an original page was inaccessible, thus providing archival copies of value to academics, researchers and journalists. Google cached websites using a bot (or intelligent agent software) to automatically copy and store the HTML code for webpages, which were then indexed and made accessible to users via links displayed in response to user search queries.¹⁹

In ruling that Google's practices were protected by the caching safe harbor, the court rejected the plaintiff's argument that by retaining cached copies for fourteen to twenty days Google was ineligible for the safe harbor because copying material for that period of time did not involve "intermediate and temporary storage" within the meaning of section 512(b)(1). Relying on the Ninth Circuit's prior construction of the terms *intermediate* and *transient* in section 512(a) to include storage of Usenet postings for fourteen days,²⁰ the court deemed Google's retention of cached copies for fourteen to twenty days to be merely "intermediate and temporary storage" within the meaning of section 512(b).²¹

4.12[5][B] Transmission from a "Person Other than the Service Provider" Through the Service Provider's System or Network to A "Person Other than" that Person

Subsection 512(b)(1)(B) is inartfully drafted and must be

¹⁷17 U.S.C.A. § 512(b)(2)(E).

¹⁸*Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1123–25 (D. Nev. 2006).

¹⁹See *Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1111 (D. Nev. 2006).

²⁰See *Ellison v. Robertson*, 357 F.3d 1072, 1081 (9th Cir. 2004); *supra* § 4.12[4].

²¹What constitutes *intermediate and temporary storage* is further analyzed below in section 4.12[5][C].

read in conjunction with section 512(b)(1)(A) to be understood. Read literally, the double negatives and cross-references included in subsection 512(b)(1)(B) may sound like a riddle from Lewis Carroll's "Jabberwocky" poem, although on close analysis the requirement is actually straightforward. The provision requires that a transmission be from a person other than the service provider (such as a third-party website or a service provider's user) and be made through the service provider's system or network to a "person other than the person" who is described in subsection 512(b)(1)(A) as the "person other than the service provider"—which by virtue of the use of double negatives may be the service provider or some other website or user. While Congress undoubtedly could have done a better job drafting the language of this section so as not to require that the transmission be to a "person other than a person" who is "a person other than a service provider," sadly it did not do so.

Subparts 512(b)(1)(A) and 512(b)(1)(B) literally require that the material at issue be:

(A) . . . made available online by a person other than the service provider; and

(B) . . . transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person.¹

The statute is confusing in that subpart 512(b)(1)(B) refers to a "person other than the person described in subparagraph (A)" which in turn refers to "a person other than the service provider." In holding that Google was entitled to the caching safe harbor for material that Google itself cached from third-party websites, the court in *Field v Google, Inc.*² assumed that the "other person" referred to in subpart 512(b)(1)(B) could be the service provider given that subpart (A) includes any person *other than* the service provider (and, by extension, anyone other than that person could include the service provider). This interpretation also is supported by the plain text of section 512(b)(1)(B).

The legislative history implies that to qualify for the caching safe harbor material must first have been requested by a

[Section 4.12[5][B]]

¹17 U.S.C.A. § 512(b)(1).

²*Field v. Google Inc.*, 412 F. Supp. 2d 1106 (D. Nev. 2006).

third party and could not be cached by a service provider on its own initiative, although there is no support for this reading on the face of the statute. The House and Senate Report explain that:

The material in question is stored on the service provider's system or network for some period of time *to facilitate access by users subsequent to the one who previously sought access to it*. For subsection (b) to apply, the material must be made available on an originating site, *transmitted at the direction of another person* through the system or network operated by or for the service provider to a different person, and stored through an automatic technical process so that users of the system or network *who subsequently request access to the material from the originating site may obtain access to the material from the system or network*.³

Based on this language in the legislative history, some commentators have argued that *Field v. Google* was wrongly decided and that “a person other than the person described in subparagraph (A)” cannot be the service provider itself, through whose system or network cached material is made available at the direction of “that other person” and that to fall within the caching safe harbor a third-party user must first request material before it may be cached by a service provider.⁴

However, there is no support on the face of the statute for this interpretation. Legislative history generally cannot provide a basis for construing the language of a statute on a point that is not ambiguous.⁵ While section 512(b)(1)(B) is inartfully drafted, it is not confusing with respect to the question of whether material must first have been requested by a user before a service provider may create a cached copy for use by subsequent users. The terms of the statute merely require that the request be made by a person other than the

³H.R. Rep. No. 105-551, 105th Cong., 2nd Sess. (1998) (emphasis added); S. Rep. No. 105-190, 105th Cong., 2nd Sess. (1998) (emphasis added).

⁴See, e.g., Nimmer on Copyright § 12B.03.

⁵See, e.g., *Murphy v. Millennium Radio Group LLC*, 650 F.3d 295, 301–05 (3d Cir. 2011) (explaining that except in rare circumstances legislative history cannot trump the plain terms of a statute and construing a different provision of the Digital Millennium Copyright Act based on the terms of the statute, rather than imposing an additional requirement suggested by legislative history); *MDY Industries, LLC v. Blizzard Entertainment, Inc.*, 629 F.3d 928, 951 (9th Cir. 2010) (holding that policy considerations “cannot trump the statute’s plain text and structure” in construing section 1201(a) of the Digital Millennium Copyright Act).

person described in section 512(b)(1)(A), who is defined as a “person other than the service provider.” If one substitutes the words “third-party website” for the term “the person described in subparagraph (A)” (since that subparagraph merely requires that the material cached be made available by “a person other than the service provider”) it is clear that the material may be requested by the service provider itself and the statute imposes no obligation that material be cached only subsequent to a first user’s request. The material merely must be transmitted from a third-party website through a service provider’s system or network to a person other than the third-party website at the direction of that other person. “*That other person*” therefore may be either a user or the service provider itself—just not the third-party website (and, pursuant to subpart 512(b)(1)(A), the material may not have been made available online by the service provider itself, as opposed to a third-party website).

The unambiguous, albeit inartfully drafted words of the statute make clear that third-party material may be cached once requested by a user or it may be cached at the direction of a service provider. The result compelled by the terms of the statute also makes logical sense since caching is a technique used by service providers to make material more quickly and easily available to users.⁶ Requiring that material only be cached after another user first requests it—so that the delivery to the first requester necessarily will be slower and more inefficient than for all subsequent users—finds no basis in logic or in the plain terms of the statute.

4.12[5][C] Intermediate and Temporary Storage

What constitutes *intermediate and temporary storage* is not defined in the statute.

Intermediate storage means storage by an intermediary that is neither the originating site nor the end user. The House and Senate reports accompanying the DMCA explain that “[t]he storage is intermediate in the sense that the service provider serves as an intermediary between the originating site and the ultimate user.”¹

Precisely what length of storage time would be deemed

⁶See generally *infra* § 9.02 (analyzing caching).

[Section 4.12[5][C]]

¹H.R. Rep. No. 105-551, 105th Cong., 2d Sess. (1998); S. Rep. No. 105-190, 105th Cong., 2d Sess. (1998).

temporary is not defined in the statute nor explained in the DMCA's legislative history. The House and Senate reports, unhelpfully, explain that temporary storage would last for "some period of time."² This likely reflects Congressional reluctance to impose specific time limits on changing technology.

In *Field v. Google, Inc.*,³ the court held that Google was entitled to section 512(b)'s caching liability limitation where it retained cached copies for fourteen to twenty days. In so ruling, the court relied on the Ninth Circuit's decision in *Ellison v. Robertson*,⁴ where a plaintiff sought to hold AOL liable for copyright infringement for hosting and allowing end users to access copyrighted materials that third parties had posted to a system of online bulletin boards.⁵ In *Ellison*, AOL had stored and allowed users to access user posts for approximately fourteen days. Citing the DMCA's legislative history, the *Ellison* court found that AOL's storage of the materials was "intermediate" and "transient" as required by section 512(a).⁶ Based on this holding, the *Field* court found that Google's practice of caching material for approximately fourteen to twenty days—like the fourteen days the *Ellison* court deemed "transient storage"—was "temporary" within the meaning of section 512(b).⁷

The *Field* court's decision rested on the statutory language used in subsections 512(a) and 512(b), which is similar but not identical.⁸ Subsection 512(b) requires that cached copying be "intermediate and temporary" whereas subsection 512(a) uses the term "intermediate and transitory."⁹ *Temporary* means "lasting for a limited time," while *transitory*

²H.R. Rep. No. 105-551, 105th Cong., 2d Sess. (1998); S. Rep. No. 105-190, 105th Cong., 2d Sess. (1998).

³*Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1123–24 (D. Nev. 2006).

⁴*Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004).

⁵*Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1123–24 (D. Nev. 2006), citing *Ellison v. Robertson*, 357 F.3d 1072, 1075–76 (9th Cir. 2004).

⁶*Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1123–24 (D. Nev. 2006), citing *Ellison v. Robertson*, 357 F.3d 1072, 1081 (9th Cir. 2004).

⁷*Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1124 (D. Nev. 2006).

⁸See *Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1124 (D. Nev. 2006) (citing *Gustafson v. Alloyd Co.*, 513 U.S. 561, 570 (1995) for the principal that "identical words used in different parts of the same act are intended to have the same meaning").

⁹Compare 17 U.S.C.A. § 512(a) with 17 U.S.C.A. § 512(b).

means only a “brief duration” of time.¹⁰ Thus, the difference between *temporary* and *transitory* suggests that intermediate storage may last a longer time when material is cached than when it is in transit.

4.12[6] Information Residing on Systems or Networks at the Direction of Users (User Storage)

4.12[6][A] In General

A service provider that meets the four threshold eligibility requirements set forth in section 4.12[3] may avoid liability for monetary relief “by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for” it, if it can meet four additional prerequisites.

First, a service provider must “not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.”¹ To be ineligible for safe harbor protection, a service provider would have to have both a financial benefit *and* the right and ability to control. If it had one but not the other, the service provider would still be eligible for the safe harbor (if it meets the other statutory requirements).²

The financial interest prong has been construed in the Ninth Circuit as requiring a showing that “‘the infringing activity constitutes a draw for subscribers, not just an added benefit.’ ”³

¹⁰*Compare Temporary Definition*, Merriam-Webster Dictionary.com, <http://www.merriam-webster.com> (last visited Apr. 29, 2013) with *Transitory Definition*, Merriam-Webster Dictionary.com, <http://www.merriam-webster.com> (last visited Apr. 29, 2013); see generally *FDIC v. Meyer*, 510 U.S. 471, 476 (1994) (using a dictionary to interpret a federal statute and stating, in the absence of a statutory definition, “we construe a statutory term in accordance with its ordinary or natural meaning”).

[Section 4.12[6][A]]

¹17 U.S.C.A. § 512(c).

²See *infra* § 4.12[6][D].

³*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117–18 (9th Cir.), cert. denied, 522 U.S. 1062 (2007); *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004) (quoting legislative history).

With respect to right and ability to control, the Second,⁴ Fourth⁵ and Ninth⁶ Circuits have held that the degree of control required to disqualify a service provider from eligibility for the DMCA safe harbor is higher than what would be required to prove right and ability to control to establish common law vicarious liability (which is analyzed in section 4.11[4]). Prior disagreement between the Second and Ninth Circuits over what constitutes right and ability to control has been resolved in favor of the Second Circuit's interpretation that right and ability to control does not presuppose knowledge of specific infringing activity.⁷ According to the Second Circuit, what is required is "something more than the ability to remove or block access to materials posted on a service provider's website."⁸ That "something more" is understood in the Second and Ninth Circuits to involve exerting "substantial influence" on the activities of users, which may include high levels of control over user activities or purposeful conduct.⁹ Right and ability to control and financial interest are analyzed in section 4.12[6][D].

Second, a service provider must designate an agent to receive notifications of claimed infringement and publicize the name and contact information of the agent on its website and in a filing with the U.S. Copyright Office. Agent registration must be renewed every three years.¹⁰ Issues involving agent designation are briefly addressed in section 4.12[6][B] and more thoroughly analyzed in section 4.12[9][A].

⁴See *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37–38 (2d Cir. 2012).

⁵See *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004).

⁶See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026–31 (9th Cir. 2013).

⁷*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 36 (2d Cir. 2012) (disagreeing with the original Ninth Circuit opinion from 2011 in *Shelter Partners*, which was replaced, following reconsideration, by *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026–31 (9th Cir. 2013)).

⁸*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012), quoting *Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011).

⁹See *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013).

¹⁰See 37 CFR § 201.38.

Third, in response to a substantially complying notification, a service provider must disable access to or remove content identified in the notification.¹¹ This requirement is discussed in section 4.12[6][B] and analyzed more thoroughly in section 4.12[9][B].

Fourth, even in the absence of a notification, a service provider must, on its own initiative, disable access to or remove material where it has (a) actual knowledge of infringing activity or (b) awareness of facts or circumstances from which infringing activity is apparent (referred to in case law and the legislative history as material that raises a “red flag”¹²)—or risk losing DMCA protection for material stored at the direction of a user. The requirements for knowledge, awareness and corrective action are set forth in subsection 4.12[6][C]. As analyzed in that subsection, courts have held that generalized knowledge or awareness that a site or service may be used for infringing activity is *not* sufficient; only knowledge or awareness of specific files or activity will disqualify a service provider from the safe harbor’s protections pursuant to subsection 512(c)(1)(A).¹³

The Second and Ninth Circuits have held that actual knowledge denotes subjective belief, whereas red flag awareness is judged by an objective reasonableness standard.¹⁴

¹¹What it means to disable access to or remove material is addressed in section 4.12[6][C].

¹²Some courts refer to “red flag” *knowledge* but this terminology is confusing given that the statute addresses “actual knowledge” and “awareness of facts or circumstances from which infringing activity is apparent.” This treatise uses the term “‘red flag’ awareness” which describes the statutory provision more accurately.

¹³*See, e.g., Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93 (2d Cir. 2016); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 30–32 (2d Cir. 2012); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 609–10 (9th Cir. 2018); *Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1057 (9th Cir. 2017); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021–23 (9th Cir. 2013); *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) (quoting *Shelter Capital* with approval on this point); *infra* § 4.12[6][C].

¹⁴*See Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1025 (9th Cir. 2013) (quoting *Viacom v. YouTube*). The Ninth Circuit has underscored that “whether ‘the specific infringement’ is ‘objectively’ obvious to a reasonable person’ may vary depending on the facts proven by the copyright holder in establishing liability.” *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026 n.15 (9th Cir. 2013).

Both Circuits have also clarified that copyright owners, not service providers, have the obligation to investigate whether material on a site or service is infringing.¹⁵

While a service provider has no obligation to take down material in response to a defective notification sent by a copyright owner, and knowledge or awareness may not be inferred from a notification that does not substantially comply with the requirements of section 512(c)(3),¹⁶ the Ninth Circuit suggested in *dicta* that an unverified notice sent by a third party (as opposed to the copyright owner who filed suit against the service provider) potentially could provide red flag awareness.¹⁷ Hence, in litigation, red flag

¹⁵See 17 U.S.C.A. § 512(m); *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 89 (2d Cir. 2016) (“the DMCA explicitly relieves service providers from having to affirmatively monitor their users for infringement”); *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 94, 98 (2d Cir. 2016) (“§ 512(m) makes clear that the service provider’s personnel are under no duty to ‘affirmatively seek[]’ indications of infringement.”); “§ 512(m) relieves the service provider of obligation to monitor for infringements posted by users on its website.”); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) (“Section 512(m) is explicit: DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider. For that reason, § 512(m) is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that infringement may be occurring.”); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 603 (9th Cir. 2018) (“The Digital Millennium Copyright Act places the burden of policing infringement on the copyright owner, not on the person or firm storing and hosting the material.”); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1022 (9th Cir. 2013) (holding that the burden of policing for infringement is on the copyright owner; “Copyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers like Veoh, who cannot readily ascertain what material is copyrighted and what is not.”); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir.) (“The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright.”), *cert. denied*, 522 U.S. 1062 (2007).

¹⁶See 17 U.S.C.A. § 512(c)(3)(B)(i); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1020–21 n.12 (9th Cir. 2013).

¹⁷See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1024–25 (9th Cir. 2013). In *Shelter Capital*, UMG had argued that Veoh had red flag awareness of infringing material based on emails sent to Veoh executives by copyright owners, including an email sent by Disney’s CEO to Michael Eisner, a Veoh investor, stating that unauthorized copies of the movie *Cinderella III* and various episodes from the television show *Lost* were posted on Veoh’s site. The Ninth Circuit panel

awareness potentially could be shown by communications from third parties (other than the owner of a copyright allegedly infringed) or service provider records memorializing or referring to those communications, among other things.

Courts also have held that, even in the absence of proof of actual knowledge or red flag awareness, a service provider may be deemed to have knowledge or awareness where willful blindness is shown.¹⁸

Actual knowledge, red flag awareness or willful blindness may be shown, among other things, by internal communications—such as email messages, texts or communications on Slack, for example—evidencing that employees were aware of infringing material on a site.¹⁹

Knowledge or awareness also may be shown where a site proactively uses human review to monitor for infringing material. Service providers, under the DMCA, are not

explained that “[i]f this notification had come from a third party, such as a Veoh user, rather than from a copyright holder, it might meet the red flag test [assuming the material was not taken down in response to the notice] because it specified particular infringing material. As a copyright holder, however, Disney is subject to the notification requirements in § 512(c)(3), which this informal email failed to meet.” *Id.* (footnote omitted).

¹⁸See, e.g., *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 98-99 (2d Cir. 2016) (holding that Vimeo was not willfully blind); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) (holding that knowledge or awareness may be established by evidence of willful blindness, which the court characterized as a deliberate effort to avoid guilty knowledge); *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043 (9th Cir. 2013) (explaining that “inducing actions”—or measures deemed to induce copyright infringement—were relevant to the court’s determination that the defendant had red flag awareness); *Capitol Records, Inc. v. MP3Tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *3–4 (S.D.N.Y. May 14, 2013) (reconsidering its earlier ruling granting summary judgment for the service provider on plaintiff’s claim for contributory infringement of those songs not subject to DMCA-compliant takedown notices, in light of the importance the Second Circuit placed on explicit fact-finding in evaluating willful blindness as a potential bar to DMCA protection in *Viacom v. YouTube*, and holding that a jury could reasonably interpret several documents as imposing a duty to make further inquiries into specific and identifiable instances of possible infringement); see also *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1023 (9th Cir. 2013) (citing *Viacom v. YouTube* for the proposition that “a service provider cannot willfully bury its head in the sand to avoid obtaining . . . specific knowledge.”).

¹⁹See, e.g., *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 90, 93, 97 (2d Cir. 2016).

required to search for infringement.²⁰ Nevertheless, proactive monitoring can help keep infringement off a site, which in turn may discourage copyright owners from filing suit. Proactive monitoring also can help rebut any inference of willful blindness. While automated filtering can help insulate a service provider from liability, systematic human review of all files on a site could deprive a service provider of safe harbor protection for red flag material, as discussed further in section 4.12[6][C].

Encouragement to users to upload certain material could be evidence of willful blindness if the material is known to be infringing. Merely encouraging uploads of creative content, such as photographs or music, would not evidence willful infringement—especially if a service has a license for material in a given category.²¹

Although responding to red flag material is plainly a requirement under section 512(c) to benefit from the user storage safe harbor in a suit brought over that material, the Ninth Circuit, in *Perfect 10, Inc. v. CCBill, LLC*,²² effectively made ongoing compliance with notice, knowledge or awareness requirements under section 512(c) part of the threshold requirements for entitlement to any of the DMCA's safe harbors.

In *CCBill*, the Ninth Circuit construed the threshold requirement in section 512(i)(1) that, to qualify for any of the liability limitations, a service provider adopt, notify subscribers about and reasonably implement a policy of

²⁰See 17 U.S.C.A. § 512(m).

²¹See, e.g., *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1022-23 (9th Cir. 2013) (having a music category was not evidence of willful blindness where the site had licenses to numerous music videos; “merely hosting a category of copyrightable content, such as music videos, with the general knowledge that one’s services could be used to share infringing material, is insufficient to meet the actual knowledge requirement under § 512(c)(1)(A)(i)” or to establish red flag awareness); *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) (encouraging users to upload photographs was not evidence of willful blindness where the site offered a database of licensed photographs that users could copy; “Although BWP is correct in stating AXS encouraged Examiners to incorporate photographs into articles, AXS provided Examiners a legal means by which to accomplish this. Examiners have access to a photo bank full of images for which AXS owns the licenses.”); see generally *infra* § 4.12[6][C].

²²*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1111 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

terminating “repeat infringers” in “appropriate circumstances” to require consideration of whether a service provider has responded to material where it had actual knowledge or “red flag” awareness (as well as notifications from third parties) to determine whether it is in fact keeping track of repeat infringers and reasonably implementing its termination policy. Thus, as a practical matter, a service provider that fails to disable access to material in response to notice, knowledge or red flag awareness, potentially could run the risk, at least in the Ninth Circuit under *CCBill*, of not only losing the benefit of the user storage safe harbor in a suit over material that was not taken down, but being stripped of DMCA protection for any of the safe harbors in litigation brought by any copyright owner.

Thus far, no other circuit has read the requirements of section 512(c) into the threshold requirements of section 512(i)(1) in the same manner as the Ninth Circuit.²³ Indeed, a different Ninth Circuit panel, without addressing this aspect of *CCBill*, explained eleven years later, in 2018, that while subsection (i) limits the eligibility for safe harbor treatment—even to sites that honor DMCA notices and remove material where they have actual knowledge or red flag awareness—“subsection (c) of the safe harbor provision aims at individual infringements, not the service as a whole.”²⁴ The court explained:

It uses the phrase “the material”—that is, the material for which an infringement remedy is sought—in the context of setting out what a service provider needs to do to avoid liability for the infringement of the copyrighted material at issue. Our sister circuit and we both read it this way. If subsection (c) were read to apply to all the material on the website, instead of the material for which a remedy was sought by the victim of infringement, then no large site would be protected by the safe harbor. It is unimaginable that any website with hundreds of thousands or millions of user uploads could successfully screen out all of the copyright infringing uploads, or even all of the uploads where infringement was apparent.²⁵

The obligation to disable access to or remove material in

²³See *supra* § 4.12[3] (analyzing the threshold requirements of section 512(i)(1)).

²⁴*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 614 (9th Cir. 2018).

²⁵*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 614 (9th Cir. 2018) (footnote omitted; citing *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021–22 (9th Cir. 2013); *Capitol Records*,

response to notice, knowledge or red flag awareness is addressed in connection with the user storage liability limitation in sections 4.12[6][C] (knowledge and red flag awareness) and 4.12[6][B] (notifications), and under *CCBill*, as part of the threshold requirement to reasonably implement a repeat infringer policy, in section 4.12[3][B][iv].

The respective burdens placed on copyright owners (to search for infringement and provide notice) and service providers (to respond to notifications and act on their own in response to knowledge or red flag awareness) encourage copyright owners and service providers to cooperate with one another.²⁶

From a practical perspective, the user storage limitation benefits service providers by potentially allowing them to avoid litigation, and if sued to get out of a case on a motion for summary judgment based on their entitlement to the user storage safe harbor, rather than having to go to trial or otherwise litigate the ultimate issue of liability. Copyright owners, in turn, benefit to the extent that service providers are given a tangible incentive to provide them with a quick and easy remedy when infringing content has been posted online, in lieu of having to seek injunctive relief simply to have material taken down from a site or service.

By its terms, section 512(c) applies to “material that resides on a system or network controlled by or for the service provider . . . by reason of the storage at the direction of a user.”²⁷ In *Hendrickson v. eBay, Inc.*,²⁸ however, a federal court in California ruled, based on the express language of 17 U.S.C.A. § 512(c)(1)(A)(i),²⁹ that section 512(c) applies both to (a) cases where a plaintiff seeks to hold a service

LLC v. Vimeo, LLC, 826 F.3d 78, 93 (2d Cir. 2016); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012)).

²⁶The legislative history provides that the Act is intended to “preserve strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements” in cyberspace, while “[a]t the same time . . . provid[e] greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.” H. Rep. No. 105-796, 105th Cong. 2d Sess. 1, 72 (1998).

²⁷17 U.S.C.A. § 512(c)(1).

²⁸*Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

²⁹That section provides that a service provider may limit its liability under the user storage limitation if it “does not have actual knowledge that the material or an activity using the material on the system is infringing.”

provider responsible for infringing “material” stored and displayed on the service provider’s website *and* (b) infringing “activity using the material” on a service provider’s system, such as merely listing infringing works for sale. Without citing *Hendrickson*, the Ninth Circuit subsequently agreed.³⁰

In all cases, however, the material at issues must have been stored at the direction of a *user*—not the service provider itself or a third party.³¹ In *BWP Media USA, Inc. v. Clarity Digital Group, LLC*,³² the Tenth Circuit broadly construed the term *user* to apply to paid, independent contractors who contributed articles that were solicited by the service provider and posted on its site.³³ In so ruling, the court rejected the copyright owner’s argument that the term *user* should exclude “an ISP’s owners, employees, and agents, . . . [or] anyone who entered into a contract and received compensation from an ISP.”³⁴ Instead, the appellate court explained that “a ‘user’ is anyone who uses a website—no

³⁰See *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1042 (9th Cir. 2013) (holding that section 512(c), by virtue of the express terms of subsection 512(c)(1)(A)(i), “explicitly covers not just the storage of infringing material, but also the infringing ‘activit[ies]’ that ‘us[e] the material [stored] on the system or network.’”).

³¹See, e.g., *Capitol Records, Inc. v. MP3Tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *6 (S.D.N.Y. May 14, 2013) (holding that MP3Tunes was not entitled to the user storage safe harbor for album art copied from Amazon.com because “while MP3Tunes’ cover art algorithm retrieved and copied cover art solely in response to a user’s song collection, the cover art itself was provided by Amazon.com, not other MP3Tunes users.”).

³²*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175 (10th Cir. 2016).

³³According to the plaintiff, the service provider issued instructions on the general topics Examiners were to write about, actively solicited new articles, and suggested that Examiners include slide shows or pictures to accompany articles. In rejecting plaintiff’s arguments, the court explained that:

BWP. . . fails to explain how this evidence crosses the chasm between encouraging the Examiners to post pictures with articles and encouraging Examiners to post infringing content. Not only did AXS make clear copyright infringement was prohibited, it also provided Examiners with licensed photographs to accompany their articles. No reasonable trier of fact could find that the infringement was at the direction of AXS.

BWP Media USA, Inc. v. Clarity Digital Group, LLC, 820 F.3d 1175, 1181 (10th Cir. 2016).

³⁴*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1180 (10th Cir. 2016).

class of individuals is inherently excluded.”³⁵ Although it ruled that the paid contributors were independent contractors, the court noted in *dicta* that even employees may be *users* for purposes of section 512(c).³⁶

On the other hand, the Ninth Circuit, in *Mavrix Photographs, LLC v. LiveJournal, Inc.*,³⁷ held that whether material submitted by users of the LiveJournal site qualified as material stored at the direction of a user within the meaning of the DMCA depended on whether volunteer, unpaid moderators who reviewed user submissions under the direction of a LiveJournal employee, and approved them for posting to the site, were acting as agents of LiveJournal such that the user submissions were actually uploaded by LiveJournal itself, rather than users.

The Ninth Circuit found the question raised a disputed fact precluding summary judgment, where LiveJournal used volunteer moderators to screen posts with varying levels of authority. LiveJournal allowed “moderators” to review posts to ensure that they contained celebrity gossip and did not include pornography or harassing content. “Maintainers” were given further authority to delete posts and remove moderators. Finally, “owners” were authorized to remove maintainers. While LiveJournal argued that it did not assent to moderators acting on its behalf, the court found there was a disputed issue of fact over whether moderators had actual authority for purposes of establishing common law agency.³⁸ In so ruling, the court explained that in evaluating safe harbor protection under section 512(c), “public acces-

³⁵*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1180 (10th Cir. 2016).

³⁶*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1181 (10th Cir. 2016).

³⁷*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045 (9th Cir. 2017).

³⁸*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1054-55 (9th Cir. 2017). The panel found the issue of control exercised by LiveJournal was disputed. Moderators were free to leave, not required to volunteer their time and could reject submissions for reasons other than those provided by LiveJournal. On the other hand, the court found that LiveJournal selected moderators, provided them with specific directions and exercised some degree of control. The appellate panel also found that at least some users believed that moderators acted with apparent authority—although this should not be relevant to the question of whether user material on the site was stored “at the direction of a user” 17 U.S.C.A. § 512(c). The proper focus of section 512(c) should be on direction

sibility is the critical inquiry.”³⁹

LiveJournal is wrongly decided in holding that agency principles should control in evaluating whether material is stored by a user or by the service itself. The relevant inquiry under section 512(c) is not whether material is stored by a user (or uploading vs. submission, in the language of the court) but rather whether it is stored “at the direction of a user”⁴⁰ Thus, pre-upload review by a third party reviewer, an independent contractor or even an employee should not transform the nature of material if, prior to review, a user directed that the material be stored. Whether

from the user, not the user’s perception of whether moderators are agents of the site or independent third parties.

³⁹*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1053 (9th Cir. 2017). The Ninth Circuit disagreed with the Tenth Circuit’s approach in *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175 (10th Cir. 2016) to the extent that *BWP*, in holding that even employees or agents could be *users*, conflicted with this Ninth Circuit panel’s view that “common law principles of agency apply to the DMCA such that a service provider is liable for the acts of its agents, including employees” *Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1053 n.8 (9th Cir. 2017).

The Ninth Circuit initially held that “posting rather than submission” was the critical issue, but subsequently withdrew and reissued its opinion to clarify that “public accessibility” was the critical issue. *See Mavrix Photographs, LLC v. LiveJournal, Inc.*, 853 F.3d 1020, 1029-31 (9th Cir.), *withdrawn and replaced by*, 873 F.3d 1045, 1054-55 (9th Cir. 2017). In fact, the critical issue is whether the material was stored *at the direction of a user*, not whether it was publicly accessible. The Ninth Circuit’s analysis on this point is inconsistent with the plain terms of the statute.

In view of its ruling on the issue of whether the volunteer moderators acted as agents for LiveJournal, the appellate panel also vacated and remanded the lower court’s order denying motions to compel responses to interrogatories seeking discovery from LiveJournal’s unnamed volunteer moderators. The appellate court directed that:

Whether the moderators are agents should inform the district court’s analysis of whether Mavrix’s need for discovery outweighs the moderators’ interest in anonymous internet speech. Given the importance of the agency analysis to the ultimate outcome of the case, and the importance of discovering the moderators’ roles to that agency analysis, the district court should also consider alternative means by which Mavrix could formally notify or serve the moderators with process requesting that they appear for their deposition at a date and time certain.

873 F.3d at 1059-60; *see generally infra* § 37.02 (analyzing the opinion in the context of the balancing test applied by courts in the Ninth Circuit in seeking to unmask the identity of anonymous or pseudonymous actors online).

⁴⁰17 U.S.C.A. § 512(c) (emphasis added).

material is directly uploaded by a user or by a reviewer might be relevant if the statute focused on whether material was stored by a user or the service provider. However, the statute provides that the relevant consideration is whether material is stored *at the direction* of a user, not *by* a user, so it should not matter who actually stores it, so long as it is stored at the user's direction.

The statute likewise does not provide that the term *user* should be construed narrowly or under principles of agency. The Tenth Circuit's analysis in *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, rather than the Ninth Circuit's construction in *LiveJournal*, is more consistent with the plain terms of the statute.

In addition to narrowly construing the term *user*, the Ninth Circuit, in *dicta* in *LiveJournal*, further elaborated on how, on remand, the lower court should construe the term "direction of the user." The panel wrote that "accessibility-enhancing activities" would not take a service provider outside the safe harbor, but "extensive, manual, and substantive activities" that go "beyond the automatic and limited manual activities we have approved as accessibility-enhancing" would mean the uploaded content was not stored *at the direction of a user*.⁴¹ The court explained that "[p]osts are at the direction of the user if the service provider played no role in posting them on its site or if the service provider carried out activities that were "narrowly directed towards enhancing the accessibility of the posts."⁴² The panel elaborated that

[a]ccessibility-enhancing activities include automatic processes, for example, to reformat posts or perform some technological change. *Shelter Capital*, 718 F.3d at 1020 (referring to accessibility-enhancing activities as those where the service provider did "not actively participate in or supervise file uploading"). Some manual service provider activities that screen for infringement or other harmful material like pornography can also be accessibility-enhancing. *Id.* at 1012 n.2. Indeed, § 512(m) of the DMCA provides that no liability will arise from "a service provider monitoring its service or af-

⁴¹*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1056 (9th Cir. 2017).

⁴²*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1056 (9th Cir. 2017).

firmatively seeking facts indicating infringing activity.” *Id.* at 1022 (quoting 17 U.S.C. § 512(m)).⁴³

Needless to say, this analysis is unsupported by the plain terms of the statute. It also constitutes terrible public policy—by discouraging service providers from manually reviewing material submitted by users for infringement or harmful content, at least before the material is uploaded to the site.⁴⁴

LiveJournal was read more narrowly by a subsequent Ninth Circuit panel in *Ventura Content, Ltd. v. Motherless*,

⁴³*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1056 (9th Cir. 2017). In *LiveJournal*, the court found the issue disputed because moderators manually reviewed submissions for their content (approving only those posts relevant to “new and exciting celebrity gossip”) and publicly posted only about one-third of them. *Id.* The court remanded with instructions for the factfinder to determine “whether LiveJournal’s manual, substantive review process went beyond the automatic processes we have approved as accessibility-enhancing activities such that the posts were still at the direction of the user.” *Id.* n.12.

⁴⁴A narrow reading of *LiveJournal* could allow post-upload review, but not pre-upload review, for material to qualify as stored “at the direction” of a user. Pre-upload review, under *LiveJournal*, could at the very least create a factual question precluding summary judgment, if not entirely taking material outside the safe harbor, if the upload process is not automated. Post-upload review should not put in jeopardy the status of material as stored “at the direction of a user” if the material is uploaded automatically, rather than manually, by a site or service. Thus, *LiveJournal* suggests that it would be better for a service provider to review material after it has been uploaded, rather than to review submissions prior to upload and manually determine which ones to post (even though there is no basis in the language of the DMCA or its legislative history to countenance this approach, which actually increases the likelihood that infringing material will be uploaded to a site and potentially copied or further distributed by other users before it is reviewed and proactively removed).

Yet, even post-upload review is not entirely risk free under *LiveJournal*. If a reviewer inspects but fails to recognize and remove material, this could raise questions about whether the service had knowledge or red flag awareness of material reviewed but left online, depending on the facts of a case. *See infra* § 4.12[6][C].

Ultimately, the safest approach for a service provider could be to simply include a button next to each user submission for the community to report material that appears to be infringing. In this way, the service would escape entirely questions of knowledge or awareness by not reviewing every user upload, even though there are both legal and business reasons for many sites to take a more proactive approach, where it is feasible to do so (including to negate any inference of willful blindness, even though under section 512(m) service providers have no obligation to proactively monitor for infringement). *See infra* § 4.12[6][C].

Inc.,⁴⁵ which held *LiveJournal* inapplicable where a service provider monitors uploaded content solely to screen for illegal material, rather than to apply a discretionary standard of what type of material to allow to be posted to a site. In *Motherless*, defendant Lange had uploaded 700,000 files from a previous website, *Hidebehind.com*, when he established the *Motherless* website in 2008. By the time of the lawsuit, these files amounted to 6% of the content on the site. The court emphasized, however, that none of the 33 video clips at issue in the suit had been uploaded by Lange or his one contractor. Nor was there any evidence that any of the 700,000 files transferred from *Hidebehind.com* were infringing.

The panel explained that section 512(m) requires that the DMCA not be construed to eliminate safe harbor protection for monitoring for infringement or disabling access to illegal material. In *Motherless*, the service provider had adopted a policy that anything legal would remain on the site. Lange and his contractor screened out child pornography, which is illegal under U.S. law, and bestiality, which is prohibited by some European countries. The panel explained that it found it “counterintuitive, to put it mildly, to imagine that Congress intended to deprive a website of the safe harbor because it screened out child pornography and bestiality rather than displaying it.”⁴⁶ Instead, it “read section 512(m) to say that Congress expressly provided that such screening does not deprive a website of safe harbor protection.”⁴⁷ The court also rejected plaintiff’s argument that by using software to highlight the “Most Popular” material, and by giving credits to users who posted the most material, *Motherless* was responsible for user uploads, as inconsistent with *UMG* as well as “inconsistent with the meaning of the words ‘at the direction of the user’ ”⁴⁸

Thus, as modified by *Motherless*, *LiveJournal* appears to apply only where a site or its agents potentially pick and

⁴⁵*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 604-08 (9th Cir. 2018).

⁴⁶*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 605 (9th Cir. 2018).

⁴⁷*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 605 (9th Cir. 2018).

⁴⁸*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 606 (9th Cir. 2018).

choose which user submitted content to be displayed on a site based on subjective criteria. Where material is reviewed solely for compliance with the law, *Motherless* holds that a service provider will not be deprived of potential safe harbor protection for material stored “at the direction of a user” solely for undertaking this type of review.

Subsequently, a district court in the Southern District of New York (in the Second Circuit) granted summary judgment for Oath, holding that a user-submitted photo added to a Huffington Post article by the user constituted material stored at the direction of a user notwithstanding “ cursory screening” by Oath for offensive and illegal content, and Oath’s addition of content tags and related video links.⁴⁹

The Second Circuit, while not specifically addressing the Ninth Circuit’s analysis, added its own potential wrinkle to the definition of what constitutes material stored at the direction of a user in *BWP Media USA Inc. v. Polyvore, Inc.*,⁵⁰ in which one member of the appellate panel that decided the case raised the specter of a service provider losing DMCA protection for making more than one copy of user-submitted content. In *Polyvore*, the Second Circuit remanded the case for consideration of whether the service provider could be held directly liable for making additional copies of user-uploaded photographs, in a case where the district court had not needed to address the issue of the provider’s possible entitlement to the DMCA safe harbor (because it entered summary judgment for the defendant on different grounds) and where the appellate panel lacked a sufficiently detailed factual record to evaluate its potential entitlement. The Second Circuit did not hold that a service provider could lose safe harbor protection for making multiple copies, but this possibility was suggested by one of the judges in a concurring opinion.

Polyvore is a messy decision. It includes a short *per curiam* opinion, remanding the case for consideration of the applicability of the DMCA without any direction on this issue, and three separate concurring opinions—one by each member of the appellate panel—addressing different aspects of the decision where there was disagreement.

⁴⁹See *Downs v. Oath Inc.*, 385 F. Supp. 3d 298, 303-05 (S.D.N.Y. 2019) (granting summary judgment for Oath on its entitlement to the DMCA safe harbor).

⁵⁰*BWP Media USA Inc. v. Polyvore, Inc.*, 922 F.3d 42 (2d Cir. 2019).

Judge Walker, in his concurring opinion, wrote that making copies “solely to facilitate user access” was protected by the safe harbor, but considered there to be a factual question over whether copies beyond the first copy made by Polyvore were made “solely to facilitate access by users” because Polyvore, as the party with the burden of proof to establish its entitlement to the safe harbor, had not pointed to evidence in the record explaining why these copies had been made.⁵¹ Polyvore, through its “Clipper” tool, allowed users to “clip” images from other websites that they could store, modify, crop, or superimpose on top of other images to make a digital photo collage. Polyvore’s software, in turn, automatically made multiple copies of each image in varying sizes, each of which was assigned a unique URL on the site.

Judges Newman and Pooler did not address this issue in their separate opinions, and agreed with Judge Walker only to the extent that they concurred that remand to the district court was appropriate to evaluate Polyvore’s entitlement to the DMCA safe harbor. Judge Pooler, however, expressed skepticism that Polyvore’s practice of automatically making multiple copies of images should result in liability, in discussing the volitional conduct requirement for direct infringement,⁵² which by analogy should be relevant as well to safe harbor analysis. Judge Pooler cited the amicus curiae brief of the Electronic Frontier Foundation for the proposition that it was “routine” and “very common” for websites to automatically generate copies of images in different sizes to allow users to view images on various devices, questioning the logic of treating a single copy as protected but further copies as potentially infringing.⁵³ By extension, there does not appear to be any logical reason to treat an initial copy as material stored at the direction of a user but to treat subsequent copies automatically generated on the same site as potentially stored without user direction. Likewise, there is nothing in the DMCA or its legislative history to support Judge Walker’s cramped view that the safe harbor applies *solely* to copies made to facilitate user access. Ultimately, Judge Walker’s lone concurrence should not be viewed as

⁵¹*BWP Media USA Inc. v. Polyvore, Inc.*, 922 F.3d 42, 58 (2d Cir. 2019) (Walker, J. concurring).

⁵²See *supra* § 4.11[2] (analyzing direct liability).

⁵³See *BWP Media USA Inc. v. Polyvore, Inc.*, 922 F.3d 42, 69 (2d Cir. 2019) (Pooler, J. concurring).

persuasive authority.

Notwithstanding some aberrational viewpoints on what constitutes material stored at the direction of a user, Second and Ninth Circuit case law is actually very favorable to service providers. Where applicable, both the Second and Ninth Circuits have construed the user storage safe harbor broadly to apply not only literally to the act of a user storing material but to any instance where liability is sought to be imposed “by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider”⁵⁴ In parallel cases involving user generated video sites, both circuits *rejected* the argument that transcoding videos uploaded by users—or converting them into a standard display format so that they could be viewed by other users regardless of the software used to create the video—and creating a “playback” feature (delivering a copy of a video to a user’s browser cache so that an uploaded video, once transcoded, could be viewed by others), transformed the uploaded works from material stored at the direction of a user (and therefore subject to the safe harbor) into new works for which the site itself could be held liable.⁵⁵

The Second Circuit further held that YouTube’s “related video” function—which displayed thumbnail images of clips determined automatically by a search algorithm to be “related” to a video selected for viewing by a user—did not bring YouTube outside the safe harbor, but remanded for further consideration the narrow question of whether third-party syndication of videos uploaded to YouTube was covered by the DMCA’s user storage safe harbor (if in fact any of the videos at issue had been syndicated, which was a fact issue to be considered on remand).⁵⁶ On remand, the district court held that YouTube’s practice of syndicating user content to third-party mobile providers did not take YouTube outside the safe harbor because the videos syndicated to Apple, Sony, Panasonic, TiVo and AT&T remained stored on YouTube’s servers and merely provided an alternative way to view ma-

⁵⁴17 U.S.C.A. § 512(c)(1).

⁵⁵*See Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38–40 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1015–20 (9th Cir. 2013).

⁵⁶*See Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38–40 (2d Cir. 2012).

terial stored by users.⁵⁷

The Ninth Circuit did not address the “related video” feature or syndication, but did consider other functions of a user generated video site, holding that a service provider did not lose safe harbor protection for creating chunked and flash files or allowing users to stream or even download videos from the site.⁵⁸

The Second and Ninth Circuits have, in effect, set a bright line standard for determining whether a service provider is entitled to the user storage liability created by section 512(c) for material initially stored by a user which looks to whether liability is sought to be imposed “by reason of” material stored “at the direction of a user”⁵⁹—and not what the site or service does with the material once stored by a user, or where on a site or service it is stored (or how prominently), so long as it “resides on a system or network controlled or

⁵⁷See *Viacom Int’l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 122-23 (S.D.N.Y. 2013). YouTube’s syndication agreements with these companies allowed them to access videos directly from YouTube’s servers to make user-submitted videos accessible to their customers using mobile devices, tablets and Internet-enabled television sets. Pursuant to these agreements, YouTube automatically transcoded user-uploaded videos into formats compatible with third party devices. YouTube’s standard syndication licenses involved “no manual selection of videos by YouTube, and the videos accessible via the third-party devices at all times remain[ed] stored on and accessed only from YouTube’s system.” *Id.* at 122. Judge Stanton therefore concluded that “[t]his ‘syndication’ serves the purpose of § 512(c) by ‘providing access to material stored at the direction of users,’ . . . and entails neither manual selection nor delivery of videos.” *Id.* (citations omitted). In rejecting Viacom’s argument that YouTube’s syndication agreements took YouTube outside the safe harbor because the agreements were entered into for YouTube’s own business purposes, Judge Stanton wrote that “the critical feature of these transactions is not the identity of the party initiating them, but that they are steps by a service provider taken to make user-stored videos more readily accessible (without manual intervention) from its system to those using contemporary hardware. They are therefore protected by the § 512(c) safe harbor.” *Id.* at 123.

Judge Stanton did not address YouTube’s separate practice of manually selecting videos to copy and remove from YouTube’s system, which were hand delivered to Verizon to make available on its own system, because none of the allegedly infringing videos at issue in the case had been syndicated to Verizon. See *id.* at 122.

⁵⁸See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1015–20 (9th Cir. 2013).

⁵⁹17 U.S.C.A. § 512(c)(1).

operated by or for the service provider”⁶⁰ The Ninth Circuit explicitly, and the Second Circuit implicitly, apply a broad “but for” standard of general causation, rather than a proximate cause test, in evaluating whether a claim is based on material stored at the direction of a user, and therefore subject to the safe harbor.⁶¹ If, but for the act of user storage, a service provider would not be exposed to liability for copyright infringement, then the service provider is entitled to the safe harbor (assuming it meets the other requirements for eligibility) regardless of what else it does with the material stored by the user on its site or service. To benefit from the liability limitation, a claim need not relate narrowly to a user’s act of storing material. Rather, the safe harbor applies if liability is premised on material that was stored at the direction of a user. Accordingly, a service provider that otherwise meets the eligibility requirements for the safe harbor will be insulated from liability for material stored at the direction of a user regardless of whether it is buried in a private storage locker in the cloud or prominently featured for public display on the homepage of a website⁶²—or anywhere in between—and may be made available for users to stream (and in the Ninth Circuit, even download), provided that liability is premised on material stored at the direction of a user and the service provider does not do something with the material to bring itself outside the safe harbor, such as compiling user material for distribution on a DVD or broadcast television or otherwise outside of “a system or network controlled or operated by or for the service

⁶⁰17 U.S.C.A. § 512(c)(1).

⁶¹This analogy was articulated expressly by the Ninth Circuit. See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1017 n.6 (9th Cir. 2013). It is also consistent with the way the Second Circuit construed the DMCA’s user storage safe harbor in *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012); see also *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1180-82 (10th Cir. 2016) (broadly defining *user* for purposes of storage “at the direction of a user,” in affirming summary judgment for the operator of Examiner.com based on its entitlement to the DMCA safe harbor).

⁶²If material that appears to be infringing is prominently made available on a site or service it could raise red flag awareness issues if observed by a service provider’s employees and not removed (see *infra* § 4.12[6][C]), but the prominence of its display would not change its character as material stored at the direction of a user.

provider . . . ,”⁶³ beyond which DMCA safe harbor protection does not extend.⁶⁴

⁶³17 U.S.C.A. § 512(c)(1).

⁶⁴In another case, the Ninth Circuit went further, ruling that the user storage safe harbor potentially even applies in narrow circumstances where the infringing material itself is not resident on a defendant’s “system or network” because subsection 512(c)(1)(A)(i) “explicitly covers not just the storage of infringing material, but also the infringing ‘activit[ies]’ that ‘us[e] the material [stored] on the system or network.’” *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1042 (9th Cir. 2013) (explaining that “the infringing activity associated with Fung—the peer-to-peer transfer of pirated content—relied upon torrents stored on Fung’s websites.”). In the context of the *Fung* case itself, however, this analysis was faulty. Section 512(c), by its terms, is limited to situations where liability is based on “storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider” 17 U.S.C.A. § 512(c)(1). The reference to *activity* in section 512(c)(1)(A)(i) accounts for the fact that the material residing on a system or network may not inherently be infringing. For example, a user lawfully may store a copy of a work in a cloud storage locker, but the act of selling access to that otherwise noninfringing copy to numerous third parties may amount to infringing activity in the form of unauthorized reproduction of an otherwise noninfringing copy. Hence, section 512(c)(1)(A)(i) stipulates that to be entitled to the safe harbor a service provider may “not have actual knowledge that the material *or an activity using the material* on the system or network is infringing” *Id.* § 512(c)(1)(A)(i) (emphasis added). This statement of one of several eligibility requirements for the safe harbor cannot reasonably be seen to modify the unambiguous provision at the outset of section 512(c)(1) that, if the various eligibility requirements (including section 512(c)(1)(A)(i)) are met, a service provider “shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated *by or for the service provider*” *Id.* § 512(c)(1) (emphasis added).

Even if this were not the case, the Ninth Circuit’s implicit definition of *material* to include torrent files, rather than material that may be infringed or infringing (or form the basis for liability for infringement), does not make sense in the context of section 512(c). Section 512(c)(1)(A)(i), by its terms, requires that any “activity” involve *material* on the service provider’s system or network. *See id.* § 512(c)(1)(A)(i) (mandating that a service provider “not have actual knowledge that the material *or an activity using the material on the system or network* is infringing”; emphasis added). While liability for copyright infringement could be imposed for activities that use torrent files stored on a defendant’s servers, the safe harbor, by its terms, applies where liability is premised on “infringement of copyright *by reason of* the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider” *Id.* § 512(c)(1) (emphasis added). The “materials” identified by the Ninth Circuit in *Fung* were tracker files,

Case law on the scope of the user storage liability limita-

which are index files that enable works to be assembled using the BitTorrent file sharing protocol but which themselves contain no copyrighted content. See *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1027 (9th Cir. 2013). Torrent files on their own are more akin to links (or “information location tools,” covered by section 512(d)) since they do not contain copyrighted material. Liability in *Fung* was not pursued by plaintiffs *by reason of* the storage of tracker files, but based on active inducement by the defendants (see *supra* § 4.11[5]), of which the presence of tracker files was merely once component that alone could not have formed the basis for copyright liability.

By contrast, in *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001), the district court found that the DMCA applied to sales by eBay where the activity was “infringing activity—the sale and distribution of pirated copies of ‘Manson’ [a DVD]—using ‘materials’ posted eBay’s website [a user’s sales listing]” *Id.* at 1088. Unlike the presence of trackers in *Fung*, the material at issue in *Hendrickson* was the basis for plaintiff’s copyright infringement suit. But for those listings, eBay could not have been held liable. On the other hand, in *Fung*, even without the presence of tracker files stored by users the defendants still would have been found liable for copyright inducement. See *supra* § 4.11[5] (discussing the *Fung* case in greater detail).

The district court in *Fung* ultimately may have been correct in concluding that section 512(c) simply was inapplicable in *Fung*. While the Ninth Circuit was correct in noting that section 512(c) is not limited to material stored on a defendant’s *server* (because the statute, by its terms, references a “system or network controlled or operated by or for the service provider,” *id.* § 512(c)(1)), the panel’s interpretation that section 512(c) extends to activities that use material (with *material* defined broadly to mean torrent files, and not more narrowly material for which direct copyright liability may be imposed), based on language used in a subsection defining an eligibility requirement for the safe harbor, appears to be incorrect.

It may be possible that on these facts or others that a “system or network” could be construed to cover BitTorrent trackers or swarms or other systems or networks where collectively material is stored in pieces and thereafter reassembled. The mere reference in section 512(c)(1)(A)(i) to *an activity*, however, is not the proper rationale for holding that the user storage safe harbor may be applicable in a case where merely some torrents may have been stored on *Fung*’s website.

In *Masck v. Sports Illustrated*, 5 F. Supp. 3d 881, 888 (E.D. Mich. 2014), the court, without much elaboration, denied Walmart’s motion for summary judgment on its entitlement to the DMCA safe harbor, seemingly crediting the plaintiffs’ argument that unlike Amazon.com, Walmart operates both online and in physical stores, and that the DMCA safe harbor may not be available for retail operations in the physical world, although the court was not entirely clear on the basis for its denial.

Similarly, in *Atari Interactive, Inc. v. Redbubble, Inc.*, 515 F. Supp. 3d 1089, 1114 (N.D. Cal. 2021), the court ruled, without much analysis, that print-on-demand service Redbubble was not entitled to safe harbor protection because, although the images at issue had been uploaded by

tion for user-uploaded video sites evolved from a pair of California district court rulings in 2008, both of which shaped the law in the Ninth Circuit and were subsequently relied upon by the Second Circuit as well. In the first case to consider the applicability of the DMCA user storage safe harbor to a user generated video site, *Io Group, Inc. v. Veoh Networks, Inc.*,⁶⁵ Northern District of California Magistrate Judge Howard Lloyd rejected the argument that a service provider's actions in transcoding user submitted videos changed the character of the material from that stored at the direction of a user (and therefore within the safe harbor) to material that "resides on the system or network operated by or for the service provider through its own acts or decisions and not at the direction of a user."⁶⁶ Among other things, Veoh transcoded uploaded videos so that they would play in flash format. It also extracted a still image from the video that it displayed along with information about the video to more effectively index the videos. The court, however, held that Veoh was not disqualified from the protections of the safe harbor on these grounds.

In granting summary judgment for the defendant based on its entitlement to the DMCA user storage safe harbor, Magistrate Judge Lloyd ruled that the "structure and language" of the safe harbor make clear that section 512(c) is "not limited to merely storing material."⁶⁷ Judge Lloyd noted that whereas the definition of service provider for purposes of the "conduit only" functions under section

third party artists to the Redbubble platform, Redbubble had not met its burden on summary judgment to establish that the images were stored "at the direction of the user" because "Redbubble actively participate[d] in modifying the files uploaded by users to display the designs on Redbubble-selected physical products." *Id.* This analysis is suspect, however, given the broad *but for* analysis adopted by the Ninth Circuit (which was not discussed in the opinion, and may not have been raised in *Atari*). See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1017 n.6 (9th Cir. 2013). It is likewise difficult to reconcile this holding with *Shelter Capital* given the similarity between automated print-on-demand services and the downloading approved of by the Ninth Circuit in that case. See *id.* at 1015-20.

⁶⁵*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

⁶⁶*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1146 (N.D. Cal. 2008) (quoting legislative history).

⁶⁷*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1147 (N.D. Cal. 2008).

512(a)⁶⁸ is very narrow (only applying to an entity “offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, *without modification to the content of the material* as sent or received”),⁶⁹ “no such limitation as to the modification of material is included in the broader definition of ‘service provider,’ ” that is applicable under section 512(c),⁷⁰ which the parties stipulated applied to Veoh. The court concluded that “[h]ad Congress intended to include a limitation as to a service provider’s modification of user-submitted information, it would have said so expressly and unambiguously.”⁷¹

Judge Lloyd also noted that case law supported “the conclusion that Veoh is not precluded from [the] safe harbor under Section 512(c) by virtue of its automated processing of user-submitted content.”⁷² He explained that in *CoStar Group, Inc. v. LoopNet, Inc.*,⁷³ the court held that the defendant was entitled to the user storage limitation even though its employees manually reviewed photos submitted by users and posted to the website only those that met the defendant’s criteria (photos that depicted real estate and did not appear to be obviously copyrighted). Judge Lloyd explained that the *LoopNet* court “concluded that the photos were uploaded, in the first instance, at the volition of users and that defendant’s employees simply performed a ‘gateway’ function that furthered the goals of the DMCA.”⁷⁴

⁶⁸See *supra* § 4.12[4].

⁶⁹586 F. Supp. 2d at 1147, *quoting* 17 U.S.C.A. § 512(k)(1)(A) (emphasis added by the court).

⁷⁰17 U.S.C.A. § 512(k) creates two different definitions for *service provider*, a broad one generally applicable to the various DMCA safe harbors and a narrower one applicable only to the transitory digital network communications safe harbor created by section 512(a). See *generally supra* § 4.12[2].

⁷¹*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1147 (N.D. Cal. 2008).

⁷²*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1147 (N.D. Cal. 2008).

⁷³*CoStar Group Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688 (D. Md. 2001), *aff’d*, 373 F.3d 544, 556 (4th Cir. 2004).

⁷⁴*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1147–48 (N.D. Cal. 2008), *citing CoStar Group Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 702 (D. Md. 2001), *aff’d on other grounds*, 373 F.3d 544 (4th Cir. 2004).

In *Io Group, Inc. v. Veoh Networks, Inc.*, Judge Lloyd similarly reasoned that Veoh had simply established a system whereby software automatically processes user-submitted content and recasts it in a format that is readily accessible to users. Veoh preselects the software parameters . . . [b]ut Veoh does not itself actively participate or supervise the uploading of files. Nor does it preview or select the files before the upload is completed. Instead, video files are uploaded through an automated process which is initiated entirely at the volition of Veoh's users.⁷⁵

Later that year, in *UMG Recordings, Inc. v. Veoh Networks, Inc.*,⁷⁶ Judge Howard Matz of the Central District of California, denied Universal Music Group's motion for partial summary judgment in its suit against Veoh, based on an even broader challenge to its entitlement to the user storage liability limitation, in an opinion that subsequently was affirmed by the Ninth Circuit in 2013.⁷⁷ Whereas *Io Group* involved the issue of transcoding (or creating flash-formatted copies of video files), UMG argued that four of the things Veoh did to uploaded videos to make them viewable and downloadable on its site (including transcoding) did not involve "storage" and were not undertaken "at the direction of a user." Specifically, UMG challenged software functions that: (1) automatically created "flash-formatted" copies of video files uploaded by users; (2) automatically created copies of uploaded video files that were comprised of smaller 256-kilobyte "chunks" of the original file; (3) allowed users to access uploaded videos via streaming; and (4) allowed users to download entire video files. While the court did not address the question of whether these functions were actually infringing, Judge Matz noted that it was undisputed that all

⁷⁵*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008).

⁷⁶*UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081 (C.D. Cal. 2008), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁷⁷The Ninth Circuit originally affirmed Judge Matz's decision in *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022 (9th Cir. 2011), which was withdrawn and replaced by a new opinion on motion for reconsideration in light of the Second Circuit's disagreement with *Shelter Capital Partners* on the issue of what constitutes right and ability to control. The panel's subsequent opinion affirming Judge Matz's order revised its prior analysis to conform to the Second Circuit. *See UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

of these software functions were directed toward facilitating access to materials stored at the direction of users.

In denying UMG's motion, the district court rejected UMG's argument for a narrow interpretation of the user storage liability limitation that would have extended protection to operational features only if they provided or constituted storage. Judge Matz did not deem it necessary to define the outermost limits of the safe harbor, but agreed with Veoh that the language of section 512(c) is "broad" and that Veoh was not disqualified from protection because of automated processing of user uploaded material to allow users to be able to view and access it when stored on Veoh's site. He explained that:

The critical statutory language really is pretty clear. Common sense and widespread usage establish that "by reason of" means "as a result of" or "something that can be attributed to." So understood, when copyrighted content is displayed or distributed on Veoh it is "as a result of" or "attributable to" the fact that users uploaded the content to Veoh's servers to be accessed by other means. If providing access could trigger liability without the possibility of DMCA immunity, service providers would be greatly deterred from performing their basic, vital and salutary function—namely, providing access to information and material for the public.⁷⁸

Judge Matz noted that section 512(c) "codifies the 'notice and takedown' procedure Congress instituted so that service providers and copyright owners could cooperate to protect copyrights."⁷⁹ Under UMG's theory, he wrote, the "safe harbor" would in fact be full of treacherous shoals if the copyright owner still could recover damages because the service provider remained liable for having provided access to the stored material that had been removed."

Judge Matz found that the legislative history and case law⁸⁰ bolstered his interpretation of the plain text of section 512(c), which he found "extend[s] to functions directly

⁷⁸*UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1089 (C.D. Cal. 2008), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁷⁹*UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1089 (C.D. Cal. 2008), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁸⁰*See UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1091–92 (C.D. Cal. 2008) (discussing prior case law), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

involved in providing access to material stored at the direction of a user.”⁸¹ Citing to the House Report’s explanation that section 512 was intended to preserve strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringement, he wrote that “this cooperative process would be pointless if service providers who provide access to material stored on their systems at the direction of users were precluded from limiting their potential liability merely because their services enabled users to access such works.”⁸² The threat of this liability “would create an enormous disincentive to provide access, thereby limiting the ‘variety and quality of services on the Internet.’”⁸³

The following year, Judge Matz granted summary judgment in favor of Veoh, finding that the DMCA user storage safe harbor insulated Veoh from all of UMG’s copyright claims.⁸⁴

On appeal, the Ninth Circuit characterized the question as “whether the functions automatically performed by Veoh’s software when a user uploads a video fall within the meaning of ‘by reason of the storage at the direction of a user.’”⁸⁵ The appellate panel answered this question in the affirmative, rejecting UMG’s argument that *storage* did not encom-

⁸¹*UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1090 (C.D. Cal. 2008), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁸²*UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1091 (C.D. Cal. 2008), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁸³*UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081 (C.D. Cal. 2008) (citing S. Rep. 105-190, at 8 (“In the ordinary course of their operations service providers must engage in all kinds of acts that expose them to potential copyright infringement liability [B]y limiting the liability of service providers, the DMCA ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.”)), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁸⁴*See UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009) (granting Veoh’s motion for summary judgment, holding that Veoh was entitled to the DMCA safe harbor), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁸⁵*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1015 (9th Cir. 2013).

pass the automatic processes undertaken by Veoh to allow public access to user-uploaded videos, based on the court's reading of "the language and structure of the statute, as well as the legislative intent that motivated its enactment"⁸⁶ Although the Ninth Circuit did not identify the outer reaches of the term *by reason of the storage at the direction of a user*, in rejecting UMG's argument for a narrow construction the appellate panel implied in *dicta* that "by reason of" in the context of the DMCA "should be read to require only 'but for' rather than proximate causation."⁸⁷

Judge Raymond C. Fisher, writing for himself and Judges Harry Pregerson and Marsha S. Berzon, emphasized that their doubts about UMG's narrow reading of the statutory term were confirmed by the fact that UMG's interpretation would lead to internal statutory conflicts:

By its terms, § 512(c) presupposes that service providers will provide access to users' stored material, and we would thus contravene the statute if we held that such access disqualified Veoh from the safe harbor. Section 512(c) codifies a detailed notice and takedown procedure by which copyright holders inform service providers of infringing material accessible through their sites, and service providers then "disable access to" such materials. 17 U.S.C. § 512(c)(1)(A)(iii), (c)(1)(C) & (c)(3)(A)(iii) (emphasis added). This carefully considered protocol, and the statute's attendant references to "disabl[ing] access" to infringing materials, *see id.*, would be superfluous if we accepted UMG's constrained reading of the statute. *See Greenwood v. CompuCredit Corp.*, 615 F.3d 1204, 1209 (9th Cir. 2010) ("We must, if possible, interpret a statute such that all its language is given effect, and none of it is rendered superfluous." (citing *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001))). Indeed, it is not clear how copyright holders could

⁸⁶*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1016 (9th Cir. 2013).

⁸⁷*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1017 n.6 (9th Cir. 2013) (citing and discussing cases interpreting similar language in other statutes). The court explained that:

"'But for' causation is a short way of saying '[t]he defendant's conduct is a cause of the event if the event would not have occurred but for that conduct.' It is sometimes stated as 'sine qua non' causation, i.e., 'without which not'" *Boeing Co. v. Cascade Corp.*, 207 F.3d 1177, 1183 (9th Cir. 2000). "In determining whether a particular factor was a but-for cause of a given event, we begin by assuming that that factor was present at the time of the event, and then ask whether, even if that factor had been absent, the event nevertheless would have transpired in the same way." *Price Waterhouse v. Hopkins*, 490 U.S. 228, 240 (1989) (plurality opinion)

Id.

even discover infringing materials on service providers' sites to notify them as the protocol dictates if § 512(c) did not contemplate that there would be access to the materials.⁸⁸

The appellate panel likewise rejected what it characterized as UMG's "novel theory" that Congress intended for the user storage safe harbor to apply only to web hosting services, citing the Electronic Frontier Foundation's *amicus curiae* brief for the proposition that "these accessing activities define web hosting—if the web host only stored information for a single user, it would be more aptly described as an online back-up service."⁸⁹ The panel emphasized that the language of the statute itself contemplated activities that went beyond mere storage in immunizing both infringing material and *activity*⁹⁰ and in providing that, to comply with the safe harbor for infringing *activity*, service providers must remove or *disable access to* allegedly infringing material, "suggesting that if the material were still being stored by the service provider, but was inaccessible, it might well not be infringing."⁹¹ The court also noted that if Congress had wanted to confine section 512(c) exclusively to web hosts, rather than reach a wider range of service providers, it likely would have made that clear in the definition of *service provider* which is narrowly defined only for section 512(a) (the safe harbor for routing) but more broadly defined for the other safe harbors, including section 512(c).⁹² Quoting from Judge Lloyd's opinion in *Io Group, Inc. v. Veoh Networks, Inc.*, the Ninth Circuit concluded that:

"Veoh has simply established a system whereby software automatically processes user-submitted content and recasts it in a format that is readily accessible to its users." *Id.* at 1148. Veoh does not actively participate in or supervise file uploading, "[n]or does it preview or select the files before the upload is completed." *Id.* Rather, this "automated process" for making files accessible "is initiated entirely at the volition of Veoh's users." *Id.*; see also *CoStar Grp., Inc. v. LoopNet, Inc.*, 373

⁸⁸*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1018 (9th Cir. 2013).

⁸⁹*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1018 (9th Cir. 2013).

⁹⁰See 17 U.S.C.A. §§ 512(c)(1)(A)(i), 512(c)(1)(A)(ii).

⁹¹*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1019 (9th Cir. 2013), citing 17 U.S.C.A. § 512(c)(1)(A)(iii).

⁹²*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1019 & n.9 (9th Cir. 2013), citing 17 U.S.C.A. §§ 512(k)(1)(A), 512(k)(1)(B).

F.3d 544, 555 (4th Cir. 2004). We therefore hold that Veoh has satisfied the threshold requirement that the infringement be “by reason of the storage at the direction of a user of material” residing on Veoh’s system. 17 U.S.C. § 512(c)(1).⁹³

The Second Circuit, in *Viacom Int’l, Inc. v. YouTube, Inc.*,⁹⁴ likewise relied on Judge Lloyd’s analysis in *Io Group, Inc. v. Veoh Networks, Inc.*,⁹⁵ as well as the Ninth Circuit’s decision in *UMG Recordings, Inc. v. Shelter Capital Partners LLC*⁹⁶ and district court Judge Matz’s earlier opinion in that case, in construing the term *by reason of storage* similarly broadly.⁹⁷ Circuit Judge José Cabranes, on behalf of himself and Judge Livingston,⁹⁸ cited *Io Group* for the proposition that “service providers seeking safe harbor under [section] 512(c) are not limited to merely storing material.”⁹⁹ The panel also cited the broader definition of *service provider* applicable to the user storage safe harbor as evidence that section 512(c) “is clearly meant to cover more than mere storage lockers.”¹⁰⁰ The panel further explained that section 512(c) “extends to software functions performed for the purpose of facilitating access to user-stored material.”¹⁰¹

⁹³*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1020 (9th Cir. 2013), quoting *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008).

⁹⁴*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).

⁹⁵*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

⁹⁶*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁹⁷*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38–40 (2d Cir. 2012).

⁹⁸Judge Roger J. Miner, who had also been assigned to the panel, passed away prior to the resolution of the case. See *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 25 n.1 (2d Cir. 2012).

⁹⁹*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 39 (2d Cir. 2012), quoting *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1147 (N.D. Cal. 2008).

¹⁰⁰*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 39 (2d Cir. 2012), quoting *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1088 (C.D. Cal. 2008), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

¹⁰¹*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 39 (2d Cir. 2012), quoting *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1088 (C.D. Cal. 2008), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013) and citing *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1031–35 (9th Cir. 2011), *opinion withdrawn and replaced*, 718 F.3d 1006 (9th Cir.

The Second Circuit panel held that three of YouTube's challenged software functions—transcoding videos into a standard display format, playback, which allowed users to view videos on “watch” pages, and the “related videos” function, which automatically displayed thumbnail images of related videos—did not cause YouTube to lose safe harbor protection.

With respect to transcoding and playback, the Second Circuit agreed with the Ninth Circuit in *Shelter Capital* and district court Judge Louis L. Stanton's decision below that “to exclude these automated functions from the safe harbor would eviscerate the protection afforded to service providers by § 512(c).”¹⁰²

The panel concluded that a similar analysis applied to YouTube's “related video” function, by which an algorithm identified and displayed thumbnail images of clips that were deemed “related” to videos viewed by a user. The Second Circuit declined to decide whether the phrase *by reason of* required a finding of proximate causation between the act of storage and the infringing activity, as Viacom had urged, because even if that showing was required, “the indexing and display of related videos retain a sufficient causal link to the prior storage of those videos.”¹⁰³

The Second Circuit remanded the case, however, on the narrow question of whether any of the videos uploaded to YouTube had been syndicated to third parties and, if so, whether potential liability for third-party syndication was outside the scope of the user storage safe harbor. The appel-

2013).

¹⁰²*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 39 (2d Cir. 2012), *opinion withdrawn and replaced*, 718 F.3d 1006 (9th Cir. 2013) (citing the district court opinion in the case).

¹⁰³*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 40 (2d Cir. 2012). The panel explained:

The record makes clear that the related videos algorithm “is fully automated and operates solely in response to user input without the active involvement of YouTube employees.” Supp. Joint App'x I:237. Furthermore, the related videos function serves to help YouTube users locate and gain access to material stored at the direction of other users. Because the algorithm “is closely related to, and follows from, the storage itself,” and is “narrowly directed toward providing access to material stored at the direction of users[]”

Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 40 (2d Cir. 2012), *quoting UMG Recordings, Inc. v. Veoh Networks, Inc.*, 620 F. Supp. 2d 1081, 1092 (C.D. Cal. 2008), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

late panel explained that YouTube had transcoded a select number of videos into a format compatible with mobile devices and syndicated (or licensed) those videos to Verizon Wireless and other companies. Plaintiffs had argued that business transactions do not occur *at the direction of a user* within the meaning of section 512(c)(1) “when they involve the manual selection of copyrighted material for licensing to a third party.”¹⁰⁴ It was undisputed that none of the videos at issue in the lawsuit had been syndicated to Verizon Wireless. Accordingly, to “avoid rendering an advisory opinion on the outer bounds of the storage provision,” the panel remanded for the narrow determination of whether any of the videos at issue in the lawsuit in fact had been syndicated to any third party.¹⁰⁵

As noted earlier in this subsection, on remand, the district court again granted summary judgment for YouTube, holding that YouTube’s practice of syndicating user content to third-party mobile providers did not take YouTube outside the safe harbor because the videos syndicated to Apple, Sony, Panasonic, TiVo and AT&T remained stored on YouTube’s servers and merely provided users with an alternative way to view material stored by users.¹⁰⁶

Second and Ninth Circuit case law ultimately make clear that section 512(c) does not distinguish between how widely accessible or prominently presented a work is once it is stored on a website at the direction of a user. Whether material is hidden inconspicuously or prominently displayed on the homepage of a site—or indeed on every single page of the site—should not affect safe harbor protection (even though it could affect damages¹⁰⁷ or potentially even secondary liability, where safe harbor protection is inapplicable¹⁰⁸) if it was stored at the direction of a user, rather than by the site itself, and if copyright liability is sought to be imposed on the service provider *by reason of* that stored material or the act of storing it and making it available for others.¹⁰⁹ The relevant consideration is whether the allegedly infringing

¹⁰⁴*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 40 (2d Cir. 2012).

¹⁰⁵*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 40 (2d Cir. 2012).

¹⁰⁶*See Viacom Int’l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 122 (S.D.N.Y. 2013).

¹⁰⁷*See infra* § 4.14[3].

¹⁰⁸*See supra* § 4.11.

¹⁰⁹The greater prominence given to material may be relevant to

material or activity, regardless of how characterized, is attributable to material stored by a service provider—*i.e.*, “that resides on a system or network controlled or operated by or for the service provider . . .”¹¹⁰—at the direction of a user. If it is, the user storage safe harbor applies, and the liability limitation is not lost regardless of the manner in which the material is stored by the service provider on its website or the various uses made of it (including even enabling user downloads, at least in the Ninth Circuit) so long as the material resides on a system or network controlled or operated by or for the service provider.

On the other hand, *Viacom v. YouTube* underscores that if material is transferred by a service provider from its site or service to a third party, where it no longer “resides on a system or network controlled or operated by or for the service provider . . .,”¹¹¹ an open question may arise about whether the safe harbor applies to that transfer (and that material), at least in the Second Circuit. Material initially stored at the direction of a user but then redistributed by a service provider in the physical world, rather than on a service provider’s system or network, for example, could place a service provider outside the safe harbor with respect to physical world distribution of that material. A service provider might not have protection for material redistributed over traditional radio or television, for example, even if that material originated with a user and originally was stored on a system or network controlled or operated by a service provider. If the content was accessed on a television or radio (or on a mobile device) from the service provider’s system or network (or a system or network operated for the service provider), however, the safe harbor should apply.

Courts, in a number of cases, have held service providers entitled to DMCA protection, typically in response to a motion for summary judgment,¹¹² granted or affirmed partial

whether the service provider has a financial interest (*infra* § 4.12[6][D]) or red flag awareness (*infra* § 4.12[6][C]) but is not *per se* disqualifying and does not change its character as user-stored material if it was in fact stored at the direction of a user.

¹¹⁰17 U.S.C.A. § 512(c)(1).

¹¹¹17 U.S.C.A. § 512(c)(1).

¹¹²*See, e.g., Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78 (2d Cir. 2016) (holding the service provider entitled to DMCA protection); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597 (9th Cir. 2018) (affirming

relief,¹¹³ or held service providers to be ineligible,¹¹⁴ or found factual issues in dispute, precluding the entry of summary judgment.¹¹⁵

Many people—especially non-lawyers—think of the user storage limitation as merely requiring the implementation of a notice and takedown mechanism. As underscored in the following subsections, a service provider also must meet other eligibility requirements to benefit from the safe harbor

summary judgment for the service provider, holding that it was entitled to DMCA safe harbor protection); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013) (affirming summary judgment for the defendant-operator of a user submitted video site); *Kinsley v. Udemy, Inc.*, Case No. 19-cv-04334-JSC, 2021 WL 1222489 (N.D. Cal. Mar. 31, 2021) (granting summary judgment for Udemy on its DMCA defense); *Dona't v. Amazon.com/ Kindle*, 482 F. Supp. 3d 1137, 1140-41 (D. Colo. 2020) (granting summary judgment for Amazon.com, where plaintiff failed to present evidence that it sent a DMCA notification to Amazon.com for the material at issue, or to refute Amazon.com's evidence that Amazon.com was entitled to the DMCA safe harbor); *Hempton v. Pond5, Inc.*, Case No. 3:15-cv-05696-BJR, 2016 WL 6217113 (W.D. Wash. Oct. 25, 2016) (granting summary judgment for Pond5, the operator of a website through which media producers may license and distribute content to third parties); *Milo & Gabby, LLC v. Amazon.com, Inc.*, No. C13-1932 RSM, 2015 WL 4394673, at *6-9 (W.D. Wash. July 16, 2015) (granting summary judgment in favor of Amazon.com on its DMCA defense), *aff'd on other grounds*, 693 F. App'x 879 (Fed. Cir.), *cert. denied*, 138 S. Ct. 335 (2017); *Avdeef v. Google*, No. 4:14-CV-788-A, 2015 WL 5076877, at *1, 3-4 (N.D. Tex. Aug. 26, 2015), *aff'd*, 678 F. App'x 239 (5th Cir. 2017); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (granting summary judgment for eBay).

¹¹³*See, e.g., Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012) (affirming in part, vacating and remanding in part, the lower court's order granting summary judgment for YouTube).

¹¹⁴*See, e.g., Werner v. Evolve Media, LLC*, 2:18-cv-7188-VAP-SKx, 2020 WL 3213808, at *8 (C.D. Cal. Apr. 28, 2020) (granting summary judgment for the copyright owner on Evolve's DMCA defense where Evolve, not a third-party user, posted all but one of the images at issue and, with respect to the last one, the image had been uploaded before Evolve had registered its DMCA agent).

¹¹⁵*See, e.g., EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 88-91 (2d Cir. 2016) (vacating the lower court's entry of summary judgment for the service provider and remanding for further proceedings); *Sid Avery and Associates, Inc. v. Pixels.com, LLC*, 479 F. Supp. 3d 859, 869 (C.D. Cal. 2020) (holding fact issues precluded summary judgment on Pixels' DMCA defense where, among other things, "unlike eBay and Amazon, Pixels may have an active role in designing, listing, selling, manufacturing, and delivering products."); *Ring v. Doe-1*, Civil Action No. 09-563 (GMS), 2015 WL 307840 (D. Del. Jan. 23, 2015) (granting summary judgment for Google on its DMCA defense, holding 14 days expeditious).

provided by section 512(c).

**4.12[6][B] Designation of an Agent and the
Obligation to Disable Access to or
Remove Material in Response to
Substantially Complying Notifications**

To qualify for the user storage safe harbor (as well as the caching and information location tools provisions of the DMCA), a service provider must designate an agent and respond to notifications. These obligations are addressed in greater detail in sections 4.12[9][A] (designation of an agent) and 4.12[9][B] (notifications).

In brief, a service provider must designate an agent to receive notifications (and potentially counter notifications) by filing a form with the U.S. Copyright Office and publicizing certain contact information about its designated agent on its website “in a location accessible to the public.”¹ Additional requirements are set forth in section 4.12[9][A]. A list of all registered DMCA agents may be found on the Copyright Office website.² In addition, as discussed in section 4.12[9][A], agent designation forms filed between 1998 and 2016 were deemed to have expired on December 31, 2017, potentially leaving some service providers outside the protections of the safe harbor unless and until they re-registered under new rules for agent designation that took effect at the end of 2016.³

To benefit from the user storage liability limitation, a service provider must expeditiously disable access to or remove material identified in a substantially complying notification. The requirements for a notification and a service provider’s obligations in responding to a notification are analyzed in detail in section 4.12[9][B].

Case law construing the statute makes clear that the DMCA places the initial burden on copyright owners to search the Internet for infringing material (which presumably they are best able to identify) and advise service provid-

[Section 4.12[6][B]]

¹17 U.S.C.A. § 512(c)(2).

²http://www.copyright.gov/onlinesp/list/s_agents.html

³See <https://www.copyright.gov/rulemaking/onlinesp/NPR/faq.html>

ers by sending notifications.⁴ A copyright owner cannot shift its obligation to search for material and send notifications by instructing a service provider prospectively to disable access to or remove material stored in the future (or to remove “all copies” that ever may appear on a site or service).⁵

Once a notification has been sent to a service provider’s designated agent, the DMCA shifts the burden to service providers to respond by expeditiously⁶ disabling access to or removing material identified in substantially complying notifications⁷ (and, as described below in section 4.12[6][C], by disabling access to or removing material that they know to be infringing or which raises a “red flag,” even if no notification has been sent). If a service provider does so, or if a copyright owner fails to send a substantially complying notification, the service provider will be shielded by the DMCA from liability for damages or attorneys’ fees (assuming that it otherwise meets the other technical requirements under the

⁴See, e.g., *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 89 (2d Cir. 2016) (“the DMCA explicitly relieves service providers from having to affirmatively monitor their users for infringement”); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 603 (9th Cir. 2018) (“The Digital Millennium Copyright Act places the burden of policing infringement on the copyright owner, not on the person or firm storing and hosting the material.”); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir.) (“The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright.”), *cert. denied*, 522 U.S. 1062 (2007).

⁵See, e.g., *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 918 (C.D. Cal. 2003); see also *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 746–47 (S.D.N.Y. 2012) (rejecting plaintiff’s contention that the defendant was required to proactively search for copies of the same work in the future once a notification is sent), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014); see generally *infra* § 4.12[9][B] (analyzing the issue in greater detail).

⁶See, e.g., *Kinsley v. Udemy, Inc.*, Case No. 19-cv-04334-JSC, 2021 WL 1222489, at *5 (N.D. Cal. Mar. 31, 2021) (granting summary judgment for Udemy on its DMCA defense, finding 3 days and same day for removal expeditious); *Hempton v. Pond5, Inc.*, Case No. 3:15-cv-05696-BJR, 2016 WL 6217113, at *8 (W.D. Wash. Oct. 25, 2016) (granting summary judgment for the defendant, where content was removed within 1 day of receiving notification of infringement); *Avdeef v. Google, Inc.*, No. 4:14-CV-788-A, 2015 WL 5076877, at *1, 3-4 (N.D. Tex. Aug. 26, 2015) (granting summary judgment for Google on its DMCA defense, holding 14 days expeditious), *aff’d*, 678 F. App’x 239 (5th Cir. 2017).

⁷17 U.S.C.A. § 512(c)(1)(C).

statute).⁸ By contrast, if the service provider fails to expeditiously disable access to or remove material identified in a substantially complying notification, it will not enjoy the benefits of the user storage safe harbor.⁹

⁸*See, e.g., UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021, 1024–25 (9th Cir. 2013) (affirming summary judgment for Veoh, the service provider, where prior to the litigation UMG had not identified to Veoh any specific infringing video available on Veoh’s system and Veoh otherwise satisfied the eligibility requirements for the user storage safe harbor); *Dona’t v. Amazon.com/ Kindle*, 482 F. Supp. 3d 1137, 1140–41 (D. Colo. 2020) (granting summary judgment for Amazon.com, where plaintiff failed to present evidence that it sent a DMCA notification to Amazon.com for the material at issue, or to refute Amazon.com’s evidence that Amazon.com was entitled to the DMCA safe harbor); *Long v. Dorset*, 369 F. Supp. 3d 939, 944–47 (N.D. Cal. 2019) (dismissing plaintiff’s complaint, in which he alleged that Facebook was not entitled to DMCA safe harbor protection, where the court found that Facebook acted expeditiously in removing over 100 images (and also responding to plaintiff’s demand that his administrator rights be restored) within five business days, where “Facebook promptly responded to plaintiff’s initial email and, over the next several days, continued to exchange emails with plaintiff to resolve the issue.”); *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 535–36 (S.D.N.Y. 2013) (holding that Vimeo was not obligated to disable access to or remove material in response to notices that were not substantially complying but in any case expeditiously removed videos where it took down material on the same day on two occasions and within 3 ½ weeks in response to a notice that covered 170 videos), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016); *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 732–34, 746–47 (S.D.N.Y. 2012) (holding that Photobucket was protected by the safe harbor where it disabled access to 700 photographs identified in substantially complying notifications within five days or less, finding notifications that did not include URLs to be noncomplying and holding that Photobucket had no ongoing obligation to proactively search for other copies of the same works identified in the earlier DMCA notices), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001) (granting summary judgment for the service provider where the copyright owner failed to submit a substantially complying notification).

⁹*See, e.g., 17 U.S.C.A. § 512(c)(1)(C); CoStar Group Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 703–04 (D. Md. 2001) (holding that factual disputes over whether removal was expeditious precluded summary judgment for either party), *aff’d on other grounds*, 373 F.3d 544, 556 (4th Cir. 2004); *see also Rosen v. Global Net Access, LLC*, No. 10-2721-DMG (E), 2014 WL 2803752, at *4–5 (C.D. Cal. June 20, 2014) (holding that a delay in removing photographs identified in a DMCA notice for more than two months, until after the defendant was served with a copy of the complaint in the lawsuit, was not *expeditious* within the meaning of the DMCA). *But see Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 535–36 (S.D.N.Y. 2013) (holding that removing 170 videos in response to a

What it means to disable access to or remove material is addressed in section 4.12[6][C].

Copyright owner and service provider obligations with respect to notifications are analyzed in greater detail in section 4.12[9][B]. A sample notification is included in the Appendix to this chapter.

4.12[6][C] Knowledge, Awareness or Corrective Measures

To be eligible for the user storage safe harbor, a service provider must disable access to or remove material in response to a substantially complying notification, actual knowledge that material is infringing or awareness of facts or circumstances from which infringing activity is apparent (referred to as “red flag” awareness). Case law makes clear that knowledge or awareness must be of specific files or activity, not generalized knowledge that a site or service may be used for infringement.¹ Knowledge or awareness are judged by objective and subjective criteria, based on evidence such

single notice within 3 weeks was expeditious), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

[Section 4.12[6][C]]

¹See, e.g., *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93 (2d Cir. 2016); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 30–32 (2d Cir. 2012); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 609–10 (9th Cir. 2018); *Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1057 (9th Cir. 2017) (“Both actual and red flag knowledge refer to knowledge of the specific infringement alleged.”); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021–23 (9th Cir. 2013); *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) (quoting *Shelter Capital* with approval on this point); see also *Atlantic Recording Corp. v. Spinrilla, LLC*, 506 F. Supp. 3d 1294, 1317 (N.D. Ga. 2020) (“Both actual and red flag knowledge relate to specific instances of copyright infringement. *Viacom Int’l. v. YouTube*, 676 F.3d 19, 31 (2d Cir. 2012). A general awareness that infringing activity occurs on the provider’s site does not preclude use of the safe harbor defense.”); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1109 (W.D. Wash. 2004) (holding, in a pre-*Shelter Capital* district court opinion that later influenced the Ninth Circuit, that general knowledge of infringing activity is not “red flag awareness,” which must be based on specific acts of infringement); *CoStar Group Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 704 (D. Md. 2001) (writing that it was impossible for LoopNet, the service provider, to know that particular images were infringing prior to receiving a notification from CoStar because the works did not include copyright notices, CoStar’s own expert could not identify a given CoStar photograph simply by reviewing it, and LoopNet would have had no way to know about CoStar’s licensing arrangements with its customers prior to

as internal emails or other messages that reflect knowledge or awareness of particular files at issue in a lawsuit (if not removed, once that knowledge or awareness is obtained). Whether a service provider has actual knowledge turns on whether it “‘subjectively’ knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement ‘objectively’ obvious to a reasonable person.”² The Ninth Circuit suggested in *dicta* that notice from a third party may create red flag awareness, although the statute makes clear that knowledge or awareness may not be inferred from a defective notification sent by a copyright owner.³ A service provider has no obligation to proactively search for infringing material.⁴ At the same time, knowledge or awareness may be shown by evidence of willful blindness.⁵ Significantly, in *Capitol Records, LLC v. Vimeo*,

receiving notice), *aff’d on other grounds*, 373 F.3d 544 (4th Cir. 2004).

²*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1025 (9th Cir. 2013) (quoting *Viacom v. YouTube*). The Ninth Circuit has underscored that “whether ‘the specific infringement’ is ‘objectively’ obvious to a reasonable person’ may vary depending on the facts proven by the copyright holder in establishing liability.” *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026 n.15 (9th Cir. 2013).

³See 17 U.S.C.A. § 512(c)(3)(B)(i) (stating that neither knowledge nor awareness may be inferred from a notice that fails to meet statutory requirements); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1024–25 (9th Cir. 2013). In *Shelter Capital*, UMG had argued that Veoh had red flag awareness of infringing material based on emails sent to Veoh executives by copyright owners, including an email sent by Disney’s CEO to Michael Eisner, a Veoh investor, stating that unauthorized copies of the movie *Cinderella III* and various episodes from the television show *Lost* were posted on Veoh’s site. The Ninth Circuit panel explained that “[i]f this notification had come from a third party, such as a Veoh user, rather than from a copyright holder, it might meet the red flag test [assuming the material was not taken down in response to the notice] because it specified particular infringing material. As a copyright holder, however, Disney is subject to the notification requirements in § 512(c)(3), which this informal email failed to meet.” *Id.* (footnote omitted).

⁴17 U.S.C.A. § 512(m); see also, e.g., *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1022 (9th Cir. 2013).

⁵See *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) (holding that knowledge or awareness may be established by evidence of willful blindness, which the court characterized as a deliberate effort to avoid guilty knowledge); *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043 (9th Cir. 2013) (explaining that “inducing actions”—or

LLC,⁶ the Second Circuit, in an opinion written by Judge Leval, framed the issues of knowledge, red flag awareness and imputed knowledge based on willful blindness, in terms of the parties' respective burdens of proof in litigation, holding that the burden to show "disqualifying knowledge . . . falls on the copyright owner"⁷ Although the DMCA is an affirmative defense, where a service provider meets its initial burden of proving entitlement to the DMCA safe harbor, the burden shifts to the copyright owner to prove that the service provider is not entitled to safe harbor protection based on knowledge or red flag awareness. If that subsequent burden is not met by the copyright owner, the service provider is deemed subject to the safe harbor.⁸ In *Vimeo*, the Second Circuit also held that in evaluating an employee's actual knowledge or red flag awareness, "[t]he hypothetical 'reasonable person' to whom infringement must be obvious is an ordinary person—not endowed with specialized knowledge or expertise concerning music or the laws of copyright."⁹

The structure of the DMCA may at first glance seem dif-

conduct deemed to induce copyright infringement—were relevant to the court's determination that the defendant had red flag awareness); *Capitol Records, Inc. v. MP3Tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *3–4 (S.D.N.Y. May 14, 2013) (reconsidering its earlier ruling granting summary judgment for the service provider on plaintiff's claim for contributory infringement of those songs not subject to DMCA-compliant takedown notices, in light of the importance the Second Circuit placed on explicit fact-finding in evaluating willful blindness as a potential bar to DMCA protection in *Viacom v. YouTube*, and holding that a jury could reasonably interpret several documents as imposing a duty to make further inquiries into specific and identifiable instances of possible infringement); see also *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1023 (9th Cir. 2013) (citing *Viacom v. YouTube* for the proposition that "a service provider cannot willfully bury its head in the sand to avoid obtaining . . . specific knowledge.").

⁶*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78 (2d Cir. 2016).

⁷*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 95 (2d Cir. 2016); see also *Atlantic Recording Corp. v. Spinrilla, LLC*, 506 F. Supp. 3d 1294, 1317 (N.D. Ga. 2020) (following *Vimeo* on this point, writing that, "[i]mportantly, if a service provider is otherwise eligible for the safe harbor defense, the burden of proof is on the copyright owner to show that the service provider failed to respond appropriately to actual or red flag knowledge.").

⁸See *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93–95 (2d Cir. 2016).

⁹*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93–94 (2d Cir. 2016).

difficult to follow. In addition to responding to notifications, a service provider, to benefit from section 512(c), must either lack actual knowledge of the infringing material or “not be aware of facts and circumstances from which the infringing activity is apparent” on its system or network or, if it has such knowledge or awareness, act expeditiously to disable access to or remove the material or activity. Awareness short of actual knowledge, according to a committee report accompanying an earlier version of the DMCA, may be thought of as facts or circumstances “which raise a ‘red flag’ that . . . users are infringing.”¹⁰

Although the statute lists each of the three ways in which the first requirement for the limitation may be satisfied in the alternative using the disjunction “or,” in fact a service provider must show that neither of the two requirements that are phrased in negative terms (that the service provider “not have actual knowledge” and that the service provider “in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent”) apply or that, if the service provider has either actual knowledge or awareness, it has satisfied the affirmative requirement to act expeditiously to remove or disable access to such material. Since a cardinal rule of statutory construction is that every word in a statute should be read in such a way as to give it meaning,¹¹ this is the only logical reading of the two double negatives and one affirmative obligation listed as alternative requirements in subsection (c)(1)(A). If literally read as requiring compliance with any one of the three alternatives listed in the subsection, a service provider could qualify for the limitation merely by alleging that it lacked actual knowledge, which would render the other two provisions meaningless.

The user storage safe harbor thus applies (assuming that the other eligibility requirements have been met) where a service provider expeditiously¹² disables access to or removes material upon learning of infringement through a notifica-

¹⁰*CoStar Group Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 702, (D. Md. 2001), *aff’d on other grounds*, 373 F.3d 544, 556 (4th Cir. 2004).

¹¹*See, e.g., United States v. Nordic Village Inc.*, 503 U.S. 30, 35–36 (1992); *Bailey v. United States*, 516 U.S. 137, 145 (1995) (noting the “assumption that Congress intended each of its terms to have meaning”); *United States v. Bass*, 404 U.S. 336, 344 (1971).

¹²In *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 612 (9th Cir. 2018), the Ninth Circuit held that a service provider acted expedi-

tion, actual knowledge or awareness of facts or circumstances from which infringement is apparent (i.e., awareness which raise a “red flag”). Conversely, it applies where material may have been overlooked but where the service provider did not receive a notification and had neither knowledge nor awareness that the material or activity was on its site or was infringing.

Knowledge or awareness may not be imputed to a service provider based on the contents of a defective notification.¹³ Whether a notification is defective is separately addressed in section 4.12[9][B]. If, however, a service provider fails to disable access to or remove material expeditiously, based on notice, knowledge or awareness, its inaction will render it ineligible for the safe harbor.¹⁴

The requirement to disable access to or remove material is just that—a requirement that a service provider “remove or disable access to” material in response to notice, knowledge or red flag awareness.¹⁵ There are legitimate reasons why a service provider may prefer to disable access to material, rather than removing it, including so that a link may be restored in response to a counter notification or a court order

tiously in removing video clips where the plaintiff provided no advance notice before filing suit and initially ignored a request from the service provider to provide URLs, where the service provider removed files on the same day that the copyright owner eventually provided the URLs. The court noted that the video clips did not identify the plaintiff as the copyright owner and that there were more than half a million videos on the defendants’ site, implicitly finding that, in those circumstances, it was reasonable for the service provider to wait for the copyright owner to provide URLs before taking down the video clips.

¹³See 17 U.S.C.A. § 512(c)(3)(B)(i) (a notification that is not substantially complying “shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent”). Where a notification is deficient but nonetheless substantially complies with the requirements for identifying the infringed work and the infringing material and includes sufficient contact information to allow the service provider to contact the complainant, the service provider must attempt to do so or “tak[e] other reasonable steps to assist” in obtaining a substantially complying notification before it may benefit from this provision. See 17 U.S.C.A. § 512(c)(3)(B)(ii); see generally *infra* § 4.12[9][B].

¹⁴See, e.g., *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001).

¹⁵See 17 U.S.C.A. § 512(c)(1)(C) (emphasis added).

in a lawsuit between the copyright owner and poster¹⁶ or to preserve evidence.¹⁷

In *Rosen v. eBay, Inc.*,¹⁸ a district court in Los Angeles held that eBay complied with the requirement to disable access to or remove copyrighted photographs in response to notifications from the plaintiff, a Paparazzi photographer named Barry Rosen, even though Rosen contended that he was able to call up the images by directly accessing the URLs for links that had been removed in response to the notifications he had sent eBay and via search engine queries. In that case, eBay had argued that it had disabled all “meaningful public” access and that (1) the plaintiff conceded that he might have accessed cached versions of the images from his own computer that were no longer accessible on eBay’s servers, (2) the images accessed via search engine queries may have been cached by third party search engines and would disappear over time as those third party caches were cleared,¹⁹ and (3) even if the plaintiff had been able to access the images directly from eBay’s servers, to do so he would have had to use the unique URL taken from the listing when it was live, which could not have been obtained by anyone outside of the company short of copying that URL prior to the time the link was disabled. In holding that eBay satisfied the requirement to disable access to or remove material in response to valid DMCA notifications, the court explained

¹⁶See *infra* § 4.12[9][C] (analyzing counter notifications and the corresponding optional obligations imposed on service providers that choose to comply with the requirements of 17 U.S.C.A. § 512(g)(1)).

¹⁷The DMCA does not affirmatively require that material be preserved and indeed expressly authorizes that material be removed in response to notice, knowledge or red flag awareness. A service provider’s failure to preserve certain evidence necessary to establish its entitlement to the DMCA safe harbor (such as records relating to termination of repeat infringers), however, could result in evidentiary sanctions that could disqualify the service provider from DMCA safe harbor protection. See *generally infra* § 4.12[18].

¹⁸*Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *11-12 (C.D. Cal. Jan. 16, 2015).

¹⁹The DMCA also provides a mechanism for copyright owners to obtain injunctive relief requiring that a service provider disable access to or remove cached copies of infringing material. See 17 U.S.C.A. §§ 512(b), 512(j); *supra* § 4.12[5][A] (analyzing the system caching safe harbor). In practice, this remedy is rarely invoked because search engines regularly refresh their caches—and usually do so more quickly than a court will act on a request for injunctive relief. Copyright owners also may be able to send DMCA takedown notifications directed at cached content.

that “this copying is clearly not a normal or expected use of eBay’s systems, and it is unclear that anyone not specifically compelled to exploit this workaround—as Rosen is—would ever use it.”²⁰ Accordingly, the court ruled that “[i]n light of the somewhat extraordinary lengths Rosen had to go to obtain copies of his images, which may or may not have actually been accessed from eBay’s servers, eBay adequately disabled access to his images when it took down the listings, even when the record is viewed in the light most favorable to Rosen.”²¹

The user storage safe harbor’s focus on notice, knowledge or awareness, and corrective action, is consistent with *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,²² in protecting service providers from the possibility that direct liability otherwise could be imposed without regard to their knowledge or intent.²³ *Netcom* was the leading case on secondary liability at the time Congress enacted the DMCA and was influential in its development.

The DMCA limits liability for eligible service providers based on a notice and take-down system, which the court in *Netcom* acknowledged might in any event otherwise be required in response to a cease and desist letter to avoid contributory infringement. Further, by requiring that a service provider not have actual knowledge or awareness, the DMCA effectively precludes the user storage limitation from being applied in most cases where a service provider could otherwise be held liable for contributory infringement (to the extent based on inducing, causing or materially contributing to the infringing conduct of another, rather than imputed

²⁰*Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *12 (C.D. Cal. Jan. 16, 2015).

²¹*Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *12 (C.D. Cal. Jan. 16, 2015).

²²*Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1374 (N.D. Cal. 1995); see generally *supra* § 4.11[2].

²³Although no district court has imposed liability on this basis since the time of the *Netcom* decision in 1995, the Clinton Administration in the NII White Paper had argued (prior to the time *Netcom* was decided) that direct liability could be imposed on that basis and some commentators believe that it was in fact in *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993). See *supra* §§ 4.11[2], 4.11[8][A], 4.11[9].

knowledge)²⁴ or the more recent cause of action for inducing copyright infringement²⁵ (both of which presuppose at least actual awareness of the primary infringer's conduct, if not active encouragement).

The requirement that a service provider act in response to red flag awareness is an obligation that did not exist prior to the enactment of the DMCA under common law theories of direct, contributory or vicarious liability, and therefore compels service providers to do more than otherwise would be required as a *quid pro quo* for being able to benefit from the user storage safe harbor. It is for this reason, among others, that Congress made clear that a service provider's failure to meet the requirements of the DMCA could not be cited as evidence of infringement.²⁶

Red flag awareness—when a service provider “in the absence of actual knowledge, . . . is not aware of facts or circumstances from which the infringing activity is apparent . . .”²⁷—may not be imputed merely because a service provider arguably *should have known* that content was infringing. Rather, it amounts to a requirement that a service provider, although lacking actual knowledge, not have awareness of facts or circumstances which would lead a reasonable person to conclude that an infringement had occurred. As explained by one court, “the question is not ‘what a reasonable person would have deduced given all the circumstances.’ . . . Instead, the question is whether the service provider deliberately proceeded in the face of blatant factors of which it was aware . . . [or] turned a blind eye to ‘red flags’ of obvious infringement.”²⁸

The DMCA presupposes that users may post infringing material on a site or service, which is why the safe harbor for material stored at the direction of the user was created in the first place. Accordingly, knowledge or awareness must relate to specific material or activity. Generalized knowledge

²⁴See *supra* § 4.11[3].

²⁵See *supra* § 4.11[6].

²⁶17 U.S.C.A. § 512(l). Another reason for this provision is that DMCA liability limitations are optional—service providers are not required to comply but rather are induced to do so by the opportunity to limit their liability through safe harbors.

²⁷17 U.S.C.A. § 512(c)(1)(A).

²⁸*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1108 (W.D. Wash. 2004) (citing Nimmer on Copyright and the legislative history).

that a site or service could be used for infringement or that infringing material may be found on the site is insufficient to disqualify a service provider from the user storage safe harbor.²⁹

²⁹See, e.g., *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93 (2d Cir. 2016); *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 30–32 (2d Cir. 2012); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 609–10 (9th Cir. 2018); *Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1057 (9th Cir. 2017); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021–23 (9th Cir. 2013); *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) (quoting *Shelter Capital* with approval on this point); see also *Atlantic Recording Corp. v. Spinrilla, LLC*, 506 F. Supp. 3d 1294, 1317 (N.D. Ga. 2020) (“Both actual and red flag knowledge relate to *specific* instances of copyright infringement. *Viacom Int'l. v. YouTube*, 676 F.3d 19, 31 (2d Cir. 2012). A general awareness that infringing activity occurs on the provider’s site does not preclude use of the safe harbor defense.”); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1109 (W.D. Wash. 2004) (holding, in a pre-*Shelter Capital* district court opinion that later influenced the Ninth Circuit, that general knowledge of infringing activity is not “red flag awareness,” which must be based on specific acts of infringement); *CoStar Group Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 704 (D. Md. 2001) (writing that it was impossible for LoopNet, the service provider, to know that particular images were infringing prior to receiving a notification from CoStar because the works did not include copyright notices, CoStar’s own expert could not identify a given CoStar photograph simply by reviewing it, and LoopNet would have had no way to know about CoStar’s licensing arrangements with its customers prior to receiving notice), *aff’d on other grounds*, 373 F.3d 544 (4th Cir. 2004).

The DMCA also mandates specificity, rather than generalized *notice*, for DMCA notifications, by requiring substantial compliance with the requirements for notifications before a service provider has the obligation to disable access to or remove material. See 17 U.S.C.A. § 512(c)(3); see also, e.g., *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1090 (C.D. Cal. 2001) (holding that, based on the facts of that case, the plaintiff was required to identify, among other things, specific listing numbers to meet the requirement of substantial compliance, while noting in *dicta* that a more general description could suffice if a plaintiff were identifying all works of a particular nature on a site).

Courts in the Ninth Circuit and Southern District of New York similarly have held that the knowledge required to establish contributory infringement must be of specific infringing files, not merely general knowledge that a site is used for infringement. See, e.g., *Luvdarts, LLC v. AT&T Mobility, LLC*, 710 F.3d 1068, 1072 (9th Cir. 2013) (affirming that the plaintiff did not state a claim for contributory infringement against mobile phone carriers over the alleged infringement of their users in forwarding text messages containing original content without authorization to do so because a plaintiff must allege “more than a generalized knowledge . . . of the possibility of infringement.”); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1172 (9th Cir. 2007) (“a computer system operator can be

As explained by the Second Circuit, the text of the DMCA itself compels the conclusion that the requisite level of actual knowledge or awareness must be based on “specific and identifiable instances of infringement.”³⁰ The Second Circuit rejected the argument that red flag awareness requires less

held contributorily liable if it ‘has *actual* knowledge that *specific* infringing material is available using its system . . .’”; citation omitted, emphasis in the original); *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1021–22 (9th Cir. 2001) (holding that a service provider could be held contributorily liable where it had actual knowledge of specific infringing material, but not merely because the structure of the system allowed for the exchange of copyrighted material); *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 751 (S.D.N.Y. 2012) (holding that for liability to attach, actual or imputed knowledge must be based on specific and identifiable infringements of individual items, not a general awareness of infringement), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014); see also *Tiffany (NJ) Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 510 n.37 (S.D.N.Y. 2008) (writing in *dicta* in a secondary trademark infringement case that “[u]nder copyright law, generalized knowledge that copyright infringement may take place in an Internet venue is insufficient to impose contributory liability.”), *aff’d*, 600 F.3d 93, 107 (2d Cir.) (“We agree with the district court. For contributory trademark infringement liability to lie, a service provider must have more than a general knowledge or reason to know that its service is being used to sell counterfeit goods. Some contemporary knowledge of which particular listings are infringing or will infringe in the future is necessary.”), *cert. denied*, 562 U.S. 1082 (2010); see generally *supra* § 4.11[3] (analyzing the requirements to prove contributory copyright infringement).

By contrast, a site owner with generalized knowledge could be held liable for inducement if it actively encourages users to infringe (although a defendant found liable for inducing copyright infringement likely would be deemed to have red flag awareness and therefore be ineligible for the DMCA safe harbors). See *supra* § 4.11[6].

³⁰*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 30, 32 (2d Cir. 2012). Judge José Cabranes, writing for himself and Judge Livingston, explained that:

[T]he basic operation of § 512(c) requires knowledge or awareness of specific infringing activity. Under § 512(c)(1)(A), knowledge or awareness alone does not disqualify the service provider; rather, the provider that gains knowledge or awareness of infringing activity retains safe-harbor protection if it “acts expeditiously to remove, or disable access to, the material.” 17 U.S.C. § 512(c)(1)(A)(iii). Thus, the nature of the removal obligation itself contemplates knowledge or awareness of specific infringing material, because expeditious removal is possible only if the service provider knows with particularity which items to remove. Indeed, to require expeditious removal in the absence of specific knowledge or awareness would be to mandate an amorphous obligation to “take commercially reasonable steps” in response to a generalized awareness of infringement. *Viacom Br.* 33. Such a view cannot be reconciled with the language of the statute, which requires “expeditious[]” action to remove or disable “the material” at issue. 17 U.S.C. § 512(c)(1)(A)(iii) (emphasis added).

Id. at 30–31.

specificity than actual knowledge, clarifying that the difference between actual knowledge and red flag awareness is “not between specific and generalized knowledge, but instead between a subjective and objective standard.”³¹ The panel elaborated that:

[T]he actual knowledge provision turns on whether the provider actually or “subjectively” knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement “objectively” obvious to a reasonable person.³²

How red a “red flag” has to be before liability will be imposed for inaction depends on whether the question is adjudicated in the Second or Ninth Circuit and remains open to debate in other courts. The standard in the Ninth Circuit is the clearest (and most favorable to service providers) while that applied in the Second Circuit is easier to recite than to specifically apply and has yet to be fleshed out in case law. Most opinions that address the issue have clarified what is *not* red flag awareness, rather than elaborating on what it is.

In *Perfect 10, Inc. v. CCBill, LLC*,³³ the Ninth Circuit set a very high bar for when awareness short of actual knowledge may be imputed to a service provider. In the Ninth Circuit, a “red flag” must be “fire engine red” before a service provider will be deemed to have an obligation to takedown material on its own initiative (short of actual knowledge or receipt of a substantially complying notification). Lighter shades of red will not trigger a take down obligation, at least in the Ninth Circuit.

In *CCBill*, *Perfect 10*, the publisher of an adult magazine, had alleged that CWIE, a website hosting company, and CCBill, a service that allowed consumers to use credit cards or checks to pay for subscriptions or memberships to

³¹*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012).

³²*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1025 (9th Cir. 2013) (quoting *Viacom v. YouTube*). The Ninth Circuit subsequently noted that “whether ‘the specific infringement’ is ‘objectively’ obvious to a reasonable person’ may vary depending on the facts proven by the copyright holder in establishing liability.” *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026 n.15 (9th Cir. 2013).

³³*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

e-commerce venues, were not entitled to the user storage safe harbor because they were aware of a number of “red flags” that signaled apparent infringement. Perfect 10 argued that defendants had awareness of infringement by providing services to illegal.net and stolencelebritypics.com. The Ninth Circuit, however, disagreed. Judge Milan D. Smith, writing for himself and Chief Judge Alex Kozinski and Judge Stephen Reinhardt, wrote that:

[W]hen a website traffics in pictures that are titillating by nature, describing photographs as “illegal” or “stolen” may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen. We do not place the burden of determining whether photographs are actually illegal on a service provider.³⁴

Perfect 10 also had argued that password hacking websites hosted by CWIE obviously hosted infringing content. While the Ninth Circuit conceded that Perfect 10 might have claims against password hacking sites for contributory infringement, it disagreed that providing service to sites that purported to offer free passwords to subscriptions sites meant that the defendants had awareness of infringing activity, which would have stripped them of protection under the DMCA safe harbor. The panel held that “[p]assword-hacking sites are . . . not *per se* ‘red flags’ of infringement.”³⁵ Judge Smith wrote that:

In order for a website to qualify as a “red flag” of infringement, it would need to be apparent that the website instructed or enabled users to infringe another’s copyright We find that the burden of determining whether passwords on a website enabled infringement is not on a service provider. The website could be a hoax, or out of date. The owner of the protected content may have supplied the passwords as a short-term promotion, or as an attempt to collect information from unsuspecting users. The passwords might be provided to help users maintain anonymity without infringing on copyright. There is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords, and verifying that they enabled illegal access to copyrighted material. We impose no such investigative duties on service providers.³⁶

The high bar set by the Ninth Circuit for when awareness

³⁴*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007), cert. denied, 522 U.S. 1062 (2007).

³⁵*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007), cert. denied, 522 U.S. 1062 (2007).

³⁶*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007),

or a “red flag” may be found was justified in *CCBill* by the fact that the DMCA places the primary burden of investigation on copyright owners (although the awareness prong plainly imposes some obligation on service providers to restrict access to or remove material that raises a red flag). In addition, the legislative history makes it clear that while service providers are not obligated to do so, they equally are not discouraged and may not be penalized (in the form of a finding of right and ability to control) from monitoring their sites or services.³⁷ A low threshold for finding red flag awareness would deter voluntary monitoring (since the act of reviewing files could lead to greater liability).

While *CCBill* established a standard for red flag awareness in the Ninth Circuit that is very favorable to service providers, it also imposes on them more stringent requirements for complying with the obligation to reasonably implement a repeat infringer policy under section 512(i). The Ninth Circuit remanded the case to the district court for consideration of whether potential red flags had been raised by third-party content.³⁸ The court concluded that the requirements that a service provider disable access to or remove material in response to notice, knowledge or awareness were relevant not merely to the user storage safe harbor but to the question of whether a service provider has reasonably implemented its repeat infringer policy, which is a threshold eligibility requirement for all of the safe harbors established in section 512(i). Thus, under *CCBill*, failure to respond in the face of knowledge, notice or red flag awareness could put at risk not merely a service provider’s entitlement to the user storage liability limitation for the material that was overlooked, but its very entitlement to any of the safe harbors if challenged by any copyright owner. The significance of the Ninth Circuit’s importing the requirement that service providers disable access to and remove material in response to notice, knowledge or awareness, into the threshold requirement of reasonable implementation of a repeat infringement policy, is addressed briefly in section 4.12[6][A] and extensively in section 4.12[3][B][iv].

Applying *CCBill*, the district court in *Io Group, Inc. v.*

cert. denied, 522 U.S. 1062 (2007).

³⁷*See infra* § 4.12[6][D] (discussing this issue in the context of right and ability to control).

³⁸*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114–15 (9th Cir. 2007), *cert. denied*, 522 U.S. 1062 (2007).

*Veoh Networks, Inc.*³⁹ ruled that Veoh, the operator of the UGC video site, could not be held to have had red flag awareness of infringing material because it allowed professional quality adult pornography to be posted to its site without the labeling information required by 22 U.S.C.A. § 2257 (which requires that certain records about the age of performers be retained and that notice of compliance be provided).⁴⁰ Io argued that Veoh should have known that no legitimate producer of sexually explicit material would have omitted the requisite labels from video clips and that the excerpts uploaded therefore must be unauthorized. The court, however, ruled that the absence of adult labels did not give Veoh the requisite level of knowledge or awareness that plaintiff's copyrights were being violated. Among other things, the court noted that none of the clips at issue included copyright notices and although one clip had a trademark notice several minutes into the clip there was no evidence from which it could be inferred that Veoh was aware of, but chose to ignore, this information.⁴¹

The court, citing the House Report and *Corbis Corp. v. Amazon.com*,⁴² emphasized that the question is not what a reasonable person would have deduced given all the circumstances, but whether the service provider deliberately proceeded in the face of blatant factors of which it was aware (i.e., turned a blind eye to red flags of obvious infringement).⁴³

In *UMG Recordings, Inc. v. Veoh Networks, Inc.*,⁴⁴ the district court, in granting summary judgment for Veoh on all

³⁹*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

⁴⁰See *infra* chapters 40, 41.

⁴¹*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1149 (N.D. Cal. 2008). The court also rejected plaintiff's argument that Veoh had failed to act expeditiously to disable access to or remove material, but the facts of that case were unusual. Io did not notify Veoh of the allegedly infringing works on its system. Independently, and for unrelated reasons, Veoh removed all adult material from its site twenty-one days after the first unauthorized Io clip allegedly was uploaded. Io also presented no evidence suggesting that Veoh failed to act expeditiously once it acquired knowledge or awareness of infringing material.

⁴²*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

⁴³See *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008).

⁴⁴*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital*

of UMG's copyright claims, followed *CCBill* in holding that Veoh did not have actual knowledge or red flag awareness of infringing material on its UGC site, and when it received a notification Veoh expeditiously disabled access to or removed the material that was the subject of the notice.

Judge Matz rejected UMG's argument that Veoh had actual knowledge because it was hosting an entire category of content—music—that was subject to copyright protection, writing:

If merely hosting user-contributed material capable of copyright protection were enough to impute actual knowledge to a service provider, the section 512(c) safe harbor would be a dead letter because vast portions of content on the Internet are eligible for copyright protection. UMG's theory would also make the DMCA's notice-and-takedown provisions completely superfluous because any service provider that hosted copyrighted material would be disqualified from the section 512(c) safe harbor regardless of whether the copyright holder gave notice or whether the service provider otherwise acquired actual or constructive knowledge of specific infringements.

The court noted that UMG's argument was also undercut by evidence that of the 244,205 videos on Veoh's service labeled "music videos," 221,842 were not identified as unauthorized by the Audible Magic music filter that Veoh employed on its site.⁴⁵

Judge Matz further rejected the argument that Veoh had knowledge based on a notice from the RIAA, where the notice merely provided names of artists, which the court held was not the same thing as a representative list of works and therefore merely a defective DMCA notification. The notices likewise did not identify the material claimed to be infringing. The court wrote that "[a]n artist's name is not information reasonably sufficient to permit the service provider to locate [such] material."⁴⁶

Judge Matz held that Veoh did not have "red flag" aware-

Partners LLC, 718 F.3d 1006 (9th Cir. 2013).

⁴⁵*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1109 (C.D. Cal. 2009) (quoting *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1105 (W.D. Wash. 2004)), *aff'd on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013); *see generally infra* § 17.05[3] (discussing music video filters, including the Audible Magic filter).

⁴⁶*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1110 (C.D. Cal. 2009) (citing 17 U.S.C.A. § 512(c)(3)(A)(iii)), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th

ness, which he construed narrowly, writing that “*CCBill* teaches that if investigation of ‘facts and circumstances’ is required to identify material as infringing, then those facts and circumstances are not ‘red flags.’”⁴⁷ UMG argued that Veoh’s founders, employees and investors knew that widespread infringement was occurring on the Veoh system. The court held, however, that general awareness of infringement, without more, was not enough to preclude protection pursuant to section 512(c)’s safe harbor. Judge Matz wrote that “[n]o doubt it is common knowledge that most websites that allow users to contribute material contain infringing items. If such general awareness were enough to raise a ‘red flag,’ the DMCA safe harbor would not serve its purpose of ‘facilitat[ing] the robust development and worldwide expansion of electronic commerce, communications, research, development, and education in the digital age,’ and ‘balanc[ing] the interests of content owners, online and other service providers, and information users in a way that will foster the continued development of electronic commerce and the growth of the Internet.”⁴⁸

Judge Matz also rejected the argument that Veoh avoided gaining knowledge of infringement by delaying implementation of the Audible Magic fingerprinting system until October 2007, even though it was available in early 2005, and by waiting nine months before filtering videos already on the system. He noted that the DMCA did not require service providers to implement filtering technology and that Veoh had previously implemented “hash” filtering earlier and attempted to develop its own filtering tool. When it could not do so, it licensed Audible Magic’s technology. The court wrote that these undertakings merely underscored Veoh’s good faith efforts to avoid or limit storage of infringing content.

Finally, the district court rejected UMG’s argument that Veoh could have searched its indices for the names of artists whose videos were identified in the RIAA notices. The court held that “the DMCA does not place the burden of ferreting

Cir. 2013).

⁴⁷*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1108 (C.D. Cal. 2009), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁴⁸*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1111 (C.D. Cal. 2009), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

out infringement on the service provider.”⁴⁹

On appeal, the Ninth Circuit affirmed Judge Matz’s order granting summary judgment to Veoh, noting that UMG did not dispute that when Veoh became aware of allegedly infringing material as a result of the RIAA’s DMCA notices, it removed the files. Rather, UMG argued that Veoh had knowledge or awareness of other infringing videos that it did not remove.⁵⁰

The Ninth Circuit rejected UMG’s argument that hosting a music category evidenced knowledge. First, the court pointed out that Veoh had licenses from Sony-BMG and therefore could have hosted licensed music. Second, the panel rejected the argument that generalized knowledge could take a service provider outside the safe harbor. The panel held that “merely hosting a category of copyrightable content, such as music videos, with general knowledge that one’s services could be used to share infringing material, is insufficient to the meet the actual knowledge requirement of § 512(c)(1)(A)(i)” or red flag awareness pursuant to section 512(c)(1)(A)(ii).⁵¹

The appellate court similarly rejected the argument that tagging user submissions as “music videos” evidenced knowledge or awareness given that the court had already concluded that hosting music videos did not disqualify Veoh from safe harbor protection.⁵²

The court likewise rejected the argument that Veoh’s

⁴⁹*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1112 (C.D. Cal. 2009), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁵⁰*See UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1020 (9th Cir. 2013). The appellate panel initially issued a decision affirming the lower court’s entry of summary judgment in December 2011, *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1036 (9th Cir. 2011), which subsequently was withdrawn and replaced by a new opinion in 2013 that, on reconsideration, harmonized the Ninth Circuit’s analysis with the Second Circuit’s intervening opinion in *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012). The Second Circuit’s discussion of *Shelter Partners* in *YouTube* refers to the earlier, now withdrawn 2011 opinion.

⁵¹*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021–23 (9th Cir. 2013), *see also BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) (citing *Shelter Capital* with approval on this point).

⁵²*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1023 (9th Cir. 2013).

purchase of key words including “50 Cent,” “Avril Lavigne” and “Britney Spears” evidenced knowledge or awareness both because these UMG artists also had recorded for Sony-BMG, which had given Veoh a license for its artists’ videos, and because “companies sometimes purchase search terms they believe will lead potential customers to their websites even if the terms do not describe the goods or services the company actually provides.”⁵³

The Ninth Circuit panel further rejected UMG’s argument that Veoh’s compliance with RIAA takedown notices gave it knowledge of infringement and should have caused it to take the initiative to use search and indexing tools to locate and remove other material by these same artists. Relatedly, UMG had argued that Veoh should have known from the MTV or other television logos watermarked on some videos removed from its site that unauthorized material had been posted, which it could have searched for. Applying *CCBill*, however, the appellate court refused to impose investigative duties on service providers (and also noted that this approach likely would have resulted in the removal as well of noninfringing content).⁵⁴

Finally, the court rejected UMG’s argument that Veoh had knowledge of infringement based on newspaper articles that referred to unauthorized material on its site, in which Veoh’s CEO acknowledged the problem and stated that Veoh took infringement seriously and removed unauthorized content when found. Judge Raymond C. Fisher, writing for the unanimous panel, explained:

The DMCA’s detailed notice and takedown procedure *assumes* that, “from time to time,” “material belonging to someone else ends up” on service providers’ websites, and establishes a process for ensuring the prompt removal of such unauthorized material. If Veoh’s CEO’s acknowledgment of this general problem and awareness of news reports discussing it was enough to remove a service provider from DMCA safe harbor

⁵³*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1023 (9th Cir. 2013). The court explained that:

For example, a sunglass company might buy the search terms “sunscreen” or “vacation” because it believed that people interested in such searches would often also be interested in sunglasses. Accordingly, Veoh’s search term purchases do little to demonstrate that it knew it hosted infringing material.

Id.

⁵⁴*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1023–24 (9th Cir. 2013), citing *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

eligibility, the notice and takedown procedures would make little sense and the safe harbors would be effectively nullified. We cannot conclude that Congress intended such a result, and we therefore hold that this evidence is insufficient to warrant a trial.⁵⁵

By contrast, as noted earlier in this section, Judge Fisher wrote in *dicta* that notices sent by third parties could provide red flag awareness, although the Ninth Circuit panel rejected the argument that email evidence presented by UMG was sufficient to create a factual dispute over Veoh's entitlement to the DMCA safe harbor because there was no evidence presented that Veoh in fact did not remove files when it received these notices (and any notices from copyright owners, as opposed to third parties, had to satisfy the requirements for DMCA notifications set forth in section 512(c)(3) before knowledge could be imputed to a service provider if it failed to disable access to or remove any material identified in the notification).⁵⁶

In *Viacom Int'l, Inc. v. YouTube, Inc.*,⁵⁷ the Second Circuit was unwilling to set the bar for red flag awareness as high as the Ninth Circuit previously had in *CCBill*, but it did set out a clear explanation of the difference between actual knowledge and red flag awareness, which the Ninth Circuit subsequently also adopted.⁵⁸ The *Viacom v. YouTube* panel explained that actual knowledge denotes subjective belief, whereas red flag awareness is judged by an objective

⁵⁵*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1024 (9th Cir. 2013).

⁵⁶*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1025 (9th Cir. 2013). The court, in *dicta*, explained how a user email informing a service provider of "infringing material and specifying its location" could provide red flag notice:

Although the user's allegations would not give Veoh actual knowledge under § 512(c)(1)(A)(i), because Veoh would have no assurance that a third party who does not hold the copyright in question would know whether the material was infringing, the email nonetheless could act as a red flag under § 512(c)(1)(A)(ii) provided its information was sufficiently specific.

Id. In its revised opinion, the Ninth Circuit panel also adopted the Second Circuit's analysis of the difference between actual knowledge and red flag awareness, as discussed below. *See id.* at 1025–26.

⁵⁷*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012).

⁵⁸*See UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1025–26 (9th Cir. 2013).

reasonableness standard.⁵⁹

A standard of objective reasonableness requires service providers to make sure that employees responsible for material stored at the direction of a user are well trained. Whether a service provider's conduct in fact is objectively reasonable, when challenged in litigation, may make determinations of red flag awareness difficult to resolve short of trial in some cases. Factual disputes over the propriety of failing to remove particular material in particular instances may be difficult to resolve on summary judgment, in at least some cases.

In practice, courts in the Second Circuit, like those in the Ninth Circuit, have imposed a high bar for when material may be found to raise a red flag, as underscored in the *Viacom v. YouTube* case itself.

Viacom v. YouTube, like *UMG v. Shelter Capital Partners*, was a case involving user-submitted videos where summary judgment had been granted in favor of the service provider and, on appeal, the copyright owner did not dispute that the service provider had removed every file identified in substantially complying DMCA notices. Indeed, in *Viacom v. YouTube*, District Court Judge Stanton of the Southern District of New York had observed that Viacom had accumulated information on approximately 100,000 videos and then sent one mass take-down notice on February 2, 2007, in response to which, by the next day, YouTube had removed virtually all of the identified videos.⁶⁰ The issue in each case was whether, notwithstanding compliance with DMCA notifications asking that specific files be taken down, the service provider nonetheless had knowledge or awareness that would preclude safe harbor protection.

In *Viacom v. YouTube*, the Second Circuit concluded that internal emails that referenced specific video files (as opposed to general percentages) could be viewed by a reasonable juror to evidence knowledge or awareness of specific instances of infringement. However, since the evidence did not make clear whether any of the videos referenced in internal emails were actually at issue in the lawsuit, the court remanded the case to the district court to determine whether

⁵⁹See *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 31 (2d Cir. 2012).

⁶⁰*Viacom Int'l Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *aff'd in part, vacated in part, rev'd in part*, 676 F.3d 19 (2d Cir. 2012).

any specific infringements of which YouTube had knowledge or awareness corresponded to any of the works at issue in the lawsuit.⁶¹

By contrast, the Second Circuit panel rejected as irrelevant internal surveys showing that YouTube employees estimated that 75-80% of YouTube streams constituted copyrighted material. While these estimates suggested that defendants were aware that “significant quantities of material on the YouTube website were infringing” the evidence was insufficient to create a triable issue of fact about whether YouTube “actually knew, or was aware of facts or circumstances that would indicate, the existence of *particular instances of infringement*.”⁶²

The Second Circuit panel remanded for further consideration the issue of whether YouTube had knowledge or awareness based on willful blindness. In *Global-Tech Appliances, Inc. v. SEB, S.A.*,⁶³ the U.S. Supreme Court had held that willful blindness is equivalent to knowledge for purposes of evaluating patent infringement. Applying this principle to the DMCA, the Second Circuit held that if a service provider made a “deliberate effort to avoid guilty knowledge” the willful blindness doctrine could be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA.⁶⁴

The appellate panel made clear that willful blindness under the DMCA, like other forms of knowledge or awareness, cannot be premised on generalized knowledge, but

⁶¹See *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 33–34 (2d Cir. 2012). On remand, the district court again granted summary judgment for YouTube, ruling, among other things, that YouTube did not have knowledge or awareness of any specific acts of infringement and had not willfully blinded itself to specific acts of infringement. See *Viacom Int'l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110 (S.D.N.Y. 2013).

⁶²*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 33 (2d Cir. 2012) (emphasis added).

⁶³*Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754, 769-70 (2011); *supra* § 4.11[6][A] (analyzing the case and its applicability to the doctrine of copyright inducement).

⁶⁴*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012), quoting *In re Aimster*, 334 F.3d at 650. On remand, the district court granted summary judgment for YouTube, holding that YouTube had not willfully blinded itself to specific acts of infringement. See *Viacom Int'l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110 (S.D.N.Y. 2013).

must be based on “specific instances of infringement”⁶⁵ Judge Cabranes also explained that service providers cannot be compelled to monitor their sites or affirmatively seek facts evidencing infringing activity as a condition for benefiting from the safe harbor, concluding that section 512(m) limited, but did not abrogate application of the willful blindness doctrine to the DMCA.⁶⁶ Thus, willful blindness may provide grounds for finding knowledge or awareness under the DMCA, but involves a more limited inquiry than when evaluating willful blindness to establish inducement because under the DMCA willful blindness may not be premised on either generalized knowledge or a failure to monitor or proactively search a site or service for infringing activity. Given this formulation, it is perhaps not surprising that Judge Cabranes cautioned that willful blindness may be difficult to assess absent explicit fact finding.⁶⁷

Although the Second Circuit characterized its analysis of willful blindness as involving an issue of first impression, in an earlier district court opinion, *Columbia Pictures Industries, Inc. v. Fung*,⁶⁸ Judge Stephen Wilson in Los Angeles had held that willful blindness amounted to red flag awareness.⁶⁹ In *Fung*, which is an inducement case discussed at length in section 4.11[6][F], the Ninth Circuit, applying

⁶⁵*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012).

⁶⁶*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012).

⁶⁷*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 n.10 (2d Cir. 2012), citing *Tiffany (NJ) v. eBay, Inc.*, 600 F.3d 93, 110 (2d Cir.), cert. denied, 562 U.S. 1082 (2010).

⁶⁸*Columbia Pictures Industries, Inc. v. Fung*, No. 06 Civ. 5578, 2009 WL 6355911 (C.D. Cal. Dec. 21, 2009), *aff'd in relevant part*, 710 F.3d 1020 (9th Cir. 2013).

⁶⁹The district court had found red flag awareness in connection with evaluating defendants' argument that they were entitled to the information location tools safe harbor, 17 U.S.C.A. § 512(d); *infra* § 4.12[7], because they disabled links whenever they received notices. Judge Wilson had found defendants ineligible for the user storage safe harbor set forth in 17 U.S.C.A. § 512(c) because the infringing material in *Fung* did not actually reside on Fung's servers. The Ninth Circuit disagreed with this analysis, declining to read requirements into the safe harbor that are not contained in the text of the DMCA and noting that section 512(c) “explicitly covers not just the storage of infringing material, but also infringing ‘activit[ies]’ that ‘us[e] the material [stored] on the system or network.’” *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1042 (9th Cir. 2013). As discussed earlier in this chapter, this analysis is incorrect. *See supra* § 4.12[6][A]. Section 512(c), while not limited to cases where material is stored on a service provider's servers, nonetheless is restricted to cases

the Second Circuit’s objective/subjective analysis of actual knowledge and red flag awareness from *Viacom v. YouTube*, ultimately ruled that Fung had red flag awareness of a broad range of infringing activity that precluded him from benefiting from either the user storage or information location tools safe harbors.⁷⁰ Fung and his company, isoHunt Web Technologies, Inc., operated the isohunt.com, torrentbox.com and podtropolis.com torrent sites and associated BitTorrent trackers, and the eDonkey site, ed2k-it.com.⁷¹ Fung’s level of knowledge and awareness was summarized by the Ninth Circuit panel but explained in greater detail in the district court’s opinion. The Ninth Circuit concluded that the record was

replete with instances of Fung actively encouraging infringement, by urging his users to both upload and download particular copyrighted works, providing assistance to those seeking to watch copyrighted films, and helping his users burn copyrighted material onto DVDs. The material in question was sufficiently current and well-known that it would have been objectively obvious to a reasonable person that the material solicited and assisted was both copyrighted and not licensed to random members of the public, and that the induced use was therefore infringing. Moreover, Fung does not dispute that he personally used the isoHunt website to download infringing material. Thus, while Fung’s inducing actions do not necessarily render him per se ineligible for protec-

involving “storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider” 17 U.S.C.A. § 512(c)(1); *supra* § 4.12[6][A] (analyzing this aspect of the court’s ruling). In *Fung*, the court did not find that the Bit Torrent tracker sites at issue constituted “a system or network controlled or operated by or for” Fung. *See* 17 U.S.C.A. § 512(c)(1). As explained in section 4.12[6][A], the Ninth Circuit’s reading of section 512(c) on this point therefore is not consistent with the plain terms of that statutory provision.

⁷⁰*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043–44, 1047 (9th Cir. 2013). The same panel that decided *Fung* also decided *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022 (9th Cir. 2011), *opinion withdrawn and replaced*, 718 F.3d 1006 (9th Cir. 2013). *Fung* was written by Judge Marsha S. Berzon, on behalf of herself and Judges Harry Pregerson and Raymond C. Fisher. *Shelter Partners* was authored by Judge Raymond C. Fisher, on behalf of himself and Judges Harry Pregerson and Marsha S. Berzon.

⁷¹A technical explanation of how BitTorrent protocols generally, and Fung’s sites in particular, operate, is set forth in section 4.11[6][F] in connection with a discussion of the *Fung* court’s analysis of defendants’ liability for copyright inducement.

tion under § 512(c), they are relevant to our determination that Fung had “red flag” knowledge of infringement.⁷²

With respect to knowledge, the district court had noted that although Fung’s sites were based in Canada, at the height of their popularity they had 10 million visitors each month, 25% of whom came from the United States to access content, more than 90% of which was found to be infringing. District Court Judge Wilson wrote that “unless Defendants somehow refused to look at their own webpages, they invariably would have known that (1) infringing material was likely to be available and (2) most of Defendants’ users were searching for and downloading infringing material.”⁷³ He wrote that in light of the “overwhelming evidence, the only way Defendants could have avoided knowing about their users’ infringement is if they engaged in ‘ostrich-like refusal to discover the extent to which [their] system[s] w[ere] being used to infringe copyright.’”⁷⁴

More broadly, the district court emphasized that inducement and the DMCA “are inherently contradictory. Inducement liability is based on active bad faith conduct aimed at promoting infringement; the statutory safe harbors are based on passive⁷⁵ good faith conduct aimed at operating a legiti-

⁷²*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043 (9th Cir. 2013).

⁷³*Columbia Pictures Industries, Inc. v. Fung*, No. 06 Civ. 5578, 2009 WL 6355911, at *17 (C.D. Cal. Dec. 21, 2009), *aff’d in relevant part*, 710 F.3d 1020 (9th Cir. 2013). The extent of defendants’ knowledge and encouragement of infringing activities is set forth in section 4.11[6][F], which discusses the case in connection with the court’s entry of summary judgment for the plaintiffs on their claim of copyright inducement.

⁷⁴*Columbia Pictures Industries, Inc. v. Fung*, No. 06 Civ. 5578, 2009 WL 6355911, at *18 (C.D. Cal. Dec. 21, 2009) (quoting *In re Aimster Copyright Litig.*, 334 F.3d 643, 655 (7th Cir. 2003)), *aff’d in relevant part*, 710 F.3d 1020 (9th Cir. 2013).

⁷⁵The district court’s reference to the safe harbor being based on “passive” conduct by service providers may be criticized as perpetuating the myth that the narrow definition of *service provider* applicable only to the transitory digital network communications safe harbor set forth in section 512(a) applies generally under the DMCA notwithstanding the much broader definition of the term when used in connection with the other safe harbors (which by no means is limited to passive service providers). Compare 17 U.S.C.A. § 512(k)(1)(A) (narrowly defining the term *service provider* for purposes only of the safe harbor created by section 512(a)) with 17 U.S.C.A. § 512(k)(1)(B) (broadly defining the same term for purposes of the user storage, information location tools and caching safe

mate internet business.”⁷⁶ The Ninth Circuit declined to endorse this view, agreeing instead with the Second Circuit⁷⁷ that DMCA safe harbors at least in theory are available to service providers in inducement cases.⁷⁸ In fact, however, the district court’s observation that evidence establishing inducement and proving entitlement to the user storage safe harbor “are inherently contradictory” represents the better view as a practical matter, even if *theoretically* safe harbor protection may be available, because of the requirement that a service provider not have red flag awareness (at least for the user storage and information location tools safe harbors and in some cases the caching safe harbor).⁷⁹ In practice, the level of knowledge that may be proven or imputed based on a finding of inducement (which requires evidence both of intent and affirmative steps) necessarily would establish awareness of facts and circumstances from which infringing activity is apparent and therefore preclude DMCA safe harbor protection.

In the appellate court ruling in *Fung*, the Ninth Circuit raised without deciding the question of whether red flag awareness would broadly preclude safe harbor protection or only for the specific files or activity at issue.⁸⁰ The Ninth Circuit panel found it unnecessary to resolve the question because in *Fung* it also found defendants ineligible for the

harbors); see generally *supra* § 4.12[2] (analyzing the definition of *service provider* in different contexts under the DMCA).

⁷⁶*Columbia Pictures Industries, Inc. v. Fung*, No. 06 Civ. 5578, 2009 WL 6355911, at *18 (C.D. Cal. Dec. 21, 2009), *aff’d in part and rev’d in part*, 710 F.3d 1020 (9th Cir. 2013).

⁷⁷See *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 41 (2d Cir. 2012) (holding that “a finding of safe harbor application necessarily protects a defendant from all affirmative claims for monetary relief.”).

⁷⁸See *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1039–40 (9th Cir. 2013) (holding that the DMCA potentially may be applied to a claim of inducement, although finding it inapplicable in that case). The *Fung* court did not suggest that the DMCA safe harbors in fact would be available in cases where a plaintiff otherwise could prove inducement, stressing merely that it was “conceivable that a service provider liable for inducement could be entitled to protection under the safe harbors” and explaining that it was “not clairvoyant enough to be sure that there are no instances in which a defendant otherwise liable for contributory copyright infringement could meet the prerequisites for one or more of the DMCA safe harbors.” *Id.* at 1040 (emphasis in original).

⁷⁹See 17 U.S.C.A. § 512(c)(1)(A)(ii).

⁸⁰*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043 n.20 (9th Cir. 2013).

safe harbor based on having a financial interest and the right and ability to control.⁸¹

Subsequent cases have either found⁸² or declined to find⁸³ evidence of willful blindness.

Among the early Circuit Court opinions analyzing knowledge or awareness, *Fung*, on the one hand, and *CCBill*, *Shelter Capital Partners* and *YouTube*, on the other, bookend the circumstances under which red flag awareness may be found (or found lacking). While service providers have no obligation to proactively search for or block infringing material and cannot be deemed to have knowledge or awareness based on a defective DMCA notice or generalized knowledge that a site or service may be used for infringement, they may not stick their heads in the sand or turn a blind eye to specific instances of infringement and expect to claim entitlement to safe harbor protection.

⁸¹*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043 n.20 (9th Cir. 2013). The financial interest/right and ability to control provision set forth in 17 U.S.C.A. § 512(c)(1)(B) is analyzed in section 4.12[6][D].

⁸²*See, e.g., Capitol Records, Inc. v. MP3Tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *3 (S.D.N.Y. May 14, 2013). In *MP3Tunes*, the district court held that certain evidence created a factual dispute on the issue of willful blindness, although the evidence described by the court sounded like it would be have been more relevant to the issue of red flag awareness based on subjective awareness judged by an objective standard of reasonableness, than willful blindness. Specifically, the court found that a jury could reasonably interpret several documents as imposing a duty to make further inquiries into specific and identifiable instances of possible infringement:

For example, an email received by MP3Tunes in April 2007 gives a specific blog title and states, “[a]lthough I don’t like ratting myself out, everything I post is in clear violation of the DMCA Another email from November 2007 states, “if you search for ‘the clash I fought the law’ . . . you will get 5 results . . . 2 of which point to the website www.officerjellnutz.com[.] This website blatantly acknowledges that it contains infringing MP3’s.” . . . In a third email, an MP3tunes employee acknowledges that while ‘it’s not clear if [content from a user’s site] is all copyright [six] material . . . it probably is

Id. The court’s confusion of red flag awareness with imputed awareness based on willful blindness merely underscores that red flag awareness in the Second and Ninth Circuits may be shown by either subjective awareness and an objectively unreasonable failure to disable access to or remove material or based on a deliberate attempt to avoid acquiring knowledge.

⁸³*See, e.g., Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 98-99 (2d Cir. 2016); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 611-12 (9th Cir. 2018); *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016).

Ultimately, by setting a high bar for what constitutes a red flag, the Ninth Circuit, in *CCBill*, provided a measure of protection to legitimate service providers on an issue that is potentially very difficult to evaluate, subject to the caveat from *dicta* in *Shelter Capital Partners* that notice from a third party could provide red flag awareness. *Fung*, by contrast, shows that pirate sites and services found liable for inducement, may not benefit from the generous leeway given to legitimate sites and services in evaluating whether they had knowledge or red flag awareness.

When material is stored at the direction of a user on a large site or service it may be very difficult in most instances for a service provider, absent receipt of a notification, to evaluate whether material is protected, in the public domain, created by the user, copied without authorization from a third party, licensed (expressly or impliedly) or employed as a fair use.

The complexities associated with identifying potential red flag material may be significant. For example, as of 2013, more than 100 hours of video were uploaded to YouTube every minute.⁸⁴

Even where a service provider has knowledge or awareness that a particular file is on its site, it may not be able to easily determine if it is authorized or infringing. Aspiring filmmakers, for example, may post seemingly amateurish work on the Internet in which they nonetheless claim protection if it is copied without authorization and stored somewhere other than where it was posted originally by the copyright owner. Conversely, clips from protected professional TV shows or music videos may be posted surreptitiously by marketing people or promoters for viral marketing

⁸⁴YouTube Statistics, <http://www.youtube.com/yt/press/statistics.html> (visited Aug. 3, 2013). As of that time, more than six billion hours of video were watched by YouTube users each month. *See id.* By comparison, as of May 2009, on average there were twenty hours of video uploaded every minute to YouTube. Timothy L. Alger, Deputy General Counsel, Google, Inc., Speech, American Bar Association Annual Meeting, Chicago, Aug. 2, 2009; YouTube Blog Post, http://youtube-global.blogspot.com/2009/05/zoinks-20-hours-of-video-uploaded-every_20.html (visited May 20, 2009). As of March 2010, that number had grown to twenty four hours of new video content uploaded every minute, with users partaking in more than 1 billion video views each day. *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 28 (2d Cir. 2012).

purposes.⁸⁵

Accordingly, proving knowledge or awareness may raise evidentiary issues in litigation, especially where the number of files potentially at issue is substantial. On remand from the Second Circuit, the district court in *Viacom Int'l, Inc. v. YouTube, Inc.*⁸⁶ addressed the issue of which party has the burden of proof when neither party can establish whether a service provider had knowledge or awareness of specific clips. In that case, YouTube had identified 63,060 video clips that were alleged to be infringing, for which it claimed it never received adequate notice from Viacom. At the time of the lawsuit, more than one billion videos were viewed daily on YouTube with more than 24 hours of new content uploaded every minute. Viacom argued that because neither side possessed the kind of evidence that would allow a clip-by-clip assessment of actual knowledge YouTube could not claim safe harbor protection since the DMCA is an affirmative defense. Judge Stanton disagreed, however, holding that the burden of notifying service providers of infringement under the DMCA is on copyright owners or their agents and cannot be shifted to the service provider to disprove.⁸⁷

⁸⁵See *infra* § 28.05 (viral marketing).

⁸⁶*Viacom Int'l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110 (S.D.N.Y. 2013).

⁸⁷*Viacom Int'l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 113–15 (S.D.N.Y. 2013). Judge Stanton characterized Viacom's argument as "ingenious, but . . . an anachronistic, pre-Digital Millennium Copyright Act (DMCA), concept." *Id.* at 114. He explained:

Title II of the DMCA (the Online Copyright Infringement Liability Limitation Act) was enacted because service providers perform a useful function, but the great volume of works placed by outsiders on their platforms, of whose contents the service providers were generally unaware, might well contain copyright-infringing material which the service provider would mechanically "publish," thus ignorantly incurring liability under the copyright law. The problem is clearly illustrated on the record in this case, which establishes that ". . . site traffic on YouTube had soared to more than 1 billion daily video views, with more than 24 hours of new video uploaded to the site every minute" . . . , and the natural consequence that no service provider could possibly be aware of the contents of each such video. To encourage qualified service providers, Congress in the DMCA established a "safe harbor" protecting the service provider from monetary, injunctive or other equitable relief for infringement of copyright in the course of service such as YouTube's. The Act places the burden of notifying such service providers of infringements upon the copyright owner or his agent. It requires such notifications of claimed infringements to be in writing and with specified contents and directs that deficient notifications shall not be considered in determining whether a service provider has actual or constructive knowledge. *Id.* § (3)(B)(i) If, as plaintiffs' assert, neither side can determine the presence or absence of specific infringements because of the vol-

Where emails or other internal communications suggest knowledge, awareness or willful blindness, the outcome may be different.⁸⁸ Thus, for example, the Second Circuit held in *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*,⁸⁹ in vacating the entry of summary judgment, that a jury could infer (but, implicitly was not necessarily required to find) red flag awareness where a service provider's executives admitted in public statements that legitimate copies of MP3 files had not been made commercially prior to January 2007 (or thereafter for some period of time, for songs by the Beatles), where internal emails identified these files to employees as having been sideloaded (or downloaded to sideload.com MP3 lockers) prior to January 2007 by users of the service. The court also held that the jury could have

ume of material, that merely demonstrates the wisdom of the legislative requirement that it be the owner of the copyright, or his agent, who identifies the infringement by giving the service provider notice. 17 U.S.C. § 512(c)(3)(A).

Id. at 114–15 (footnote omitted). The court further noted that “[t]he system is entirely workable: in 2007 Viacom itself gave such notice to YouTube of infringements by some 100,000 videos, which were taken down by YouTube by the next business day.” *Id.* at 115.

⁸⁸See, e.g., *Capitol Records, Inc. v. MP3Tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *4 (S.D.N.Y. May 14, 2013) (“reluctantly” concluding that the issue of red flag awareness under the DMCA could not be resolved on summary judgment given that under *Viacom v. YouTube* “[s]omething less than a formal takedown notice may now establish red flag knowledge” and EMI had introduced communications purporting to acknowledge likely infringement); see also *Capitol Records, Inc. v. MP3Tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *3 (S.D.N.Y. May 14, 2013) (finding a factual dispute on the issue of willful blindness based on emails received by MP3Tunes or composed by MP3Tunes employees). But see *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-99 (2d Cir. 2016) (rejecting evidence of employee interaction with allegedly infringing videos as evidence of knowledge, red flag awareness or willful blindness); *Capitol Records, LLC v. Vimeo, LLC*, Nos. 09-CV-10101 (RA), 09-CV-10105 (RA), 2021 WL 2181252 (S.D.N.Y. May 28, 2021) (granting summary judgment for Vimeo on all 281 user generated videos at issue, and rejecting that employees interacted with user-submitted videos—including, among other things, by applying music credits and tags, liking videos or adding them to promotional channels, or commenting on a video—as evidence that employees possessed facts making infringement objectively obvious “[b]ecause . . . a service provider cannot be presumed to know that content on its site is licensed or does not qualify as fair use, Plaintiff’s lack of evidence in that respect is dispositive.”).

⁸⁹*EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 92-94 (2d Cir. 2016) (reversing a lower court ruling vacating a jury verdict with respect to red flag awareness and willful blindness).

found that the defendant's service was "conceived of and designed to facilitate infringement," and that the defendant therefore was ineligible for DMCA protection due to willful blindness, based on trial testimony that MP3Tunes was intended to allow users to sideload "everything that was on the internet that was not locked down" and evidence that MP3Tunes executives encouraged sideloading of infringing music files (and in fact did so themselves).⁹⁰

Knowledge or awareness also may be shown where a site proactively monitors for infringing material. Service providers, under the DMCA, are not required to search for infringement⁹¹—they need only respond when they have knowledge or red flag awareness or if they receive a substantially complying notification. As a practical matter, however, many sites that host user content seek to deter infringement by reviewing user submissions, either before or after material is uploaded to a site.

Proactive monitoring can help keep infringement off a site, which in turn may discourage copyright owners from filing suit. It also can help rebut any inference of willful blindness. Where an agent or employee has reviewed material, however, the failure to take down a file could be found to constitute evidence of knowledge or awareness or to create a factual dispute precluding summary judgment (and necessitating a trial on the issue of a service's entitlement to DMCA protection), depending on the facts of a given case, which could substantially increase the costs and risks associated with litigating a DMCA case.

Judges and juries, in practice, usually cut some slack to a service that shows itself to be compliance oriented but may not have recognized a given file as infringing and taken it down, while not giving the benefit of the doubt to services where infringement is rampant and the site does not appear to actively deter or discourage it. Because red flag awareness is judged by an objective standard, however, there is some risk to monitoring and a perverse disincentive for service providers to proactively deter infringement.

Sites that allow users to upload music, often use filters to automatically identify attempted uploads of infringing music.

⁹⁰*EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 91–92 (2d Cir. 2016).

⁹¹*See* 17 U.S.C.A. § 512(m).

Assuming a site uses the filter to automatically block uploads, it should not be deemed to have knowledge or awareness of infringing material stored on the site. Of course, if a service provider employs filtering but allows files tagged as infringing to remain on the site, it likely would be found to have red flag awareness of those files (absent other facts such as confirmation that a particular file was flagged as a “false positive”). Filtering to block or remove infringing content, however, can reduce liability and rebut evidence of willful blindness.

The same is not necessarily true for material subject to human review. Where an agent or employee has reviewed material, the failure to take down a file could be found to constitute evidence of knowledge or awareness or to create a factual dispute precluding summary judgment, which could increase the costs and risks associated with litigating a DMCA dispute.

The conundrum of whether to use human reviewers to proactively monitor for infringement was brought into sharp focus by the Ninth Circuit’s ruling in *Mavrix Photographs, LLC v. LiveJournal, Inc.*⁹² In that case, LiveJournal allowed “moderators” to review posts prior to upload to ensure that they contained celebrity gossip and did not include pornography or harassing content. “Maintainers” were given further authority to delete posts and remove moderators. Finally, “owners” were authorized to remove maintainers. Approximately two-thirds of user submissions were rejected by these volunteers, who only uploaded one-third of user submissions to the site.⁹³

In an earlier part of the opinion discussed in section 4.12[6][A], the Ninth Circuit held that there was a disputed question of fact precluding summary judgment on the issue of LiveJournal’s entitlement to the DMCA safe harbor over whether pre-upload review by volunteer LiveJournal moderators meant that material submitted by users but only uploaded after review was posted by LiveJournal itself, or qualified as material stored “at the direction of a user,” which the Ninth Circuit panel held turned on questions of common

⁹²*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045 (9th Cir. 2017).

⁹³*See Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1050, 1059 (9th Cir. 2017).

law agency.⁹⁴ While LiveJournal argued that it did not assent to moderators acting on its behalf, the court found there was a disputed issue of fact over whether they had actual authority for purposes of establishing common law agency.⁹⁵

With respect to knowledge or awareness, the appellate panel wrote in *dicta* that if the photographs at issue were found to have been stored at the direction of a user, on remand, LiveJournal would have to show that it lacked both actual knowledge and red flag awareness of the alleged infringement.⁹⁶ The panel agreed with the lower court that there was no evidence of LiveJournal's actual knowledge because Mavrix had not sent a takedown notice to LiveJournal and the employee responsible for supervising moderators did not remember approving the posts. The panel, however, directed the district court to evaluate red flag awareness—specifically whether the service provider was “aware of facts and circumstances that would have made the specific infringement ‘objectively’ obvious to a reasonable person” which it characterized as “a high bar.”⁹⁷ The panel reiterated that to qualify as a red flag, “[t]he infringement must be immediately apparent to a non-expert.”⁹⁸ It noted, however, that some of the images contained watermarks, which could be relevant to the inquiry.⁹⁹ Accordingly, it instructed that to “determine whether LiveJournal had red flag knowledge, the

⁹⁴See *Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1052-57 (9th Cir. 2017); *supra* § 4.12[6][A].

⁹⁵*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1054-56 (9th Cir. 2017). Moderators were free to leave, not required to volunteer their time and could reject submissions for reasons other than those provided by LiveJournal. On the other hand, LiveJournal selected moderators, provided them with specific directions and exercised some degree of control. The appellate panel also found that at least some users believed that moderators acted with apparent authority.

⁹⁶*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1057-58 (9th Cir. 2017).

⁹⁷*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1057-58 (9th Cir. 2017) (quoting earlier cases).

⁹⁸*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1058 (9th Cir. 2017).

⁹⁹*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1058 n.14 (9th Cir. 2017) (“The existence of a watermark, and particularly . . . [a] watermark with a company name, is relevant to the knowledge inquiry.”). To both justify its focus on watermarks but also caution against concluding that the existence of a watermark is conclusive evidence, the panel noted that:

fact finder should assess if it would be objectively obvious to a reasonable person that material bearing a generic watermark or a watermark referring to a service provider's website was infringing."¹⁰⁰

The issue of watermarks was addressed by a subsequent Ninth Circuit panel, in *Ventura Content, Ltd. v. Motherless, Inc.*,¹⁰¹ in which the court held that the operator of a user-submitted porn site had neither actual knowledge nor red flag awareness of 33 videoclips that had been uploaded to the defendant's website by users of the site. In that case, the plaintiff and its expert witness argued that the defendants must have had actual knowledge of the video clips because they appeared to be professionally produced and a few had watermarks. The appellate court rejected this argument, however, because the watermarks displayed the URLs for pornography aggregators (such as *videosz.com* and *monstercockbabes.com*) and "gave no hint that Ventura owned the material."¹⁰²

The panel also rejected the argument that the high quality of the videos created at least a factual question precluding summary judgment on the issue of actual knowledge. The court explained that "[p]rofessionally created work often is posted online to publicize and attract business for the creator. Amateurs often do professional quality work in artistic endeavors, and amateurs are no less entitled to copyright protection than professionals, so it is not apparent why professionalism matters. And digital cameras have become so good and so easy to use that even home movies of children's birthday parties can look professionally done."¹⁰³ The panel also observed that it could not see what on the Ventura

Congress explained that red flag knowledge includes "customary indicia . . . such as a standard and accepted digital watermark." H.R. Rep. 105-55, pt. 1, at 25 (1998). *But see Veoh Networks Inc.*, 665 F. Supp. 2d at 1115 (declining to rely on this report because it addressed a "version of the DMCA that is significantly different in its text and structure than the version that Congress ultimately adopted").

Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d at 1058 n.13.

¹⁰⁰*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1058 (9th Cir. 2017).

¹⁰¹*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 608-12 (9th Cir. 2018).

¹⁰²*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 608 (9th Cir. 2018).

¹⁰³*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 608 (9th Cir. 2018).

videos distinguished them from amateur creations.¹⁰⁴

For similar reasons, the *Motherless* panel rejected plaintiff's argument that defendants had red flag awareness, which the court referred to as *apparent awareness*. The court found that there was nothing about the clips that would have made infringement apparent. With 12.6 million pictures and video clips on the site, the majority found it "hard to imagine" that the site's owner, or the contractor he paid to help him review thumbnail images of uploaded videos for Terms of Use violations, "would have spotted all the infringing videos with the few seconds of viewing they gave to each one."¹⁰⁵ The court emphasized that the mere "suspicion of infringement" is not the same as "facts making infringement obvious."¹⁰⁶ The majority concluded that "even if it were obvious to a reasonable person that some of the material on the site must be infringing, that is not enough to lose the safe harbor. It must be obvious that the particular material that is the subject of the claim is infringing. Here, it would not be obvious to a reasonable person that the clips excerpted from Ventura movies were infringing."¹⁰⁷

Although the majority in *Motherless* discussed the contents

¹⁰⁴*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 608 (9th Cir. 2018). The panel noted that "Ventura could have indicated its ownership by watermarking its videos as copyrighted, but it did not. And Ventura could have notified Motherless that the clips infringed on its copyright when it discovered them on Motherless's site, but it did not." *Id.* at 609.

¹⁰⁵*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 609 (9th Cir. 2018). The site used software that generated thumbnail images of five images from each video clip (captured at the 20, 40, 60, 80 and 100% time points in the clip), which the site owner or his contractor reviewed for Terms of Use violations. *See id.* at 601.

¹⁰⁶*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 610 (9th Cir. 2018), *quoting Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 98 (2d Cir. 2016). The panel explained:

The copyright owner must show knowledge, actual or red flag, for the videos that infringed its copyright and are the subject of its claim. And for red flag knowledge, infringement must be apparent, not merely suspicious. Congress used the word "apparent," not "suspicious" or some equivalent. Ventura, not Lange, is in charge of policing Motherless for its copyrighted material. Congress could have put the burden of policing infringement in suspicious circumstances on the provider, but it instead put it on the copyright holder.

Motherless, Inc., 885 F.3d at 610.

¹⁰⁷*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 611 (9th Cir. 2018), *citing Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93 (2d Cir. 2016) (*citing Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 30-31 (2d Cir. 2012)).

of 33 videos, in fact the defendants only reviewed five thumbnail images (or screen shots) taken at set intervals from each uploaded video. Had the court viewed the videos differently, it would have been relevant whether the thumbnails actually reviewed included the portions found objectively to evidence red flag awareness.

In addition to considering actual knowledge or awareness, the court also rejected plaintiff's argument that red flag (or apparent) awareness could be inferred based on willful blindness because the Motherless site took active steps to deter infringement.¹⁰⁸

Motherless serves as a reminder that the threshold for inferring knowledge or awareness, in the absence of expressly incriminating evidence (such as an admission at a deposition or a contemporaneous email or other electronic communication), is high. *LiveJournal* nevertheless underscores that a service provider that chooses to systematically manually review material submitted by users, to deter infringement or for other business reasons, potentially could have a more difficult time prevailing on the DMCA defense because of a plaintiff's ability to challenge any material on its site as objectively raising a red flag, even if reviewers fail to identify it as such and the service has no knowledge of the material. If every single file is reviewed, for example, then a plaintiff could challenge, *ex post facto*, a service's failure to disable access to or remove any file found on the service because red flag awareness is judged by objective criteria.¹⁰⁹ If every file on a site can be analyzed objectively, the risk of liability is greater because even the best reviewer may not recognize particular material as raising a red flag. This inquiry would also lengthen and make more expensive any infringement

¹⁰⁸See *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 611-12 (9th Cir. 2018) (contrasting *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020 (9th Cir. 2013)).

¹⁰⁹One district court imposed a higher burden of proof for a copyright owner to establish knowledge or red flag awareness where a service provider meets its threshold burden of showing entitlement to the DMCA safe harbor. See *Capitol Records, LLC v. Vimeo, LLC*, Nos. 09-CV-10101 (RA), 09-CV-10105 (RA), 2021 WL 2181252, at *5-12 (S.D.N.Y. May 28, 2021) (ruling that, under Second Circuit law, a copyright owner must not only show that the service provider reviewed a video but that the employees who reviewed the video "possessed facts that would enable them to identify the presence of copyrighted material in each of the Videos-in-Suit . . . [and that they] knew how to distinguish infringement from fair or authorized use, and that they were able to do so for each Video-in-Suit.").

suit. By contrast, if a service does not systematically manually review every file, but rather simply instructs employees to take down red flag material when they become aware of it, then absent direct evidence of knowledge or awareness (such as an employee admission in an email or testimony at a deposition), it is unlikely that a copyright owner could meet its burden of establishing knowledge or awareness based solely on the existence of an infringing file on a service provider's servers.¹¹⁰

The objective test for red flag awareness potentially creates a disincentive for service providers to routinely review all material uploaded to a site.¹¹¹

In many cases, of course, there is no clear record to show which user files, if any, actually were reviewed. Where it is unclear whether a site or its agents or employees had knowledge or awareness of specific files in the absence of a DMCA notification, whether a service provider can benefit from the safe harbor may depend on which party has the burden of proof.

In *Capitol Records, LLC v. Vimeo, LLC*,¹¹² Second Circuit Judge Leval recast the issues of knowledge, red flag awareness and imputed knowledge based on willful blindness in terms of the parties' respective burdens of proof in litigation.

Although the DMCA is an affirmative defense, Judge Leval held that where a service provider meets its initial burden of proving entitlement to the DMCA safe harbor, the burden shifts to the copyright owner to prove that the service provider is not entitled to safe harbor protection based on knowledge or red flag awareness (if the service provider allegedly failed to remove infringing files in the face of knowledge or awareness). If that subsequent burden is not met by the copyright owner, the service provider is deemed subject to the safe harbor.¹¹³

In *Vimeo*, the copyright owner had argued that Vimeo was

¹¹⁰See *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-99 (2d Cir. 2016) (discussing shifting burdens of proof under the DMCA).

¹¹¹As discussed earlier, the court's analysis of what constitutes material stored "at the direction of a user" further creates a disincentive for service providers to undertake pre-upload review of user submissions. See *supra* § 4.12[6][A].

¹¹²*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78 (2d Cir. 2016).

¹¹³See *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-95 (2d Cir. 2016).

not entitled to safe harbor protection because its employees had interacted with allegedly infringing content by posting comments, adding infringing videos to a channel or “liking” the video. Judge Leval held, however, that this was not enough. He explained that, in evaluating actual knowledge or red flag awareness, “[t]he hypothetical “reasonable person” to whom infringement must be obvious is an ordinary person—not endowed with specialized knowledge or expertise concerning music or the laws of copyright.”¹¹⁴ Thus, a service provider will not lose DMCA protection merely because an employee sees or likes infringing content and doesn’t recognize it as infringing. Judge Leval reiterated that section 512(m) “makes clear that the service provider’s personnel are under no duty to ‘affirmatively seek[]’ indications of infringement.”¹¹⁵ Judge Leval reiterated that where, as in *Vimeo*, the service provider has established its entitlement to DMCA protection, the burden to show “disqualifying knowledge . . . falls on the copyright owner”¹¹⁶

Accordingly, Judge Leval held that a “copyright owner’s mere showing that a video posted by a user on the service provider’s site includes substantially all of a recording of recognizable copyrighted music, and that an employee of the service provider saw at least some part of the user’s material, is insufficient to sustain the copyright owner’s burden of proving that the service provider had either actual or red flag knowledge of the infringement.”¹¹⁷ Judge Leval justified this rule on several grounds:

First, the employee’s viewing might have been brief. The fact that an employee viewed enough of a video to post a brief comment, add it to a channel (such as kitten videos) or hit the “like” button, would not show that she had ascertained that its audio track contains all or virtually all of a piece of music.

Second, the insufficiency of some viewing by a service provid-

¹¹⁴*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-94 (2d Cir. 2016).

¹¹⁵*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 94 (2d Cir. 2016).

¹¹⁶*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 95 (2d Cir. 2016); see also *Atlantic Recording Corp. v. Spinrilla, LLC*, 506 F. Supp. 3d 1294, 1317 (N.D. Ga. 2020) (following *Vimeo* on this point, writing that, “[i]mportantly, if a service provider is otherwise eligible for the safe harbor defense, the burden of proof is on the copyright owner to show that the service provider failed to respond appropriately to actual or red flag knowledge.”).

¹¹⁷*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 96 (2d Cir. 2016).

er's employee to prove the viewer's awareness that a video contains all or virtually all of a song is all the more true in contemplation of the many different business purposes for which the employee might have viewed the video. The purpose of the viewing might include application of technical elements of computer expertise, classification by subject matter, sampling to detect inappropriate obscenity or bigotry, and innumerable other objectives having nothing to do with recognition of infringing music in the soundtrack. Furthermore, the fact that music is "recognizable" (which, in its dictionary definition of "capable of being recognized" would seem to apply to all music that is original and thus distinguishable from other music), or even famous (which is perhaps what the district court meant by "recognizable"), is insufficient to demonstrate that the music was in fact recognized by a hypothetical ordinary individual who has no specialized knowledge of the field of music. Some ordinary people know little or nothing of music. Lovers of one style or category of music may have no familiarity with other categories. For example, 60-year-olds, 40-year-olds, and 20-year-olds, even those who are music lovers, may know and love entirely different bodies of music, so that music intimately familiar to some may be entirely unfamiliar to others.

Furthermore, employees of service providers cannot be assumed to have expertise in the laws of copyright. Even assuming awareness that a user posting contains copyrighted music, the service provider's employee cannot be expected to know how to distinguish, for example, between infringements and parodies that may qualify as fair use. Nor can every employee of a service provider be automatically expected to know how likely or unlikely it may be that the user who posted the material had authorization to use the copyrighted music. Even an employee who was a copyright expert cannot be expected to know when use of a copyrighted song has been licensed. Additionally, the service provider is under no legal obligation to have its employees investigate to determine the answers to these questions.¹¹⁸

As applied to Vimeo, Judge Leval explained that plaintiffs

¹¹⁸*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 95-97 (2d Cir. 2016). Judge Leval conceded that:

It is of course entirely possible that an employee of the service provider who viewed a video did have expertise or knowledge with respect to the market for music and the laws of copyright. The employee may well have known that the work was infringing, or known facts that made this obvious. The copyright owner is entitled to discovery in order to obtain the specific evidence it needs to sustain its burden of showing that the service provider did in fact know of the infringement or of facts that made infringement obvious. But the mere fact that a video contains all or substantially all of a piece of recognizable, or even famous, copyrighted music and was to some extent viewed (or even viewed in its entirety) by some employee of a service provider would be insufficient

established merely that some employee of Vimeo had some contact with a user-posted video that played all, or nearly all, of a recognizable song, which was “not sufficient to satisfy plaintiffs’ burden of proof that Vimeo forfeited the safe harbor by reason of red flag knowledge with respect to that video.”¹¹⁹

The appellate panel vacated the lower court rulings on knowledge or awareness based on the conduct of employees, remanding with instructions that Vimeo “is entitled to summary judgment on those videos as to the red flag knowledge issue, unless plaintiffs can point to evidence sufficient to carry their burden of proving that Vimeo personnel either knew the video was infringing or knew facts making that conclusion obvious to an ordinary person who had no specialized knowledge of music or the laws of copyright.”¹²⁰

(without more) to sustain the copyright owner’s burden of showing red flag knowledge.

Id. at 97.

¹¹⁹*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 97 (2d Cir. 2016).

¹²⁰*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 98 (2d Cir. 2016).

On remand, Judge Ronnie Abrams granted summary judgment for Vimeo on all 281 user generated videos (holding that fact issues precluded summary judgment with respect to 26 additional videos uploaded by employees), ruling, with respect to the user-uploaded videos, that “[b]ecause . . . a service provider cannot be presumed to know that content on its site is licensed or does not qualify as fair use, Plaintiff’s lack of evidence in that respect is dispositive.” *Capitol Records, LLC v. Vimeo, LLC*, Nos. 09-CV-10101 (RA), 09-CV-10105 (RA), 2021 WL 2181252, at *12 (S.D.N.Y. May 28, 2021). Judge Abrams dismissed arguments that Vimeo executives were familiar with copyright law concepts and music licensing because the relevant question was whether the Vimeo employees who reviewed the videos-in-suit “possessed facts that would enable them to identify the presence of copyrighted material in each of the Videos-in-Suit. [Plaintiffs] also bear the burden of demonstrating that Vimeo employees knew how to distinguish infringement from fair or authorized use, and that they were able to do so for each Video-in-Suit.” *Id.* at *5. Although plaintiff presented evidence that some employees were generally aware of copyright obligations, Judge Abrams reiterated that the Second Circuit had held that the DMCA does not impose an amorphous obligation to take commercially reasonable steps in response to a generalized awareness of infringement, noting that “[e]ven if Vimeo did adopt a cavalier approach towards copyright infringement, that would not disqualify Vimeo from the safe harbor, because it does not demonstrate that it failed to act in the face of specific, “objectively obvious” instances of infringement.” *Id.* at *6. At most, plaintiffs’ evidence permitted “an inference that some Vimeo employees may have been broadly familiar with concepts such as fair use. Such evidence does not, on its own, permit the Court to infer that this

Judge Leval also rejected plaintiffs' argument that Vimeo's knowledge or awareness could be established through willful blindness. Plaintiffs had argued that, based on evidence that Vimeo monitored videos for infringement of *visual* content but not for infringement of *audio* content, Vimeo demonstrated willful blindness to infringement of music. Plaintiffs also argued that Vimeo's awareness of facts suggesting a likelihood of infringement gave rise to a duty to investigate further, and that Vimeo's failure to do so showed willful blindness that justifies liability. Finally, they argued that, having encouraged users to post infringing matter, Vimeo could not then close its eyes to the resulting infringements without liability. In rejecting those arguments, Judge Leval explained:

§ 512(m) relieves the service provider of obligation to monitor for infringements posted by users on its website. We see no reason why Vimeo's voluntary undertaking to monitor videos for infringement of visual material should deprive it of the statutory privilege not to monitor for infringement of music. Plaintiffs' argument is refuted by § 512(m).

Their second argument, that awareness of facts suggesting a likelihood of infringement gave rise to a duty to investigate further, does not fare better. Section 512(c) specifies the consequences of a service provider's knowledge of facts that might show infringement. If the service provider knows of the infringement, or learns of facts and circumstances that make infringement obvious, it must act expeditiously to take down the infringing matter, or lose the protection of the safe harbor. But we can see no reason to construe the statute as vitiating the protection of § 512(m) and requiring investigation merely because the service provider learns facts raising a *suspicion* of infringement (as opposed to facts making infringement *obvious*). Protecting service providers from the expense of monitoring was an important part of the compromise embodied in the safe harbor. Congress's objective was to serve the public interest by encouraging Internet service providers to make expensive investments in the expansion of the speed and capacity of the Internet by relieving them of burdensome expenses and liabilities to copyright owners, while granting to the latter compensating protections in the service providers' takedown

knowledge armed employees with the ability to distinguish infringements from authorized or fair use with respect to any of the Videos-in-Suit." *Id.* at *7. Judge Abrams likewise rejected evidence that employees interacted with user-submitted videos—including, among other things, by applying music credits and tags, liking videos or adding them to promotional channels, or commenting on a video—as evidence that the employee possessed facts making infringement objectively obvious. *Id.* at *7-12.

obligations. If service providers were compelled constantly to take stock of all information their employees may have acquired that might suggest the presence of infringements in user postings, and to undertake monitoring investigations whenever some level of suspicion was surpassed, these obligations would largely undo the value of § 512(m). We see no merit in this argument.

Plaintiffs' third argument may fare better in theory, but is not supported by the facts of this case In *Viacom*, we made clear that actual and red flag knowledge under the DMCA ordinarily must relate to "specific infringing material," *id.* at 30, and that, because willful blindness is a proxy for knowledge, *id.* at 34–35, it too must relate to specific infringements. Plaintiffs argue, however, that Vimeo, in order to expand its business, actively encouraged users to post videos containing infringing material. They argue that, notwithstanding the formulation in *Viacom*, a service provider cannot adopt a general policy of urging or encouraging users to post infringing material and then escape liability by hiding behind a disingenuous claim of ignorance of the users' infringements.¹²¹

Judge Leval concluded that the evidence didn't support this last argument and therefore declined to decide whether plaintiffs' interpretation of *Viacom* was correct as a matter of law.

Approximately two months before the Second Circuit issued its opinion in *Vimeo*, the Tenth Circuit had also addressed whether the conduct of employees or independent contractors could deprive a service provider of DMCA safe harbor protection. In that case, *BWP Media USA, Inc. v. Clarity Digital Group, LLC*,¹²² the Tenth Circuit considered whether a site that used affiliates (called "examiners") to contribute articles for compensation could qualify for DMCA protection.

Although the court did not reach the question of whether knowledge or awareness on the part of examiners could be imputed to the site because the issue was not properly preserved for appeal, its analysis of the related question of whether user uploads constituted material stored "at the direction of a user" makes clear that a service provider would not automatically lose DMCA protection for the infringing activity of employees in the Tenth Circuit where the employ-

¹²¹*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 98-99 (2d Cir. 2016).

¹²²*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175 (10th Cir. 2016).

ees were merely acting as users of the service, rather than in their capacity as employees. The court construed the term *user* very broadly, holding that uploads by examiners, who were independent contractors, qualified as material stored at the direction of a user, even though it was solicited by the site, which paid for it.¹²³ The appellate panel also explained that its analysis would apply equally if the examiners were agents of the service provider or employees.¹²⁴ By extension, although the panel did not reach the issue, employee knowledge or awareness should not be imputed to a service provider, at least in the Tenth Circuit, where the employee was merely acting as a user of the site, and not an employee.¹²⁵

On the issue of knowledge or awareness based on willful blindness, the court in *BWP Media* held that the plaintiff could not establish willful blindness based on the service provider's encouragement of examiners to upload photographs, where the site provided users with access to a database of licensed images (and there was nothing in the record to suggest that the service either encouraged infringement or turned a blind eye to it).¹²⁶

As illustrated in that case, the presence of licensed material may make it harder for a copyright owner to establish knowledge, red flag awareness or willful blindness based merely on a service encouraging uploads to the site¹²⁷ or because an employee could have difficulty differentiating

¹²³*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1179-81 (10th Cir. 2016); see *supra* § 4.12[6][A] (analyzing *BWP Media*'s holding on what constitutes "storage at the direction of a user").

¹²⁴*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1181 (10th Cir. 2016).

¹²⁵In *Capitol Records, LLC v. Vimeo, LLC*, Nos. 09-CV-10101 (RA), 09-CV-10105 (RA), 2021 WL 2181252, at *12 (S.D.N.Y. May 28, 2021), the district court denied in part summary judgment with respect to 26 videos uploaded by Vimeo employees, even as it granted summary judgment for Vimeo with respect to all user-submitted videos, because fact issues precluded summary judgment on the question of whether these videos were uploaded by Vimeo employees in their personal capacities as users or as agents of Vimeo.

¹²⁶*BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016).

¹²⁷See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1022-23 (9th Cir. 2013) (holding that "merely hosting a category of copyrightable content, such as music videos, with the general knowledge that one's services could be used to share infringing material, is insuf-

which material is licensed or unlicensed.¹²⁸

Applying *Vimeo* (and consistent with *BWP*), Southern District of New York Judge Jed Rakoff held, in *Downs v. Oath Inc.*,¹²⁹ that Oath did not lose DMCA safe harbor protection based on red flag awareness, where its employee reviewed the photograph at issue for offensive and illegal content and added content tags and related video links, despite plaintiff's argument that the photo should have raised a red flag because it included a *New York Daily News* credit line. Judge Rakoff held that, as in *Vimeo*, the Oath reviewer may have viewed plaintiff's photograph only briefly, while she was viewing the article "for multiple purposes, including subject matter classification and screening for offensive content."¹³⁰ While he conceded that it was possible that the reviewer—identified as Chloe Cohn—saw the *New York Daily News* photo credit, Judge Rakoff explained that under *Vimeo* "this possibility is not enough to create a triable issue as to red flag knowledge" because the burden of proof was on the plaintiff to demonstrate that Cohn had acquired knowledge of "facts and circumstances from which infringing activity was obvious."¹³¹ As in *Vimeo*, the court considered the fair use and licensing issues associated with images made it difficult to expect that an employee "could be expected to distinguish between infringements and fair or authorized uses."¹³² Judge Rakoff explained that "immunity under the DMCA's safe harbor does not depend on whether a 'HuffPost professional' or a 'trained professional in Cohn's position' would or should have known that the photograph in Kim's article was infringing. Instead, immunity depends on whether the infringement would have been 'obvious to a reasonable person . . . not endowed with specialized knowledge

ficient to meet the actual knowledge requirement under § 512(c)(1)(A)(i)" or to establish red flag awareness); *BWP Media USA, Inc. v. Clarity Digital Group, LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) ("Although BWP is correct in stating AXS encouraged Examiners to incorporate photographs into articles, AXS provided Examiners a legal means by which to accomplish this. Examiners have access to a photo bank full of images for which AXS owns the licenses.").

¹²⁸See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1023 (9th Cir. 2013).

¹²⁹*Downs v. Oath Inc.*, 385 F. Supp. 3d 298 (S.D.N.Y. 2019).

¹³⁰*Downs v. Oath Inc.*, 385 F. Supp. 3d 298, 306 (S.D.N.Y. 2019).

¹³¹*Downs v. Oath Inc.*, 385 F. Supp. 3d 298, 306 (S.D.N.Y. 2019).

¹³²*Downs v. Oath Inc.*, 385 F. Supp. 3d 298, 306-07 (S.D.N.Y. 2019).

or expertise concerning . . . the laws of copyright.’ ”¹³³

In *Vimeo* on remand, five years after the Second Circuit’s ruling, Judge Ronnie Abrams granted summary judgment for Vimeo on all 281 user generated videos, but held that fact issues precluded summary judgment with respect to 26 additional videos uploaded by employees where it was disputed whether the employees were acting in their individual capacity or as agents of Vimeo. With respect to the user-uploaded videos, Judge Abrams held that plaintiffs had a double burden of proof to show that Vimeo reviewers (1) “possessed facts that would enable them to identify the presence of copyrighted material in each of the Videos-in-Suit” and (2) “knew how to distinguish infringement from fair or authorized use, and that they were able to do so for each Video-in-Suit.”¹³⁴ In granting summary judgment for Vimeo on the user-submitted videos, Judge Abrams rejected evidence that employees interacted with user-submitted videos—including, among other things, by applying music credits and tags, liking videos or adding them to promotional channels, or commented on a video—as evidence that the employee possessed facts making infringement objectively obvious.¹³⁵ She likewise rejected arguments that Vimeo executives were familiar with copyright law concepts and music licensing as relevant because the DMCA does not impose an amorphous obligation to take commercially reasonable steps in response to a generalized awareness of infringement, noting that “[e]ven if Vimeo did adopt a cavalier approach towards copyright infringement, that would not disqualify Vimeo from the safe harbor, because it does not demonstrate that it failed to act in the face of specific, “objectively obvious” instances of infringement.”¹³⁶ At most, plaintiffs’ evidence permitted “an inference that some Vimeo employees may have been broadly familiar with concepts such as fair use. Such evidence does not, on its own, permit the Court to infer that this knowledge armed employees with

¹³³*Downs v. Oath Inc.*, 385 F. Supp. 3d 298, 305-06 (S.D.N.Y. 2019), quoting *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-94 (2d Cir. 2016).

¹³⁴*Capitol Records, LLC v. Vimeo, LLC*, Nos. 09-CV-10101 (RA), 09-CV-10105 (RA), 2021 WL 2181252, at *5 (S.D.N.Y. May 28, 2021).

¹³⁵*Capitol Records, LLC v. Vimeo, LLC*, Nos. 09-CV-10101 (RA), 09-CV-10105 (RA), 2021 WL 2181252, at *7-12 (S.D.N.Y. May 28, 2021).

¹³⁶*Capitol Records, LLC v. Vimeo, LLC*, Nos. 09-CV-10101 (RA), 09-CV-10105 (RA), 2021 WL 2181252, at *6 (S.D.N.Y. May 28, 2021).

the ability to distinguish infringements from authorized or fair use with respect to any of the Videos-in-Suit.”¹³⁷

As a majority of courts have now held that knowledge or awareness must be shown by reference to specific instances of infringement, not merely generalized knowledge that a site or service may be used for infringing activity, plaintiffs in DMCA cases increasingly allege willful blindness. Willful blindness, in a sense, is the flip side of generalized knowledge, in that a site that has generalized knowledge or awareness that the service may be used for infringement but no knowledge or awareness of specific files, could be accused of turning a blind eye to infringement. While all user sites in some sense have generalized knowledge that they could be used for infringement, willful blindness requires a much greater showing than that. Sites that seek to deter infringement and do not encourage it would not be found willfully blind absent direct evidence of turning a blind eye to specific instances of infringement.

Entitlement to DMCA safe harbor protection generally is resolved on summary judgment (unless it is apparent from the face of a complaint that the defendant is entitled to the defense). In rare instances, the issue of entitlement to the DMCA safe harbor may be resolved at trial. When that happens, copyright owners have sometimes chosen to streamline their trial presentation by selecting categories of works to present to the jury where the volume of allegedly infringing material is substantial. For example, in *Capitol Records, Inc. v. MP3Tunes, LLC*,¹³⁸ the record company plaintiffs chose to focus on, and obtained jury findings of red flag awareness and willful blindness, with respect to: (1) takedown notices identifying ten or more infringing files on a domain; (2) Sideloads of MP3s before January 2007; (3) Sideloads by MP3Tunes executives;¹³⁹ and (4) works by The Beatles.

In post-trial proceedings, the court granted the individual

¹³⁷*Capitol Records, LLC v. Vimeo, LLC*, Nos. 09-CV-10101 (RA), 09-CV-10105 (RA), 2021 WL 2181252, at *7 (S.D.N.Y. May 28, 2021).

¹³⁸*Capitol Records, Inc. v. MP3Tunes, LLC*, 48 F. Supp. 3d 703 (S.D.N.Y. 2014), *aff'd in part, rev'd in part sub nom. EMI Christian Music Group, Inc. v. MP3tunes, LLC*, 844 F.3d 79 (2d Cir. 2016).

¹³⁹Evidence presented at trial, which the court ruled supported the jury's finding of red flag awareness and willful blindness, included that MP3Tunes' executives sideloaded songs and, in the process of doing so, viewed the source domain's URL along with the artist and track title. They knew personal sites on storage service domains and student pages

defendant's motion for judgment as a matter of law on the first category because neither red flag awareness nor willful blindness could be imputed based on evidence that MP3Tunes could have but did not investigate domains listed multiple times in DMCA notices to uncover other instances of infringement not identified in the notices. Judge Pauley explained that the DMCA only imposes an obligation on service providers "to track repeat infringement by users, not third parties."¹⁴⁰ This ruling was not challenged on appeal.

Judge Pauley also granted defendants' motion for judgment as a matter of law with respect to jury findings of red flag awareness and willful blindness based on user sideloads of (a) MP3 files prior to January 2007 and (b) songs by the Beatles, which were rulings that the Second Circuit vacated on appeal. The Second Circuit held that the jury could have inferred red flag awareness where a service provider's executives made public statements acknowledging that legitimate copies of MP3 files had not been made commercially prior to January 2007 (or thereafter for some period of time, for songs by the Beatles), where internal emails identified these files to employees as having been sideloaded by users of the service.¹⁴¹ In an amended opinion, however, the panel further cautioned in a footnote that it did not "mean to suggest that a copyright holder may create red-flag knowledge merely by asserting that distribution of its works is 'never

on college websites had a high probability of hosting infringing material and nonetheless sideloaded files from what the evidence suggested were obviously infringing websites such as clockworkchaos.net, fileden.com, www.myfilestash.com, and oregon-state.edu. Judge Pauley explained that "[b]ecause MP3Tunes' Executives observed those clearly infringing source domains, the jury could conclude that it would be objectively obvious to a reasonable person (here, MP3Tunes) that any tracks sideloaded from those domains were infringing." *Capitol Records, Inc. v. MP3Tunes, LLC*, 48 F. Supp. 3d 703, 717 (S.D.N.Y. 2014). These specific findings were not challenged on appeal.

¹⁴⁰*Capitol Records, Inc. v. MP3Tunes, LLC*, 48 F. Supp. 3d 703, 716 (S.D.N.Y. 2014).

¹⁴¹*EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 93 (2d Cir. 2016). The court also held that the jury could have found that the defendant's service was "conceived of and designed to facilitate infringement," and that the defendant therefore was ineligible for DMCA protection based on willful blindness, based on trial testimony that MP3Tunes was intended to allow users to sideload "everything that was on the internet that was not locked down" and evidence that MP3Tunes executives encouraged sideloading of infringing music files (and in fact did so themselves). *See id.* at 93-44.

authorized.’ ”¹⁴²

With respect to employee uploads, the Second Circuit addressed the issue in the context of repeat infringement and liability based on principles of respondeat superior, rather than specifically in terms of knowledge, awareness or willful blindness under the DMCA, although the appellate panel’s rulings implicitly assume knowledge or red flag awareness by MP3Tunes executives.¹⁴³

Among other things, the *MP3Tunes* case underscores the potential costs to both copyright owners and service providers of litigating DMCA issues in cases where thousands of files are at issue. In ruling on post-trial motions in 2014, Judge William H. Pauley III lamented that “[w]hile the world has moved beyond the free-MP3-download craze, the parties in this case have not. This hard-fought litigation spans 7 years and 628 docket entries. Numerous substantive motions were heard. And decisions by this Court did not deter the parties from revisiting the same issues time and again. As trial approached, the parties launched salvos of motions *in limine* seeking to resurrect discovery disputes, relitigate prior motions, and level an impressive array of claims and

¹⁴²*EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 93 n.8 (2d Cir. 2016).

¹⁴³The Second Circuit held that a reasonable jury could infer that a service provider consciously avoided knowing about specific repeat infringers using its service, which would amount to a failure to reasonably implement its repeat infringer policy, where company executives were encouraged to and did personally use a service to link to or download infringing music for their personal use. See *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 90-91 (2d Cir. 2016); *supra* § 4.12[3][B] (discussing the case in the context of repeat infringer policies under the DMCA). Elsewhere in the opinion, the court held that a reasonable jury could infer that the company was liable for employee infringement under principles of respondeat superior, where, among other things, evidence was presented at trial that an executive wrote an email asserting that MP3Tunes employees “would see[d] the [sideload.com] index with higher quality tracks,” an employee testified that she and other MP3tunes employees “specifically sought out websites on the Internet to locate files and sideload them into the Sideload index,” and that they all did so “as employees of MP3tunes,” and where the CEO directed that same employee to provide other MP3tunes employees a “list of some sites featuring free MP3s. . . for sideloading purposes.” *Id.* at 97. The panel elaborated that “[t]here was also ample evidence from which a juror could reasonably have inferred that these executive sideloads were performed from MP3tunes’s offices. And it was clearly in MP3tunes’s interest to increase the number of quality songs on sideload.com by using its employees to expand the index.” *Id.*

defenses Despite this Court’s efforts to winnow the issues, the parties insisted on an 82–page verdict sheet on liability and a 331–page verdict sheet on damages that included dense Excel tables, necessitating at least one juror’s use of a magnifying glass.”¹⁴⁴ The case resulted in a jury verdict against MP3Tunes and its owner of \$48,061,073 in damages.¹⁴⁵ And that was all before the appeal. On appeal, the Second Circuit vacated the district court’s entry of partial summary judgment for the defendants on MP3Tunes’ entitlement to DMCA safe harbor protection based on the lower court’s application of too narrow a definition of what constitutes a “repeat infringer,” and reversed the district court’s grant of judgment as a matter of law for the defendants on claims of infringement of pre-January 2007 and Beatles MP3 files, based on red flag awareness and willful blindness.¹⁴⁶

While the *MP3Tunes* case involved a risky business model—characterized by Judge Pauley as one “designed to operate at the very periphery of copyright law”¹⁴⁷—it nonetheless provides a cautionary tale for service providers on how complex and expensive it can be to litigate DMCA issues and how risky it may be to cut corners in implementing the DMCA, turn a blind eye to infringement or ignore red flags.

Where service providers know or become aware of specific infringing material or activity, they must take action or risk losing safe harbor protection.

4.12[6][D] Direct Financial Benefit/Right and Ability to Control

The requirement that a service provider “not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and

¹⁴⁴*Capitol Records, Inc. v. MP3Tunes, LLC*, 48 F. Supp. 3d 703, 710 (S.D.N.Y. 2014).

¹⁴⁵*Capitol Records, Inc. v. MP3Tunes, LLC*, 48 F. Supp. 3d 703, 711, 733 (S.D.N.Y. 2014). (ordering plaintiffs to elect remittitur or a new trial).

¹⁴⁶See *EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 89-94 (2d Cir. 2016).

¹⁴⁷*Capitol Records, Inc. v. MP3Tunes, LLC*, 48 F. Supp. 3d 703, 710 (S.D.N.Y. 2014), *aff’d in part, rev’d in part sub nom. EMI Christian Music Group, Inc. v. MP3tunes, LLC*, 844 F.3d 79 (2d Cir. 2016).

ability to control such activity”¹ is derived from the common law test for vicarious copyright liability, which may be imposed where a defendant (1) has the right and ability to supervise the infringing activity, and (2) has a direct financial interest in it.² While a plaintiff has the burden of proving both prongs to establish vicarious liability, the analogous DMCA provision allows a service provider to benefit from the user storage safe harbor even if one element applies, so long as both elements are not found.³ Thus, a service provider will be entitled to the safe harbor if it has a financial interest but no right and ability to control⁴ or if it

[Section 4.12[6][D]]

¹17 U.S.C.A. § 512(c)(1)(B).

²See, e.g., *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996); see generally *supra* §§ 4.11[4], 4.11[5] (discussing common law vicarious liability cases).

³See, e.g., *Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1044-46 (9th Cir. 2013) (holding the defendant ineligible for the user storage safe harbor because he had both a financial interest—where the defendant earned advertising revenue from ads marketed based on the popularity of infringing material on his sites, where approximately 90-96 percent (or perhaps slightly less) of the content on the service was infringing and the defendant actively induced infringement by users of the service — and the right and ability to control, because Fung organized torrent files on his sites using a program that matched file names and content with specific search terms describing material likely to be infringing, such as “screener” or “PPV,” and personally assisted users in locating infringing content, and where there was “overwhelming evidence that Fung engaged in culpable, inducing activity . . . [that] demonstrate[d] the substantial influence Fung exerted over his users’ infringing activities . . .”).

⁴See, e.g., *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1110 (W.D. Wash. 2004) (“Because Amazon does not have the right and ability to control the infringing material, it is not necessary for this Court to inquire as to whether Amazon receives a direct financial benefit from the allegedly infringing activity.”).

In *Agence France Presse v. Morel*, 934 F. Supp. 2d 547, 568 (S.D.N.Y. 2013), the court denied the defendant’s summary judgment motion in part because it found that there was a dispute over whether the defendant had received a financial benefit directly attributable to infringing activity. To the extent that the court made this ruling without considering whether the defendant had the right and ability to control it was wrongly decided. Other aspects of the court’s DMCA analysis are also subject to criticism. See *supra* §§ 4.12[2] (criticizing the court’s interpretation of the term *service provider*), 4.12[6][C] (criticizing the court’s mischaracterization of the knowledge or awareness prong as requiring that a service provider have a “requisite intent” to qualify for the safe harbor).

has the right and ability to control but no financial interest⁵ (or, of course, if neither prong applies).

The financial interest prong has been construed in the Ninth Circuit to require a showing that “the infringing activity constitutes a draw for subscribers, not just an added benefit.”⁶ Case law construing the financial interest prong is discussed later in this subsection.

The Second, Fourth and Ninth Circuits have held that right and ability to control within the meaning of section 512(c)(1)(B) of the DMCA requires a higher showing than what would be required to establish common law vicarious liability—*i.e.*, more than merely the ability to block access or remove content—because otherwise section 512(c)(1)(B) would disqualify any service provider that in fact has the ability to do exactly what section 512(c) of the DMCA requires service providers to do to benefit from the safe harbor, namely, to disable access to or remove material in response to notice, knowledge or awareness of infringing

⁵*See, e.g., Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir.) (“Because CWI does not receive a direct financial benefit, CWIE meets the requirements of § 512(c).”), *cert. denied*, 522 U.S. 1062 (2007).

⁶*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1044-45 (9th Cir. 2013) (finding a financial interest where the defendant earned advertising revenue from ads marketed based on the popularity of infringing material on his sites, where approximately 90-96 percent (or perhaps slightly less) of the content on his sites was infringing and where the defendant actively induced infringement by users of his sites); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117-18 (9th Cir.) (finding that evidence that the service provider hosted, for a fee, websites that contained infringing material inadequate to establish the requisite financial benefit based on the literal language of the legislative history), *cert. denied*, 522 U.S. 1062 (2007); *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004) (quoting legislative history) (holding that “financial interest” under the DMCA should be found where “there is a causal relationship between the infringing activity and any financial benefit a defendant reaps . . . ;” affirming the finding that there was no financial interest based on inadequate proof that “customers either subscribed because of the available infringing material or cancelled subscriptions because it was no longer available.”); *see also Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1059 (9th Cir. 2017) (reversing and remanding the lower court’s entry of summary judgment for the service provider with directions to the fact finder to “determine whether LiveJournal financially benefitted from infringement that it had the right and ability to control” where LiveJournal derived revenue from advertising based on the number of page views received, and there was disputed evidence presented by the copyright owner that approximately 84% of posts on the relevant board contained infringing material).

activity.⁷ Although the Ninth Circuit initially held in 2011 that right and ability control presupposes knowledge or awareness of particular infringing activity,⁸ on reconsideration in 2013 it agreed with the Second Circuit that knowledge is irrelevant to right and ability to control; what must be shown in the Second and Ninth Circuits is “something more than the ability to remove or block access to materials posted on a service provider’s website.”⁹ As discussed below, the exact contours of this test remain to be fleshed out, but the standard set by these circuits is high and likely requires a showing that a service provider exerted substantial influence on the activities of users in ways that encourage infringement or involve purposeful conduct. According to the Ninth Circuit, right and ability to control should be assessed at the time of the alleged infringements.¹⁰

The Second and Ninth Circuit standard for what constitutes right and ability to control within the meaning of section 512(c)(1)(B) of the DMCA was derived from earlier, lower court opinions—largely from district courts in the

⁷See *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37–38 (2d Cir. 2012); *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026–31 (9th Cir. 2013). Vicarious liability is addressed in section 4.11[4].

⁸See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1041 (9th Cir. 2011) (holding that “until [a service provider] becomes aware of specific unauthorized material, it cannot exercise its ‘power or authority’ over the specific infringing item. In practical terms, it does not have the kind of ability to control infringing activity the statute contemplates.”), *opinion withdrawn and replaced*, 718 F.3d 1006 (9th Cir. 2013).

⁹*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012), quoting *Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1029–30 (9th Cir. 2013) (quoting *Viacom v. YouTube* and also explaining that “whereas the vicarious liability standard applied in *Napster* can be met by merely having the general ability to locate infringing material and terminate users’ access, § 512(c) requires ‘something more.’”); see also, e.g., *Kinsley v. Udemy, Inc.*, Case No. 19-cv-04334-JSC, 2021 WL 1222489, at *4 (N.D. Cal. Mar. 31, 2021) (granting summary judgment for Udemy on its DMCA defense, holding that the ability to remove material does not mean right and ability to control; “Udemy has over 50,000 courses on its marketplace, and its ability to remove infringing content once notified does not create the ‘right and ability to control’ that § 512 contemplates.”).

¹⁰*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1058 (9th Cir. 2017).

Ninth Circuit.

District courts had held that merely having the ability to disable access to or remove infringing material or discontinue service to an infringer,¹¹ enforcing policies that prohibit users from engaging in illegal or unauthorized conduct,¹² or providing vendors with transaction processing capabilities for credit card purchases¹³ did not evidence “the right and ability to control” infringing activity within the meaning of section 512(c)(1)(B).

The first appellate court to consider the scope of right and ability to control under the DMCA was the Fourth Circuit, in *CoStar Group Inc. v. LoopNet, Inc.*,¹⁴ in 2004. In explaining that the defense provided by section 512(c)(1)(B) is not coextensive with the standard for vicarious liability, the Fourth Circuit court wrote that a service provider “can become liable indirectly upon a showing of additional involvement sufficient to establish a contributory or vicarious violation of the Act. In that case, the ISP could still look to the DMCA for a safe harbor if it fulfilled the conditions therein.”¹⁵

In an earlier case, *Hendrickson v. eBay, Inc.*,¹⁶ a district court in California construed the “right and ability to control” language more narrowly than under the test for vicarious liability based on the language of the DMCA itself. The court

¹¹See, e.g., *Downs v. Oath Inc.*, 385 F. Supp. 3d 298, 308 (S.D.N.Y. 2019) (finding no right and ability to control); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1151 (N.D. Cal. 2008) (“the plain language of section 512(c) indicates that the pertinent inquiry is not whether Veoh has the right and ability to control its system, but rather, whether it has the right and ability to control the infringing activity.”); *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1098, (C.D. Cal. 2004), *aff’d in relevant part*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1109–10 (W.D. Wash. 2004); *CoStar Group Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 704 (D. Md. 2001), *aff’d*, 373 F.3d 544, 556 (4th Cir. 2004); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

¹²See *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

¹³See, e.g., *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1109–10 (W.D. Wash. 2004); *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 918 (C.D. Cal. 2003).

¹⁴*CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544 (4th Cir. 2004).

¹⁵*CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004).

¹⁶*Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

explained:

[T]he “right and ability to control” the infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or stored on its system. To hold otherwise would defeat the purpose of the DMCA and render the statute internally inconsistent. The DMCA specifically requires a service provider to remove or block access to materials posted on its system when it receives notice of claimed infringement. *See* 17 U.S.C.A. § 512(c)(1)(C). The DMCA also provides that the limitations on liability *only* apply to a service provider that has “adopted and reasonably implemented . . . a policy that provides for the termination in appropriate circumstances of [users] of the service provider’s system or network who are repeat infringers.” *See* 17 U.S.C.A. § 512(i)(1)(A). Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA.

The *Hendrickson v. eBay* court likewise rejected the suggestion that eBay’s voluntary practice of engaging in “limited monitoring” for apparent infringement under its VeRO¹⁷ program evidenced that it had the right and ability to control infringing conduct within the meaning of the DMCA. The court, citing legislative history, wrote that “Congress did not intend for companies such as eBay to be penalized when they engage in voluntary efforts to combat piracy over the Internet.”¹⁸

¹⁷Additional information on eBay’s Verified Rights Owner’s—or VeRO—program may be found in section 6.10[2][I] and in chapter 50.

¹⁸The court also concluded that that eBay did not have the right and ability to control the infringing activity at issue in the suit because the allegedly “infringing activity”—sales between third parties—occurred offline between eBay’s users. The court emphasized that:

[U]nlike a traditional auction house, eBay is not actively involved in the listing, bidding, sale and delivery of an item offered for sale on its website . . . eBay never has possession of, or opportunity to inspect, . . . items because . . . [they] are only in the possession of the seller When auctions end, eBay’s system automatically sends an email to the high bidder and the seller identifying each other as such After that, all arrangements to consummate the transaction are made directly between the buyer and seller eBay has no involvement in the final exchange and generally has no knowledge whether a sale is actually completed (i.e., whether payment exchanges hands and the goods are delivered) If an item is sold, it passes directly from the seller to the buyer without eBay’s involvement eBay makes money through the collection of an “insertion fee” for each listing and a “final value fee” based on a percentage of the highest bid amount at the end of the auction.

In *Hendrickson v. Amazon.com, Inc.*,¹⁹ Judge Hatter of the Central District of California ruled that Amazon.com's practice of providing payment processing services to third-party sellers on its site meant that Amazon.com received a financial benefit but did not give it "control over the sale" for purposes of the DMCA. As explained by the court (in describing a relationship between site owner and third-party seller that is common to many online businesses):

Amazon merely provided the forum for an independent third-party seller to list and sell his merchandise. Amazon was not actively involved in the listing, bidding, sale or delivery of the DVD. The fact that Amazon generated automatic email responses when the DVD was listed and again when it was sold, does not mean that Amazon was actively involved in the sale. Once a third-party seller decides to list an item, the responsibility is on the seller to consummate the sale. While Amazon does provide transaction processing for credit card purchases, that additional service does not give Amazon control over the sale.²⁰

Two district courts in California suggested in *dicta* that

¹⁹*Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914 (C.D. Cal. 2003).

²⁰*Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 918 (C.D. Cal. 2003). While *Hendrickson v. Amazon.com, Inc.* influenced the development of subsequent district court case law on right and ability to control, it was not cited in either the Second Circuit's opinion in *Viacom v. YouTube* or the Ninth Circuit's ruling in *UMG v. Shelter Capital Partners*.

Two other early district court opinions (both issued on the same day in the same case) were neither cited in *Viacom v. YouTube* or *UMG v. Shelter Capital Partners* nor particularly influential in the development of DMCA law. In *Tur v. YouTube, Inc.*, No. CV 064436 FMC AJWX, 2007 WL 4947612 (C.D. Cal. June 20, 2007), the court denied cross-motions for summary adjudication on the issue of YouTube's entitlement to the user storage safe harbor, in a suit brought by a videographer who alleged that unauthorized copies of his works had been posted to YouTube. Judge Cooper denied the plaintiff's motion, which had been based solely on the argument that YouTube earned revenue from banner advertisements, writing that "as the statute makes clear, a provider's receipt of a financial benefit is only implicated where the provider also 'has the right and ability to control the infringing activity.'" *Id.*, quoting 17 U.S.C.A. § 512(c)(1).

Similarly, in *Tur v. YouTube, Inc.*, No. CV 064436 FMC AJWX, 2007 WL 1893635 (C.D. Cal. June 20, 2007), *aff'd as moot*, 562 F.3d 1212 (9th Cir. 2009), the court denied YouTube's motion for summary judgment, concluding that it could not determine right and ability to control under the DMCA because insufficient evidence had been presented on "the process undertaken by YouTube from the time a user submits a video clip to the point of display on the YouTube website." In so ruling, the court cited both DMCA and vicarious liability cases for the proposition that "right and ability to control" under the DMCA "mean[s] 'something more' than

“right and ability to control” for user generated video sites “presupposes some antecedent ability to limit or filter copyrighted material.”²¹ Discussing earlier common law cases, the district court in *Io Group, Inc. v. Veoh Networks, Inc.*²² also suggested that “[t]urning a blind eye to detectable acts of infringement for the sake of profit” (as in *A&M Records, Inc. v. Napster, Inc.*)²³ or engaging in “a mutual enterprise of infringement” (like the proprietor and vendors at the swap meet at issue in *Fonovisa, Inc. v. Cherry Auction Inc.*)²⁴ would also likely qualify.²⁵

In *Io Group, Inc. v. Veoh Networks, Inc.*,²⁶ the court rejected the argument that Veoh had the right and ability to control because it had and enforced policies prohibiting users from (a) violating the intellectual property rights of others, (b) making unsolicited offers, sending ads, proposals or junk mail, (c) impersonating other people, (d) misrepresenting sources of material, (e) harassing, abusing, defaming, threatening or defrauding others, (f) linking to password protected areas and (g) spidering material.

just the ability of a service provider to remove or block access to materials posted on its website or stored in its system Rather, the requirement presupposes some antecedent ability to limit or filter copyrighted material.” The Ninth Circuit ultimately affirmed the denial of YouTube’s motion for summary adjudication as moot, based on the lower court’s subsequent order granting plaintiff’s voluntary dismissal to allow him to join a putative class action suit against YouTube pending in the Southern District of New York. *See Tur v. YouTube, Inc.*, 562 F.3d 1212 (9th Cir. 2009); *see also Tur v. YouTube, Inc.*, No. CV 064436 FMC AJWX, 2007 WL 4947615 (C.D. Cal. Oct. 19, 2007) (granting plaintiff’s motion for voluntary dismissal).

²¹*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1151 (N.D. Cal. 2008) (granting summary judgment for the defendant on this issue; quoting *Tur v. YouTube, Inc.*); *Tur v. YouTube, Inc.*, No. CV 064436, 2007 WL 1893635 (C.D. Cal. June 20, 2007) (*dicta* in an order denying YouTube’s motion for summary judgment), *aff’d as moot*, 562 F.3d 1212 (9th Cir. 2009).

²²*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

²³*A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001); *see generally supra* § 4.11[9][F].

²⁴*Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir. 1996); *see generally supra* §§ 4.11[4], 4.11[8][B], 4.11[8][C].

²⁵586 F. Supp. 2d at 1151–52 (citing other cases). Napster and other vicarious liability cases are analyzed extensively in section 4.11[4].

²⁶*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

The court in *Veoh* held that “the plain language of section 512(c) indicates that the pertinent inquiry is not whether Veoh had the right and ability to control its *system*, but rather, whether it has the right and ability to control the *infringing activity*. Under the facts and circumstances presented here, the two are not one and the same.”²⁷ As the court further explained, the statute presupposes a service provider’s control of its system or network.²⁸

The *Veoh* court rejected plaintiff’s argument that Veoh, a UGC video site, had the same right and ability to control as Napster because “Napster existed solely to provide the site and facilities for copyright infringement, and its control over its system was directly intertwined with its ability to control infringing activity.”²⁹ It also emphasized that “Veoh’s right and ability to control its system does not equate to the right and ability to control infringing activity.”³⁰ Judge Lloyd explained that, unlike Napster, there was no suggestion that Veoh sought to encourage infringement.³¹ He also cast “right and ability to control” squarely in the context of infringement, noting that even if Veoh had the ability to review and remove infringing material there was no evidence to suggest that Veoh could easily identify what material was infringing.³² Finally, the court rejected the argument that Veoh should have changed its business practices to have verified the source of all incoming videos by obtaining and confirming the names and addresses of the submitting user,

²⁷*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1151 (N.D. Cal. 2008) (emphasis in original).

²⁸*See* 17 U.S.C.A. § 512(c)(1) (applying the safe harbor to “material that resides on a system or network controlled or operated by or for the service provider”; emphasis added).

²⁹586 F. Supp. 2d at 1153.

³⁰586 F. Supp. 2d at 1153.

³¹*See supra* § 4.11[9][F] (analyzing the *Napster* case).

³²586 F. Supp. 2d at 1153. The court wrote that “Veoh’s ability to control its index does not equate to an ability to identify and terminate infringing videos.” 586 F. Supp. 2d at 1153 (emphasis in original). The court further stressed that there was no evidence presented to suggest that Veoh “failed to police its system to the fullest extent permitted by its architecture” and, to the contrary, the record showed that Veoh had “taken down blatantly infringing content, promptly respond[ed] to infringement notices, terminate[d] infringing content on its system and in its users’ hard drives (and prevents that same content from being uploaded again), and terminates the accounts of repeat offenders.” 586 F. Supp. 2d at 1153–54.

the producer and the user's authority to upload a given file. Judge Lloyd ruled that "[d]eclining to change business operations is not the same as declining to exercise a right and ability to control infringing activity."³³ In addition, he reiterated that "the DMCA does not require service providers to deal with infringers in a particular way."³⁴

In granting summary judgment for Veoh in *UMG Recordings, Inc. v. Veoh Networks, Inc.*,³⁵ Judge Howard Matz of the Central District of California addressed right and ability more pointedly in rejecting various arguments raised by UMG, writing that "the capacity to control and remove material are features that an internet service provider that stores content must have in order to be eligible for the safe harbor. 'Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA.'"³⁶

The Ninth Circuit forcefully amplified this theme in affirming the trial court's order in *UMG Recordings, Inc. v. Shelter Capital Partners LLC*.³⁷ In *Shelter Capital*, the appellate panel rejected UMG's argument that right and ability to control under the DMCA should be considered coextensive with the common law standard for imposing vicarious liability, which the court pointed out was phrased "loose[ly] and has varied" in different court opinions.³⁸ Judge Raymond C. Fisher, writing for himself and Judges Harry Pregerson and Marsha S. Berzon, explained that:

Given Congress' explicit intention to protect qualifying service

³³586 F. Supp. 2d at 1154.

³⁴586 F. Supp. 2d at 1154.

³⁵*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

³⁶*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1113 (C.D. Cal. 2009) (quoting *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1093–94 (C.D. Cal. 2001)), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026–31 (9th Cir. 2013). The court ruled that Veoh's ability to block and filter content did not amount to a right and ability to control.

³⁷*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1041–45 (9th Cir. 2011), *opinion withdrawn and replaced*, 718 F.3d 1006 (9th Cir. 2013).

³⁸*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026–30 (9th Cir. 2013).

providers who would otherwise be subject to vicarious liability, it would be puzzling for Congress to make § 512(c) entirely coextensive with the vicarious liability requirements, which would effectively exclude all vicarious liability claims from the § 512(c) safe harbor In addition, it is difficult to envision, from a policy perspective, why Congress would have chosen to exclude vicarious infringement from the safe harbors, but retain protection for contributory infringement. It is not apparent why the former might be seen as somehow worse than the latter.³⁹

The panel also noted that if that had been Congress's intention to exclude vicarious liability from the scope of DMCA safe harbor protection, "it would have been far simpler and much more straightforward to simply say as much."⁴⁰

Judge Fisher emphasized that section 512(c) "actually presumes that service providers have the sort of control that UMG argues satisfies the § 512(c)(1)(B) 'right and ability to control' requirement: they must 'remove[] or disable access to' infringing material when they become aware of it."⁴¹ He explained that right and ability to control could not mean, as it does under Ninth Circuit common law vicarious liability law, the ability to locate infringing material and terminate users' access, because "[u]nder that reading, service providers would have the 'right and ability to control' infringing activity regardless of their becoming 'aware of' the material."⁴² Quoting district court Judge Matz, the appellate panel explained that "Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in

³⁹*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1028–29 (9th Cir. 2013), citing Edward Lee, *Decoding the DMCA Safe Harbors*, 32 Colum. J.L. & Arts 233, 236–67 (2009) and Mark A. Lemley, *Rationalizing Internet Safe Harbors*, 6 J. Telecomm. & High Tech. L. 101, 104 (2007).

⁴⁰*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1029 (9th Cir. 2013), quoting *Ellison v. Robertson*, 189 F. Supp. 2d 1051, 1061 (C.D. Cal. 2002), *aff'd in part and rev'd in part on different grounds*, 357 F.3d 1072 (9th Cir. 2004).

⁴¹*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1027 (9th Cir. 2013), quoting 17 U.S.C. §§ 512(c)(1)(A)(iii), 512(c)(1)(C).

⁴²*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1027 (9th Cir. 2013).

acts that are specifically required by the DMCA.”⁴³

The Ninth Circuit initially had construed *right and ability to control* as requiring knowledge of specific files or activity, in a December 2011 opinion that subsequently was withdrawn and replaced in March 2013 following criticism from the Second Circuit and a motion for reconsideration. Initially, the Ninth Circuit panel had held that “the ‘right and ability to control’ under § 512(c) requires control over specific infringing activity the provider knows about. A service provider’s general right and ability to remove materials from its services is, alone, insufficient.”⁴⁴ Judge Fisher explained that:

[I]t is not enough for a service provider to know as a general matter that users are capable of posting unauthorized content; more specific knowledge is required. Similarly, a service provider may, as a general matter, have the legal right and necessary technology to remove infringing content, but until it becomes aware of specific unauthorized material, it cannot exercise its “power or authority” over the specific infringing item. In practical terms, it does not have the kind of ability to control infringing activity the statute contemplates.⁴⁵

In short, the appellate court explained that “the DMCA recognizes that service providers who are not able to locate and remove infringing materials they do not specifically know of should not suffer the loss of safe harbor protection.”⁴⁶ As discussed below, this aspect of the court’s ruling subsequently was withdrawn.

In *Viacom Int’l, Inc. v. YouTube, Inc.*,⁴⁷ the Second Circuit adopted a fact-based inquiry to right and ability to control,

⁴³*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1027 (9th Cir. 2013), quoting *UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1113 (C.D. Cal. 2009) (quoting *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1093–94 (C.D. Cal. 2001)) (internal quotation marks omitted) and citing *Io Grp., Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1151 (N.D. Cal. 2008) (same)).

⁴⁴*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1043 (9th Cir. 2011), *opinion withdrawn and replaced*, 718 F.3d 1006, 1026–30 (9th Cir. 2013).

⁴⁵*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1041 (9th Cir. 2011), *opinion withdrawn and replaced*, 718 F.3d 1006, 1026–30 (9th Cir. 2013).

⁴⁶*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1043 (9th Cir. 2011), *opinion withdrawn and replaced*, 718 F.3d 1006, 1026–30 (9th Cir. 2013).

⁴⁷*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38–40 (2d Cir. 2012).

declining to follow the Ninth Circuit's analysis in its 2011 opinion in *Shelter Partners*. Judge José Cabranes, writing for himself and Judge Livingston,⁴⁸ rejected the analysis of both the lower court and *Shelter Partners* that a service provider must know of a particular instance of infringement before it may control it because it would render the requirement that a service provider not have the right and ability to control duplicative of the provision requiring that a service provider not have knowledge of infringing activity and fail to act on that knowledge.⁴⁹ Judge Cabranes explained:

The trouble with this construction is that importing a specific knowledge requirement into § 512(c)(1)(B) renders the control provision duplicative of § 512(c)(1)(A). Any service provider that has item-specific knowledge of infringing activity and thereby obtains financial benefit would already be excluded from the safe harbor under § 512(c)(1)(A) for having specific knowledge of infringing material and failing to effect expeditious removal. No additional service provider would be excluded by § 512(c)(1)(B) that was not already excluded by § 512(c)(1)(A). Because statutory interpretations that render language superfluous are disfavored, . . . we reject the District Court's interpretation of the control provision.⁵⁰

On the other hand, the Second Circuit agreed with the Ninth Circuit in rejecting plaintiff's argument that the term "right and ability to control" codified the common law doctrine of vicarious liability because, to do so, would render the statute internally inconsistent by making the ability of a service provider to comply with the statute's requirement to disable access to or remove material in response to a DMCA notice, knowledge or awareness a disqualifying condition for the safe harbor.⁵¹

Instead, the Second Circuit held that "right and ability to

⁴⁸Judge Roger J. Miner, who had also been assigned to the panel, passed away prior to the resolution of the case. See *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 25 n.1 (2d Cir. 2012).

⁴⁹See *supra* § 4.12[6][C] (analyzing knowledge, awareness and the failure to take corrective measures).

⁵⁰*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 36 (2d Cir. 2012) (citation omitted).

⁵¹See *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37 (2d Cir. 2012). The panel acknowledged the "general rule with respect to common law codification . . . that when 'Congress uses terms that have accumulated settled meaning under the common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of those terms.'" *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37 (2d Cir. 2012), quoting *Neder v. United States*, 527 U.S. 1,

control” infringing activity within the meaning of section 512(c)(1)(B) “requires something more than the ability to remove or block access to materials posted on a service provider’s website.”⁵² The court conceded, however, that defining the “something more” that is required is a “more difficult . . . question”⁵³

In remanding the case back to the district court to evaluate whether YouTube had had the right and ability to control, the court provided little guidance beyond suggesting that right and ability to control in the context of section 512(c) may involve instances where service providers exert “substantial influence on the activities of users”⁵⁴

The court cited two cases, however, as potential examples to consider. Judge Cabranes noted that only one court previously had found that a service provider had the right and ability to control infringing activity under section

21 (1999). However, Judge Cabranes explained that since “[u]nder the common law vicarious liability standard, ‘[t]he ability to block infringer’ access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise’ . . . [t]o adopt that principle in the DMCA context . . . would render the statute internally inconsistent” because section 512(c) actually presumes that service providers have the ability to block access to infringing material. *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37 (2d Cir. 2012), quoting *Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 157 (S.D.N.Y. 2009) (quoting *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001)). If the right and ability to control provision were read to be coextensive with the common law standard for vicarious liability then “the prerequisite to safe harbor protection under § 512(c)(1)(A)(iii) & (C) would at the same time be a disqualifier under § 512(c)(1)(B).” *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37 (2d Cir. 2012). The panel noted that had Congress intended to carve out vicarious liability from the scope of the safe harbor “the statute could have accomplished that result in a more direct manner.” *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37 (2d Cir. 2012), quoting *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1045 (9th Cir. 2011), *opinion withdrawn and replaced*, 718 F.3d 1006, 1029 (9th Cir. 2013) (restating the same proposition).

⁵²*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012), quoting *Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011).

⁵³*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012).

⁵⁴*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012). As discussed later in this section, the district court, on remand, granted summary judgment for YouTube, holding that YouTube did not exert substantial influence over its users during the time period at issue in the lawsuit. See *Viacom Int’l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 117-22 (S.D.N.Y. 2013).

512(c)(1)(B). In that case, *Perfect 10, Inc. v. Cybernet Ventures, Inc.*,⁵⁵ Judge Cabranes explained that the court had found control “where the service provider instituted a monitoring program by which user websites received ‘detailed instructions regard[ing] issues of layout, appearance, and content’ and the service provider had forbidden ‘certain types of content and refused access to users who failed to comply with its instructions.’”⁵⁶ More specifically, in *Cybernet*, the defendant, an adult verification service, not only dictated detailed instructions on acceptable layout, appearance and content, but also refused to allow sites to use its verification services unless they complied with its dictates and it monitored those sites to ensure that celebrity images did not “oversaturate the content found within the sites that make up Adult Check.”⁵⁷

Judge Cabranes also suggested in *dicta* that copyright inducement under *MGM Studios, Inc. v. Grokster, Ltd.*,⁵⁸ where liability is premised on “‘purposeful, culpable expression and conduct,’ . . . might also rise to the level of control under § 512(c)(1)(B).”⁵⁹

Both of these opinions—one where a provider sought to affirmatively control content, the other where defendants were found liable for inducing infringement—involved cases, according to Judge Cabranes, of “a service provider exerting substantial influence on the activities of users, without necessarily—or even frequently—acquiring knowledge of specific infringing activity.”⁶⁰

Where inducement is shown, a service provider in any case likely would be ineligible for the DMCA safe harbor based on willful blindness amounting to red flag awareness.⁶¹

Viewed in context, substantial influence should be under-

⁵⁵*Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146 (C.D. Cal. 2002).

⁵⁶*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012), quoting *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1173 (C.D. Cal. 2002).

⁵⁷*Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1173 (C.D. Cal. 2002).

⁵⁸*MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005).

⁵⁹*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012), quoting *MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 937 (2005).

⁶⁰*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012).

⁶¹*See Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1043

stood to mean influence that encourages infringement given that the Second Circuit construed *right and ability to control* to not be coextensive with the common law standard for proving vicarious liability. Although the court's analysis of *Cybernet* could be read to suggest that service providers that proactively monitor their sites or services to deter infringement could lose DMCA protection for their efforts to deter infringement, this would seem to run counter to the purpose of the DMCA. The House Report accompanying the DMCA makes clear that the "legislation [wa]s not intended to discourage the service provider from monitoring its service for infringing material. Courts should not conclude that the service provider loses eligibility for limitations on liability . . . solely because it engaged in a monitoring program."⁶² Thus, the court's reference to the exertion of substantial influence should be understood to mean that a service provider could lose safe harbor protection for "exerting substantial influence on the activities of users"⁶³ in ways that encourage infringement.

This conclusion is buttressed by a review of district court cases (from the Second and Ninth Circuit) that the court cited approvingly in support of its holding that "something more" was required to show right and ability to control than merely the ability to remove or block access to infringing material.⁶⁴ The Second Circuit's holding on this point was quoted from Southern District of New York Judge William H. Pauley III's opinion in *Capitol Records, Inc. v. MP3Tunes*,

(9th Cir. 2013) (explaining that "inducing actions"—or measures deemed to induce copyright infringement—were relevant to the court's determination that the defendant had red flag awareness); *supra* § 4.12[6][C] (analyzing knowledge, awareness and the failure to take corrective measures).

⁶²H.R. Conf. Rep. No. 796, 105th Cong., 2d Sess. 73 (1998), reprinted in 1998 U.S.C.C.A.N. 639, 649.

⁶³*Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012).

⁶⁴*See Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012), citing *Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011); *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 757–58 (S.D.N.Y. 2012), *aff'd mem.*, 569 F. App'x 51 (2d Cir. 2014); *UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1114–15 (C.D. Cal. 2009), *aff'd sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1151 (N.D. Cal. 2008); and *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1110 (W.D. Wash. 2004).

LLC,⁶⁵ which in turn cited *Io Group, Inc. v. Veoh Networks, Inc.*⁶⁶ for the proposition that “the pertinent inquiry is not whether [the service provider] has the right and ability to control its system, but rather, whether it has the right and ability to control the *infringing activity*.”⁶⁷

In *Capitol Records, Inc. v. MP3Tunes, LLC*,⁶⁸ the court found that a service provider did not have the right and ability to control simply because it could monitor and remove infringing songs downloaded by users. Judge Pauley emphasized that MP3tunes users alone chose the websites they linked to using the defendant’s service and the songs they downloaded and stored in their lockers, without involvement by the service provider, MP3tunes. He explained that:

At worst, MP3tunes set up a fully automated system where users can choose to download infringing content. *Io Grp.*, 586 F. Supp. 2d at 1147 (granting safe harbor protection to a website that automatically created content from user submissions of unauthorized copyrighted work). If enabling a party to download infringing material was sufficient to create liability, then even search engines like Google or Yahoo! would be without DMCA protection. In that case, the DMCA’s purpose—innovation and growth of internet services—would be undermined. *See CoStar Grp.*, 164 F. Supp. 2d at 704, n.9 (if the “standard could be met merely by the ability to remove or block access to materials[, it] would render the DMCA internally inconsistent”). Accordingly, this Court finds that there is no genuine dispute that MP3tunes neither received a direct financial benefit nor controlled the infringing activity.⁶⁹

⁶⁵*Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011), *reconsideration granted on other grounds*, 2013 WL 1987225 (S.D.N.Y. May 14, 2013).

⁶⁶*Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

⁶⁷*Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011), *quoting Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1151 (N.D. Cal. 2008) (emphasis in original).

⁶⁸*Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627 (S.D.N.Y. 2011), *reconsideration granted in part*, 2013 WL 1987225 (S.D.N.Y. May 14, 2013).

⁶⁹*Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645–46 (S.D.N.Y. 2011). In ruling on defendants’ motion for reconsideration, Judge Pauley, in evaluating plaintiff’s claim for common law vicarious liability, emphasized that “the ‘direct financial benefit’ prong of the common law vicarious liability standard is construed more broadly than it is under the DMCA . . .” *Capitol Records, Inc. v. MP3Tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *10 (S.D.N.Y. May 14, 2013).

In *Wolk v. Kodak Imaging Network, Inc.*,⁷⁰ which also was cited with approval by the Second Circuit in *Viacom v. YouTube*, Southern District of New York Judge Robert W. Sweet held that Photobucket did not have the right and ability to control the infringing activity of its users. In support of his finding, Judge Sweet cited *Corbis Corp. v. Amazon.com, Inc.*⁷¹ (another case cited approvingly in *Viacom v. YouTube*) for the proposition that the right and ability to control infringing activity “must take the form of prescreening content, rendering extensive advice to users regarding content and editing user content.”⁷² He added, however, that “considering that millions of images are uploaded daily [to Photobucket], it is unlikely that this kind of prescreening is even feasible.”⁷³

Thus, while the Second Circuit test leaves for future courts to decide what conduct by a service provider in fact may amount to right and ability to control, rather than establishing a clearer, bright line test, the bar it sets is high and plainly should be focused on right and ability to control *infringing activity* as evidenced by a service provider’s “exerting substantial influence on the activities of users”⁷⁴

In response to the Second Circuit’s criticism, the Ninth Circuit, on motion for reconsideration, withdrew its opinion in *Shelter Partners* in March 2013 and replaced it with a new one that abandoned its conclusion that a service provider must have knowledge of infringing files or activity in order to have the right and ability to control.⁷⁵ Instead, the Ninth Circuit adopted the Second Circuit’s holding that

⁷⁰*Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724 (S.D.N.Y. 2012), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014).

⁷¹*Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

⁷²*Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 748 (S.D.N.Y. 2012) (*citing Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1110 (W.D. Wash. 2004)), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014).

⁷³*Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 748 (S.D.N.Y. 2012) (*citing Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1153 (N.D. Cal. 2008) (writing that where “hundreds of thousands of video files” had been uploaded to a website, “no reasonable juror could conclude that a comprehensive review of every file would be feasible.”)), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014).

⁷⁴*Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012).

⁷⁵*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026–31 (9th Cir. 2013).

right and ability to control may be shown by “something more” than the ability to remove or block access to materials posted on a service provider’s website,⁷⁶ thus eliminating a potential circuit split that could have justified U.S. Supreme Court review. That “something more” is understood in the Second and Ninth Circuits to involve exerting “substantial influence” on the activities of users, which may include high levels of control over user activities or purposeful conduct.⁷⁷

In *Shelter Partners*, the lower court had found that the allegedly infringing material resided on Veoh’s system, Veoh had the ability to remove the material, Veoh could have searched for potentially infringing content and Veoh could have implemented and did implement filtering to deter infringing user uploads. The Ninth Circuit panel concluded that this was not enough to show right and ability to control under the DMCA, writing that “Veoh’s interactions with and conduct towards its users” did not rise to the level of substantial influence based on high levels of control over user activities, as in *Cybernet*, or purposeful conduct, as in *Grokster*.⁷⁸ Accordingly, the panel again affirmed the entry of summary judgment for Veoh, albeit under a different standard for evaluating right and ability to control.

Likewise, on remand, in *Viacom v. YouTube*, the district court again granted summary judgment for YouTube, finding that YouTube did not exert substantial influence over the activities of its users during the time preceding its acquisition by Google.⁷⁹ Summarizing case law, the district court emphasized that “knowledge of the prevalence of infringing activity, and welcoming it, does not itself forfeit the safe harbor. To forfeit that, the provider must influence

⁷⁶See *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012), quoting *Capitol Records, Inc. v. MP3Tunes, LLC*, 821 F. Supp. 2d 627, 645 (S.D.N.Y. 2011); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1029–30 (9th Cir. 2013).

⁷⁷See *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013). Although the Ninth Circuit referenced personal conduct, it might have been more appropriate to articulate the standard in terms of personal misconduct.

⁷⁸*UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030–31 (9th Cir. 2013).

⁷⁹*Viacom Int’l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 117–22 (S.D.N.Y. 2013). Viacom did not challenge YouTube’s conduct subsequent to its acquisition by Google.

or participate in the infringement.”⁸⁰

On remand, Viacom had argued that the “something more” was shown by YouTube’s editorial decisions to remove some but not all infringing material, by its efforts to facilitate video searches on its site but restrict access to certain proprietary search tools and by enforcement of rules prohibiting pornographic content. Judge Stanton, however, concluded that these decisions merely placed much of the burden on Viacom and other copyright owners to search YouTube for infringing clips, which “is where it lies under the safe harbor”⁸¹ The court likewise found that YouTube’s decisions to restrict its monitoring efforts to certain groups of infringing clips and to restrict access to its proprietary search mechanisms did “not exclude it from the safe harbor, regardless of their motivation.”⁸² Moreover, the only evidence that YouTube may have steered viewers toward infringing videos involved a show, “Lil Bush,” whose creators themselves had made the clip available on YouTube. In summary, the court explained that:

[D]uring the period relevant to this litigation, the record establishes that YouTube influenced its users by exercising its right not to monitor its service for infringements, by enforcing basic rules regarding content (such as limitations on violent, sexual or hate material), by facilitating access to all user-stored material regardless (and without actual or constructive knowledge) of whether it was infringing, and by monitoring its site for some infringing material and assisting some content owners in their efforts to do the same. There is no evidence that YouTube induced its users to submit infringing videos, provided users with detailed instructions about what content to upload or edited their content, prescreened submissions for quality, steered users to infringing videos, or otherwise interacted with infringing users to a point where it might be said to have participated in their infringing activity.⁸³

In *Capitol Records, LLC v. Vimeo, LLC*,⁸⁴ the district court similarly found that a service provider did not have the right

⁸⁰*Viacom Int’l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 118 (S.D.N.Y. 2013).

⁸¹*Viacom Int’l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 120 (S.D.N.Y. 2013).

⁸²*Viacom Int’l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 120 (S.D.N.Y. 2013).

⁸³*Viacom Int’l, Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 121 (S.D.N.Y. 2013).

⁸⁴*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 526-27

and ability to control within the meaning of the DMCA where it did not exert substantial influence on user activity or substantial influence through inducement of infringement.⁸⁵ In *Vimeo*, evidence was presented that Vimeo used a form of monitoring program—which the court characterized as consisting “of the Community Team’s removal of certain content from the Website with the assistance of Moderator Tools, its discretion to manipulate video visibility and its intermittent communication with users—[which] lacks the ‘something more’ that *Viacom* demands.”⁸⁶ The *Vimeo* court contrasted these features with *Cybernet*, where the service provider dictated the “layout, appearance, and content” of participating sites and refused “to allow sites to use its system until they compl[ie]d with [those] dictates.”⁸⁷ Vimeo, the court emphasized, left editorial decisions to its users and used monitoring to filter out content that was not original to users.⁸⁸

The district court in *Vimeo* likewise found unpersuasive the argument that because Vimeo employees had discretion over how they interacted with content on the site they exerted substantial influence over user activity, writing that “it is difficult to imagine how Vimeo’s staff of seventy-four (as of 2012) could, through its discretionary and sporadic interactions with videos on the Website, exert substantial influence on approximately 12.3 million registered users uploading 43,000 new videos each day.”⁸⁹ Among other things, the court noted that the “likes” of current Vimeo employees constituted approximately 0.2% of all “likes” on the website and the comments left by current Vimeo employees

(S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁸⁵*Vimeo* was appealed to the Second Circuit but the appellate court addressed just three issues (ruling in Vimeo’s favor on all three): (1) the applicability of the DMCA to pre-1972 sound recordings; (2) red flag awareness; and (3) willful blindness.

⁸⁶*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 529 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁸⁷*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 529 (S.D.N.Y. 2013), (quoting *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1173 (C.D. Cal. 2002)), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁸⁸*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 529 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁸⁹*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 530 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

constituted 1.6% of all comments.⁹⁰ The court also noted that the Staff Picks channel, which contained videos selected by Vimeo employees, represented only one of approximately 354,000 channels on the website as of November 2012.⁹¹

The district court had further rejected evidence that some employees responded to user questions by ignoring or turning a blind eye to infringement, as evidencing a right and ability to control. Judge Abrams wrote that he was “troubled” by these communications, but characterized them as “scattered examples” that did “not demonstrate a substantial influence over users’ activities.”⁹² The Second Circuit agreed. Judge Leval, writing for himself and Judges Hall and Lynch, explained that:

The evidence cited to us by Plaintiffs, consisting of a handful of sporadic instances (amongst the millions of posted videos) in which Vimeo employees inappropriately encouraged users to post videos that infringed music cannot support a finding of the sort of generalized encouragement of infringement supposed by their legal theory. It therefore cannot suffice to justify stripping Vimeo completely of the protection of § 512(m). Moreover, because that evidence was not shown to relate to any of the videos at issue in this suit, it is insufficient to justify a finding of red flag knowledge, under the principle of *Viacom*, as to those specific videos. Thus, notwithstanding a few unrelated instances in which its employees improperly encouraged specific infringements, Vimeo can still assert the protection of § 512(m) for the present suit, and claim the benefit of the safe harbor, in the absence of a showing by Plaintiffs of facts sufficient to demonstrate that Vimeo, having actual or red flag knowledge of infringement in the videos that are the subject of Plaintiffs’ suit, failed to promptly take them down.⁹³

In so ruling, the Second Circuit considered willful blindness in the context of knowledge or awareness, not specifically right or ability to control.

In *Vimeo*, plaintiffs had argued to the district court that Vimeo induced infringement “by example” by making videos that incorporated infringing content. Specifically, the plaintiffs pointed to: (1) ten of the videos at issue that had

⁹⁰*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 530 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁹¹*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 530 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁹²*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 530 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁹³*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 99 (2d Cir. 2016).

been uploaded by Vimeo employees; (2) other videos not at issue in the suit which had also been uploaded by employees and included unauthorized music; (3) one video containing unauthorized music that had been created by the “Vimeo Street Team” (a group of employees who created videos and engaged with the Vimeo community; (4) videos created as part of a project to accompany every song on a Beatles album, which included contributions from Vimeo employees (in some cases prior to their being hired by Vimeo); (5) a Vimeo tutorial video made available via link from a page containing a video that incorporated the Beatles’ copyrighted sound recording “Helter Skelter”; and (6) “lip dub” videos featuring Vimeo’s co-founder and other employees lip-syncing to commercial sound recordings.⁹⁴ The district court explained that this evidence “simply does not rise to the level of that adduced in *Grokster*—either in quantity or in kind.⁹⁵ The court acknowledged that some of the videos created by Vimeo employees such as the co-founder’s lip dub “incorporated infringing music, and users’ submissions may have often incorporated the same. But the relevant standard at issue here—inducement by way of the exertion of substantial influence on the activities of users—cannot be met by evidence of stray instances of wrongful conduct by Vimeo employees . . . and/or a generalized effort to promote videos that incorporate music.”⁹⁶

The court similarly rejected the argument that Vimeo employee communications with, and provision of technical assistance to, Vimeo users, constituted inducement. While the court conceded that instructing users how to engage in an infringing use could amount to the kind of active step taken to encourage direct infringement that was found actionable in *Grokster*, it characterized the emails identified by plaintiffs as merely “[o]ffering technical support as to the ordinary use of a service” which the court explained is not inducement.⁹⁷ Similarly, it wrote that “a handful of . . . examples of Vimeo employees responding to user requests

⁹⁴*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 531-32 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁹⁵*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 532 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁹⁶*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 533 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁹⁷*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 534 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

about copyrighted music with statements that indicate tacit, or at times explicit, acceptance of infringing uploads” that “may have induced a particular user to infringe” did not rise to the level of inducement by way of exertion of substantial influence on users’ activities.⁹⁸ That standard, the court wrote, “is not met by the limited anecdotal evidence Plaintiffs have provided. To establish the right and ability to control, there must be a showing that the service provider’s substantial influence over users’ activities was significantly more widespread and comprehensive.”⁹⁹

The court likewise rejected the argument that structural aspects of the website, such as its privacy settings, evidenced inducement, where there was nothing in the record to suggest these features were implemented to enable users to upload infringing material and then restrict copyright holders’ access to it.¹⁰⁰

Judge Abrams similarly found unpersuasive the argument that Vimeo’s failure to implement filtering technologies that could be used to locate infringing content amounted to inducement, writing that “just because Vimeo can exercise control does not mean that it must. A holding to the contrary would conflict with the express language of § 512(m), which makes clear that service providers may not lose safe harbor protection for failure to monitor or affirmatively seek out infringement.”¹⁰¹

The court further rejected evidence of internal discussions about the lawsuit or the allegation that Vimeo sought to promote its site’s permissive policy towards infringement of music, which was based largely on the fact that Vimeo, unlike other sites, had not implemented filtering technology.¹⁰²

In *Rosen v. eBay, Inc.*,¹⁰³ Judge Michael Fitzgerald of the Central District of California rejected the plaintiff’s argu-

⁹⁸*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 534 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁹⁹*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 534 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

¹⁰⁰*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 534 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

¹⁰¹*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 534 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

¹⁰²*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 534-35 (S.D.N.Y. 2013), *aff’d in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

¹⁰³*Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081

ment that eBay had the right and ability to control within the meaning of the DMCA because it required users to post pictures of items offered for sale on eBay and required that pictures conform to set size and quality requirements.¹⁰⁴ In so ruling, the court emphasized that “eBay does not direct users what to list, does not come into contact with the items being posted, and beyond the basic content requirements, including the photograph requirement, has no control over what its users list until the listing is complete.”¹⁰⁵

In contrast to the legitimate service providers at issue in *Viacom v. YouTube*, *Shelter Partners* and similar cases, the Ninth Circuit panel in *Columbia Pictures Industries, Inc. v. Fung*,¹⁰⁶ an inducement case, had little difficulty finding that the defendants, the operators of various BitTorrent tracker sites who the court found liable for inducement, were ineligible for the user storage safe harbor because they had the right and ability to control infringing activity. Applying the test adopted in *Viacom v. YouTube* and in the Ninth Circuit in *Shelter Partners*, the panel explained that while Fung’s inducement activities did not “*categorically* remove him from protection under § 512(c), they demonstrate[d] the substantial influence Fung exerted over his users’ infringing activities”¹⁰⁷ In *Fung*, the panel held that where a service provider fails to satisfy the right and ability to control/financial benefit prong set forth in section 512(c)(1)(B), “the

(C.D. Cal. Jan. 16, 2015).

¹⁰⁴*See Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *13 (C.D. Cal. Jan. 16, 2015).

¹⁰⁵*Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *13 (C.D. Cal. Jan. 16, 2015).

¹⁰⁶*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020 (9th Cir. 2013).

¹⁰⁷*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1046 (9th Cir. 2013). The panel explained:

Fung unquestionably had the ability to locate infringing material and terminate users’ access. In addition to being able to locate material identified in valid DMCA notices, Fung organized torrent files on his sites using a program that matches file names and content with specific search terms describing material likely to be infringing, such as “screener” or “PPV.” And when users could not find certain material likely to be infringing on his sites, Fung personally assisted them in locating the files. Fung also personally removed “fake[], infected, or otherwise bad or abusive torrents” in order to “protect[] the integrity of [his websites’] search index[es].” Crucially, Fung’s ability to control infringing activity on his websites went well beyond merely locating and terminating users’ access to infringing material. As noted, there is overwhelming evidence that Fung engaged in culpable, inducing activity like that in *Grokster*

service provider loses protection with regard to any infringing activity using the service.”¹⁰⁸

In *Mavrix Photographs, LLC v. LiveJournal, Inc.*,¹⁰⁹ a later Ninth Circuit opinion, a three judge panel, in remanding the case for further consideration, identified efforts undertaken by a service provider to *deter* infringement as potential evidence of right and ability to control under the DMCA.¹¹⁰ The court’s cursory treatment of right and ability to control merely identified certain features of the service without considering that these factors actually deter, rather than encourage infringement (although that issue presumably could be raised on remand). In all likelihood, the high percentage of rejected uploads, and the plaintiff’s disputed assertion that 84% of posts on the relevant board contained infringing material, colored the panel’s perceptions in that case.

By contrast, in *Ventura Content, Ltd. v. Motherless, Inc.*,¹¹¹ which was decided after *Mavrix* and cites to that opinion, the Ninth Circuit held that a user generated photo and video porn site did not have the right and ability to control, within the meaning of the DMCA, merely because it screened

Id. For convenience, the Ninth Circuit referred to the defendants collectively as “Fung.”

¹⁰⁸*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1046 (9th Cir. 2013). The panel explained that “[t]he term ‘right and ability to control such activity’ so reflects, as it emphasizes a general, structural relationship and speaks of ‘such activity,’ not any particular activity.” *Id.*

¹⁰⁹*Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1058-59 (9th Cir. 2017).

¹¹⁰In reversing the district court’s entry of summary judgment for the service provider, the panel, in discussing right and ability to control, explained that:

LiveJournal’s rules instruct users on the substance and infringement of their posts. The moderators screen for content and other guidelines such as infringement. Nearly two-thirds of submitted posts are rejected, including on substantive grounds. ONTD maintains a list of sources that have complained about infringement from which users should not submit posts. LiveJournal went so far as to use a tool to automatically block any posts from one source. In determining whether LiveJournal had the right and ability to control infringements, the fact finder must assess whether LiveJournal’s extensive review process, infringement list, and blocker tool constituted high levels of control to show “something more.”

Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1059 (9th Cir. 2017).

¹¹¹*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597 (9th Cir. 2018).

uploads, and deleted videos that contained child pornography or bestiality or which appeared to infringe on third party copyrights.¹¹² In that case, eight users had uploaded 33 allegedly infringing clips. The court conceded that the defendant “certainly had the physical ability to control any and all infringing activity[,]” but merely by monitoring to remove illegal material it did not have the ability “to exert ‘substantial influence’ on its users’ activities.”¹¹³ The court distinguished *Fung* – finding the facts in *Motherless* closer to *UMG* – and rejected the notion that because Motherless rewarded uploaders of the most popular content with points “redeemable for items of negligible value, such as coffee mugs and t-shirts . . .” or nominal cash payments, it had the right and ability to control; writing that this activity “did not amount to encouragement of infringing material.”¹¹⁴

In *Greg Young Publishing, Inc. v. Zazzle, Inc.*,¹¹⁵ a district

¹¹²See *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 612-13 (9th Cir. 2018).

¹¹³See *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 613 (9th Cir. 2018) (quoting *UMG and Viacom v. YouTube*).

¹¹⁴See *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 613 (9th Cir. 2018). Among other things, users forfeited their credits if they uploaded any material that violated the site’s Terms of Use (ToU). Each time a user uploaded a video, he or she received a warning that “Anyone uploading illegal images/videos will be reported to the authorities. Your IP address . . . has been recorded.” *Id.* at 600-01. Motherless did not edit, review, or approve file names, titles, or tags added by users. The ToU, among other things, prohibited posting copyrighted material without the prior written consent of the copyright owner and invited takedown notices from copyright owners. In addition to responding to takedown notices, Motherless also allowed copyright owners to access a software program that allowed them to directly remove material that they believed to be infringing. The site used software that generated thumbnail images of each picture and five images from each video clip (captured at the 20, 40, 60, 80 and 100% time points in the clip). It also maintained links to certain classes of content, such as “Most Popular” and “Most Viewed.” Lange, the site owner, and a contractor he employed, reviewed each thumbnail for “obvious signs of child pornography, copyright notices, watermarks, and any other information that would indicate” illegal content or a ToU violation. He also deleted all files identified in copyright notices, whether DMCA-compliant or not. Motherless also used software to prevent users from re-uploading previously deleted material. Since 2008, Motherless had deleted over 4.5 million pictures and videos for ToU violations, approximately 4-6% of which were for copyright infringement. Motherless also implemented a repeat infringer policy. *See id.* at 601.

¹¹⁵*Greg Young Publishing, Inc. v. Zazzle, Inc.*, Case No. 2:16-CV-05487, 2017 WL 2729584, at *8 (C.D. Cal. May 1, 2017).

court held that Zazzle, a site that allowed users to upload images which other users could then imprint on products that Zazzle manufactured and sold, was entitled to DMCA protection for images uploaded to its website but not to the extent it manufactured and sold products bearing those images. Zazzle had argued that it lacked the ability to control the sale of allegedly infringing images because the production process was automated, with printing and product fulfillment occurring automatically after its content management team approved an order. Central District of California Judge Wilson, however, concluded that “even if the entire process were automatic, that would suggest at most that Zazzle had chosen not to exercise its right and ability to reject infringing products, not that it *lacked* the right or ability to do so.”¹¹⁶ This analysis, however, places undue emphasis on what in the modern digital economy are merely

¹¹⁶*Greg Young Publishing, Inc. v. Zazzle, Inc.*, Case No. 2:16-CV-05487, 2017 WL 2729584, at *8 (C.D. Cal. May 1, 2017); see also *Sid Avery and Associates, Inc. v. Pixels.com, LLC*, 479 F. Supp. 3d 859, 869 (C.D. Cal. 2020) (following *Zazzle* in holding that fact issues precluded summary judgment on Pixels’ DMCA defense where “unlike eBay and Amazon, Pixels[, a print-on-demand service,] may have an active role in designing, listing, selling, manufacturing, and delivering products. . . . Pixels’ ‘fulfillment centers’ apparently manufacture and ship products at Pixels’ direction and based on Pixels’ specifications. . . . Pixels and its vendors use contributors’ images to create products that are sold to consumers—transferring them from photographs to phone cases. In so doing, they may exercise control over user-generated content.”). A similar approach was taken in *H-D U.S.A., LLC v. SunFrog, LLC*, 282 F. Supp. 3d 1055 (E.D. Wis. 2017), in denying a motion to dismiss, where the court held that SunFrog, a print-on-demand business that allowed users to upload images that could be printed on blank t-shirts for purchase, was not entitled to the user storage safe harbor because, as alleged in plaintiff’s complaint, “SunFrog actually knows that its users create and that it prints and sells infringing material,” and “continues to permit this to occur because it is profitable.” *Id.* at 161-62. The district court concluded that SunFrog had the ability to control the infringing activity of its users because, even though “SunFrog might complain that it lacks the practical means to monitor all design creation and printing for infringement, it built and operates both the platform and the production line in which infringement occurs.” *Id.* at 1062. Contrasting it to eBay (in *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1094 (C.D. Cal. 2001)), which “had no involvement in consummating the transaction involving the infringing goods, other than providing a platform for the buyer and seller to interact,” the court ruled that “SunFrog’s business model is quite unlike eBay’s: SunFrog promotes infringing designs created by its users, it has possession of and an opportunity to inspect the goods it prints before shipment, and it knows that purchases of infringing goods are consummated because it actually prints and ships the goods to the buyer. In contrast to eBay, SunFrog is

backend services. An image on a website may be downloaded and printed by a user without jeopardizing a service provider's entitlement to DMCA safe harbor protection. Merely allowing images to be automatically printed on paper, or, as in *Zazzle*, on t-shirts or other blank products, does not mean a site has the ability to control third party infringement (or even necessarily know which images are infringing)—especially when the printing process is automated. Indeed, in *UMG Recordings, Inc. v. Shelter Capital Partners LLC*,¹¹⁷ the Ninth Circuit found a website that allowed users

intimately—indeed indispensably—involved in transactions involving infringing goods. Regardless of the ease of doing so, then, SunFrog has ‘some ability to limit or filter copyrighted material.’” 282 F. Supp. 3d at 1062, citing *MGM, Inc. v. Grokster*, 545 U.S. 91, 926 (2005).

Grokster, however, was a copyright inducement case, not a case construing the DMCA, and both the statute and case law are clear that a service provider need not proactively search for potentially infringing material to be entitled to DMCA safe harbor protection. See, e.g., *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 94, 98 (2d Cir. 2016) (“§ 512(m) makes clear that the service provider’s personnel are under no duty to ‘affirmatively seek[]’ indications of infringement.”; “§ 512(m) relieves the service provider of obligation to monitor for infringements posted by users on its website.”); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) (“Section 512(m) is explicit: DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider. For that reason, § 512(m) is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that infringement may be occurring.”); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 603 (9th Cir. 2018) (“The Digital Millennium Copyright Act places the burden of policing infringement on the copyright owner, not on the person or firm storing and hosting the material.”); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1022 (9th Cir. 2013) (holding that the burden of policing for infringement is on the copyright owner; “Copyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers like Veoh, who cannot readily ascertain what material is copyrighted and what is not.”).

Further, DMCA case law is clear that “right and ability to control” means the ability to exert “substantial influence” on users’ activities, not the ability to remove or block access. E.g., *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 603 (9th Cir. 2018). The court in *SunFrog* simply applied the wrong legal standard.

SunFrog also underscores that it may be difficult to successfully assert the DMCA safe harbor—which is an affirmative defense—on a motion to dismiss. See *H-D U.S.A., LLC v. SunFrog, LLC*, 282 F. Supp. 3d 1055, 1061 (E.D. Wis. 2017) (noting that, in general, a plaintiff need not anticipate defenses to state a claim for infringement).

¹¹⁷See *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d

to view *and download* music videos was entitled to safe harbor protection. While companies that operate in the physical world may not claim benefit from the DMCA for material provided to them by users, service providers that otherwise are entitled to safe harbor protection should not be found to have the right and ability to control, and thus lose that protection, merely because they provide back end printing, production or shipping services. There is no functional difference between allowing a user to print an image on an attached printer, or a t-shirt or mug, or to download a video, as with the Veoh user generated video system at issue in *Shelter Partners*.

Something more under the Second and Ninth Circuit tests for the right and ability to control prong of the test for DMCA eligibility requires an effort to exert “substantial influence” to induce infringement, or exercise “high levels of control over the activities of users,”¹¹⁸ not merely the provision of backend services.

While human review theoretically could expose a service provider to losing DMCA protection in some cases if it were found to have actual knowledge or red flag awareness, quality control review for print jobs (which typically look at size, spacing, centering, color and the like) should not take a company outside the safe harbor for *right and ability to control*.

A broad construction of what constitutes right and ability to control also is inconsistent with the “but for” test applied to determine DMCA eligibility.¹¹⁹

Neither the Second Circuit in *Viacom v. YouTube* nor the

1006, 1015–20 (9th Cir. 2013).

¹¹⁸*E.g.*, *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 38 (2d Cir. 2012); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 603 (9th Cir. 2018); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013); *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1151 (N.D. Cal. 2008) (“the plain language of section 512(c) indicates that the pertinent inquiry is not whether Veoh has the right and ability to control its *system*, but rather, whether it has the right and ability to control the *infringing activity*” (emphasis in original)); *id.* at 1153 (concluding that “Veoh’s ability to control its index does not equate to an ability to identify and terminate infringing videos”).

¹¹⁹*See UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1018–20 (9th Cir. 2013) (rejecting arguments to read section 512(c) narrowly and explaining that the statute is to be construed broadly to protect more than simply web hosting services, and analogizing the “by reason of” language to require only “but for” rather than proximate

Ninth Circuit in *UMG v. Shelter Capital Partners* addressed the financial interest prong of section 512(c)(1) and whether it should likewise be construed as imposing a tougher standard for proving vicarious liability.

Without addressing that specific question, the Ninth Circuit in 2018, in *Ventura Content, Ltd. v. Motherless, Inc.*,¹²⁰ held that the operator of a site that hosted user-submitted porn videos and photos did not have a financial benefit directly attributable to the infringing activity even though it had an incentive program that gave users points (which could be exchanged for items such as t-shirts or mugs or at the rate of five cents per point cash) to upload videos and earned revenue from advertising, where there was no evidence that the service provider “made any money directly” from the video clips at issue in that case. In that case, the appellate panel emphasized—in a short, one paragraph discussion—that, unlike in *Fung*, Motherless did not advertise itself as a place to get pirated materials. Thus, while the court conceded that “the more pornography Motherless had, the more users it would attract, and more views would lead to more advertising revenue[,]” it found that this alone did not evidence a financial interest in infringement. The panel explained that “[t]he words ‘the’ and ‘directly’ in the statute . . . must mean that some revenue has to be distinctly attributable to the infringing material at issue.”¹²¹ Because there was no evidence that Motherless made any money directly from the Ventura clips, the court found no financial interest.

Similarly, in *Downs v. Oath Inc.*,¹²² Judge Rakoff of the Southern District of New York, in granting summary judgment for the service provider on its entitlement to the DMCA safe harbor, rejected the argument that Oath had a financial interest in infringement because it accepted advertising for user generated content hosted on its site.¹²³

In *Perfect 10, Inc. v. CCBill LLC*, an earlier Ninth Circuit

causation).

¹²⁰*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 613 (9th Cir. 2018).

¹²¹*Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 613 (9th Cir. 2018).

¹²²*Downs v. Oath Inc.*, 385 F. Supp. 3d 298, 307 (S.D.N.Y. 2019).

¹²³*Downs v. Oath Inc.*, 385 F. Supp. 3d 298, 307 (S.D.N.Y. 2019). He explained:

panel had held that the financial interest prong should be construed coextensively with the common law standard, rather than more narrowly.¹²⁴ Some courts and commentators previously had concluded that section 512(c)(1)(B) merely codified the elements of a claim for vicarious liability as part of the user storage limitation, meaning that the DMCA safe harbor for user storage would not apply to claims of vicarious infringement.¹²⁵

Downs has made no showing that the advertising revenue HuffPost received was “distinctly attributable” to infringing activity. There is no evidence that HuffPost encouraged infringement, or that it promoted advertising by pointing to infringement, or even that its users primarily engaged in infringing conduct. To the contrary, the undisputed evidence shows that HuffPost simply ran advertisements on user-generated articles, some of which inevitably contained infringing material.

Id.

¹²⁴*See Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117 (9th Cir.) (“Based on the ‘well-established rule of construction that where Congress uses terms that have accumulated settled meaning under common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of those terms,’” . . . we hold that ‘direct financial benefit’ should be interpreted consistent with the similarly worded common law standard for vicarious liability.”; citations omitted), *cert. denied*, 522 U.S. 1062 (2007).

In *UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. 2009), *aff’d sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013), the district court held that the phrase *direct financial benefit* should be construed consistently with the common law standard, but *right and ability to control* should be construed more narrowly to avoid a “catch 22” whereby the only entities that would benefit from the DMCA would be sites that host user content, which by definition could be deemed ineligible under the common law standard for right and ability to control. On appeal, the Ninth Circuit agreed that the right and ability to control under the DMCA requires a higher showing than what is required to establish common law vicarious liability but did not address how to construe *direct financial benefit*. *See* 718 F.3d at 1026 n.16.

¹²⁵*See CoStar Group Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 704 (D. Md. 2001) (citing 3 Melville B. Nimmer and David Nimmer, Nimmer on Copyright § 12B.04[A][2], at 12B-38 (2001)), *aff’d on other grounds*, 373 F.3d 544 (4th Cir. 2004); *Ellison v. Robertson*, 189 F. Supp. 2d 1051, 1061 (C.D. Cal. 2002), *rev’d in relevant part on other grounds*, 357 F.3d 1072 (9th Cir. 2004). In *Ellison*, the district court explained:

The DMCA did not simply rewrite copyright law for the online world. Rather it crafted a number of safe harbors which insulate ISPs from most liability should they be accused of violation traditional copyright law [W]hen Congress chooses to utilize exact phrases that have a specialized legal meaning under copyright law (i.e., “the right and ability to control infringing activity”), and gives those phrases a certain meaning in one context (i.e., under the DMCA, the ability to delete or block access to infringing materials after the infringe-

A coextensive reading of right and ability to control, which has now been clearly rejected by the Second, Fourth and Ninth Circuits,¹²⁶ would have rendered superfluous the requirements that a service provider disable access to or remove material where it has red flag awareness¹²⁷ or reasonably implement a repeat infringer policy¹²⁸ in vicarious infringement cases, since service providers are not otherwise required to do either of these things to avoid common law vicarious liability.¹²⁹ Presumably, Congress would not have imposed additional requirements on service providers to qualify for a safe harbor if the safe harbor provided no further protection than what existed under common law standards.

Construing the DMCA as merely codifying the common law standard for vicarious liability also would appear to conflict with the explanation in the legislative history that “the limitations of liability apply *if* the provider is found to be liable under existing principles of law.”¹³⁰ Congress intended to create a safe harbor applicable *if* liability otherwise would be imposed, and gave service providers an incentive to comply with provisions governing notifications, red flag awareness and adoption and reasonable implementation of a repeat infringer policy that otherwise were not expressly required to avoid liability for secondary copyright infringement.

A narrow reading of the element of “control” is also suggested by reference in the legislative history on content monitoring. The House Report states that the Act was “not intended to discourage the service provider from monitoring

ment has occurred is not enough to constitute “the right and ability to control”), Congress’s choice provides at least persuasive support in favor of giving that phrase a similar meaning when used elsewhere in copyright law.

189 F. Supp. 2d at 1061 (footnotes omitted).

¹²⁶See *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37–38 (2d Cir. 2012); *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 555 (4th Cir. 2004); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026–31 (9th Cir. 2013); *supra* § 4.12[6][D].

¹²⁷17 U.S.C.A. § 512(c)(1)(A); see generally *supra* § 4.12[6][C].

¹²⁸17 U.S.C.A. § 512(i); see generally *supra* § 4.12[3][B].

¹²⁹See *supra* § 4.11[4].

¹³⁰H. Rep. No. 105-796, 105th Cong. 2d Sess. 1, 73 (1998) (emphasis added).

its service for infringing material.”¹³¹ It further directs that “[c]ourts should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program.”¹³² Thus, it may be inferred that a service provider may not be found to have “the . . . ability to control . . .” an act of infringement merely because it monitors content online.

A narrow reading of what constitutes a directly attributable financial interest is also suggested by the House Report accompanying an earlier version of section 512(c)(1)(B),¹³³ which explained that:

In determining whether the financial benefit criterion is satisfied, courts should take a common-sense, fact-based approach, not a formalistic one. In general, a service provider conducting a legitimate business would not be considered to receive a “financial benefit directly attributable to the infringing activity” where the infringer makes the same kind of payment as noninfringing users of the provider’s service. Thus, receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a “financial benefit directly attributable to the infringing activity.” Nor is subsection (c)(1)(B) intended to cover fees based on the length of the message (e.g., per number of bytes) or by connect time. It would however, include any such fees where the value of the service lies in providing access to infringing material.¹³⁴

This is a narrower reading of “financial benefit” than in *Fonovisa, Inc. v. Cherry Auction, Inc.*,¹³⁵ for example, where the Ninth Circuit found that a flea market operator had a “direct financial interest” in the infringing activity of some of the vendors at the flea market because it earned admission fees, concession stand sales and parking fees from such

¹³¹H. Rep. No. 105-796, 105th Cong. 2d Sess. 1, 72 (1998).

¹³²H. Rep. No. 105-796, 105th Cong. 2d Sess. 1, 72 (1998).

¹³³Section 512(c)(1)(B) provides that a service provider “does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.” The earlier version included this language but used “if the provider” instead of “in a case in which the service provider,” which is not a material difference. The structure of the bill in this earlier version distinguished between direct liability and secondary liability, treating each separately, whereas the version ultimately enacted refers only to copyright infringement.

¹³⁴H.R. Conf. Rep. No. 551, 105th Cong., 2d Sess. 54 (1998).

¹³⁵*Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996).

vendors, even though these same flat fees were charged to all vendors—not just those who were engaged in infringing activity.¹³⁶

Whether this in fact was intended to be narrower than the standard applied in common law cases is less clear. The same House Report asserts that Congress was merely “codify[ing] and clarify[ing]” the existing standard for vicarious liability:

The financial benefit standard in subparagraph (B) is intended to codify and clarify the direct financial benefit element of vicarious liability as it has been interpreted in cases such as *Marobie-FL, Inc. v. National Association of Fire Equipment Distributors* As in *Marobie*, receiving a one-time set-up fee and flat periodic payments for service from a person engaging in infringing activities would not constitute receiving “a financial benefit directly attributable to the infringing activity.” Nor is subparagraph (B) intended to cover fees based on the length of the message (per number of bytes, for example) or by connect time. It would, however, include any such fees where the value of the service lies in providing access to infringing material.¹³⁷

However, the *Marobie*¹³⁸ court, in reaching this conclusion, relied on *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,¹³⁹ which in turn reached this conclusion by following the lower court decision in *Fonovisa, Inc. v. Cherry Auction Inc.*,¹⁴⁰ which was subsequently reversed on this very point by the Ninth Circuit in early 1996.

It is apparent from the Committee Report that Congress, writing in 1998, did not realize that *Marobie* relied on *Netcom* which relied on another district court opinion that had been reversed on appeal, and that the law at that time in fact was that a one-time set-up fee and flat periodic payments could be sufficient to constitute a direct financial interest, at least in the Ninth Circuit under *Fonovisa*. Alternatively, the drafters of the Committee Report perhaps appreciated this infirmity which is why they cited *Marobie*, rather than *Netcom*

¹³⁶See *supra* § 4.11[4] (analyzing vicarious liability).

¹³⁷H.R. Rep. 105-551, Pt. I, at 25 to 26 (1998).

¹³⁸*Marobie-FL, Inc. v. National Ass’n of Fire Equipment Distributors*, 983 F. Supp. 1167 (N.D. Ill. 1997); see generally *supra* § 4.11[9][C].

¹³⁹*Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1376–77 (N.D. Cal. 1995).

¹⁴⁰*Fonovisa, Inc. v. Cherry Auction, Inc.*, 847 F. Supp. 1492, 1496 (E.D. Cal. 1994), *rev’d*, 76 F.3d 259, 263 (9th Cir. 1996); see generally *supra* §§ 4.11[5], 4.11[8][B], 4.11[8][C].

itself. In either case, Congress arguably had conflicting goals in mind in providing that section 512(c)(1)(B) was intended to both (a) codify and clarify existing common law; and (b) provide that a flat fee or other payment charged without regard to whether a customer is an infringer does not constitute a “direct financial interest.”

While it is not entirely clear whether Congress was more concerned with codifying the standard for vicarious liability or clarifying that fixed fee payments would not satisfy the “financial benefit” prong of section 512(c)(1)(B), the specific discussion and reference to *Marobie* suggest that it was the latter, not the former.

In practice, the law continues to be muddled on what constitutes a direct financial interest. Courts in the Ninth Circuit purport to apply the same standard for “direct financial benefit” under section 512(c)(1)(B) as would apply at common law.¹⁴¹ In fact, the common law standards for “direct financial benefit” in digital copyright cases have evolved in the Ninth Circuit since the time the DMCA was enacted. *Fonovisa*, decided in 1996, held that a company that charged a flat fee to all vendors nonetheless had a direct financial interest in the activities. In *A&M Records, Inc. v. Napster, Inc.*,¹⁴² the Ninth Circuit appeared to adopt an even more liberal standard, holding that a defendant that charged no money at all nonetheless had a financial interest in the infringing activities of its users where its future revenues were dependent on expanding its user base, and the draw that brought users to the site was the free availability of infringing material.¹⁴³ That seemingly more liberal common law standard, however, was applied under the DMCA in two subsequent cases to find a financial interest lacking.

In *Ellison v. Robertson*,¹⁴⁴ the Ninth Circuit held that AOL did not have a financial interest in third-party acts of infringement where AOL charged customers a monthly flat fee for access and there was no evidence that AOL attracted or retained subscribers because of the alleged acts of infringement or lost subscriptions because of its eventual obstruc-

¹⁴¹See *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

¹⁴²*A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001).

¹⁴³See *supra* § 4.11[5].

¹⁴⁴*Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004).

tion of the infringement.¹⁴⁵ Similarly, in *Perfect 10, Inc. v.*

¹⁴⁵*Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004). The lower court had accepted AOL's argument that with respect to infringing material originally posted on another service and automatically copied to AOL's Usenet servers, AOL did not have a direct financial interest because "AOL did not receive any financial compensation from its peering agreements and participation in Usenet." In addition, the district court emphasized that Usenet usage constituted a very small percentage of AOL's total member usage (0.25%) and "any 'draw' to one particular newsgroup, such as alt.binaries.e-book, [wa]s miniscule and remote, as the pro rata 'draw' of any single newsgroup (AOL carries more than 43,000 total) constitute[d] approximately 0.00000596% of AOL's total usage." *Ellison v. Robertson*, 189 F. Supp. 2d 1051, 1062 (C.D. Cal. 2002), *aff'd in relevant part on other grounds*, 357 F.3d 1072 (9th Cir. 2004). The district court also noted that the portion of Usenet usage related to copyright infringement was even smaller, as evidenced by the fact that only 10 of AOL's 20 million users inquired when AOL blocked the relevant newsgroup. Whereas *Fonovisa* involved "a symbiotic relationship . . . between the infringing vendors and the landlord" . . . [b]y contrast, . . . Usenet usage related to copyright infringement constitute[d] a miniscule portion of AOL usage. The financial benefit accruing to AOL from such infringing usage, if any benefit exists at all, is too indirect and constitutes far too small a 'draw' to fairly support the imposition of vicarious . . . liability." 189 F. Supp. 2d at 1063.

As with its analysis of the control prong, the district court in *Ellison* concluded, based on the Senate Report accompanying an earlier version of the statute, that the DMCA provided "persuasive support for interpreting 'direct financial benefit' to require something more than the indirect, insignificant benefits that have accrued to AOL, as a result of copyright infringement on its Usenet servers." 189 F. Supp. 2d at 1063. *But see Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124, 157 (S.D.N.Y. 2009) (rejecting the argument that infringing music accounted for less than 1% of the total newsgroups available on defendants' service because "the law is clear that to constitute a direct financial benefit, the 'draw' of infringement need not be the primary, or even a significant, draw—rather, it need only be a draw."), *citing Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004) ("The essential aspect of the 'direct financial benefit' inquiry is whether there is a causal relationship between the infringing activity and any financial benefit the defendant reaps, regardless of how substantial the benefit in proportion to a defendant's overall profits.") and *Arista Records, Inc. v. Flea World, Inc.*, No. 03-2670 (JBS), 2006 WL 842883 (D.N.J. Mar. 31, 2006)). The Ninth Circuit in *Ellison* affirmed the finding that there was no financial interest based on inadequate proof that "customers either subscribed because of the available infringing material or cancelled subscriptions because it was no longer available." *Ellison*, 357 F.3d at 1079. Ultimately, the difference between *Ellison* and *Usenet.com*—which both involved services that made accessible the Usenet—is that AOL was a legitimate service provider that incidentally provided access to the Usenet, whereas *Usenet.com* was a service that made an effort to make infringing music files available—and

CCBill, LLC,¹⁴⁶ the Ninth Circuit held that “the relevant inquiry is ‘whether the infringing activity constitutes a draw for subscribers, not just an added benefit.’”¹⁴⁷

The same standard was applied in a subsequent Ninth Circuit case in which the court found that Fung, the operator of various BitTorrent tracker sites, and the entities he operated, were ineligible for the user storage safe harbor because they received a financial benefit and had the right and ability to control. In *Columbia Pictures Industries, Inc. v. Fung*,¹⁴⁸ the court held that the connection between the infringing activity and the defendants’ income stream derived from advertising “was sufficiently direct to meet the direct ‘financial benefit’ prong of § 512(c)(1)(B).”¹⁴⁹ Applying Ninth Circuit law, the court in *Fung* explained that:

[I]n the context of service providers who charge for their services, . . . a service provider receives a direct financial benefit from infringing activity where “there is a causal relationship between the infringing activity and any financial benefit a defendant reaps, regardless of how substantial the benefit is in proportion to a defendant’s overall profits.” . . . Thus, where a service provider obtains revenue from “subscribers,” the relevant inquiry is “‘whether the infringing activity constitutes a draw for subscribers, not just an added benefit.’”¹⁵⁰

The court found that defendants promoted advertising by pointing to infringing activity; obtained advertising revenue that depended on the number of visitors to his sites; attracted primarily visitors who were seeking to engage in infringing activity, as that is mostly what occurred on his sites; and encouraged that infringing activity. The appellate

available for longer—on its site. Thus, infringing content was not deemed to be a draw in *Ellison*, while it was in *Usenet.com*.

¹⁴⁶*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

¹⁴⁷*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117–18 (9th Cir.) (quoting *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004)), cert. denied, 522 U.S. 1062 (2007). In *CCBill*, the appellate court found that evidence that the service provider hosted, for a fee, websites that contained infringing material inadequate to establish the requisite financial benefit. 488 F.3d at 1118 (relying on legislative history).

¹⁴⁸*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1044–46 (9th Cir. 2013).

¹⁴⁹*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1045 (9th Cir. 2013).

¹⁵⁰*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1044 (9th Cir. 2013) (citations and footnote omitted).

panel explained, “[g]iven this confluence of circumstances, Fung’s revenue stream was tied directly to the infringing activity involving his websites, both as to his ability to attract advertisers and as to the amount of revenue he received.”¹⁵¹

In an earlier opinion, a district court in the Southern District of New York expressed the view that “it is clear that the ‘direct financial benefit’ prong of the common law vicarious liability standard is construed more broadly than it is under the DMCA”¹⁵²

As with the financial interest prong, common law vicarious liability decisions applying the right and ability to control in digital copyright cases also have evolved since the time the DMCA was enacted (and indeed may have been influenced by DMCA case law).

While section 512(c)(1)(B) is arguably intended to be construed narrowly, right and ability to control also has been interpreted more strictly in vicarious liability cases involving service providers, at least in the Ninth Circuit. In *Perfect 10, Inc. v. Amazon.com, Inc.*¹⁵³ and *Perfect 10, Inc. v. VISA Int’l Service Ass’n*,¹⁵⁴ for example, Ninth Circuit panels held that the defendants did not have the right and ability

¹⁵¹*Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1045 (9th Cir. 2013). Fung was not a case involving a legitimate service provider. In Fung, the Ninth Circuit affirmed the entry of summary judgment for the plaintiffs on the issue of copyright inducement. *See supra* § 4.11[6][F] (discussing the Fung court’s holding on inducement). In elaborating on the evidence that supported the finding that *Fung* received a financial benefit, the court wrote:

Here, the record shows that Fung generated revenue by selling advertising space on his websites. The advertising revenue depended on the number of users who viewed and then clicked on the advertisements. Fung marketed advertising to one advertiser by pointing to the “TV and movies . . . at the top of the most frequently searched by our viewers,” and provided another with a list of typical user search queries, including popular movies and television shows. In addition, there was a vast amount of infringing material on his websites—whether 90–96% or somewhat less—supporting an inference that Fung’s revenue stream is predicated on the broad availability of infringing materials for his users, thereby attracting advertisers. And, as we have seen, Fung actively induced infringing activity on his sites.

Id.

¹⁵²*Capitol Records, Inc. v. MP3Tunes, LLC*, No. 07 Civ. 9931 (WHP), 2013 WL 1987225, at *10 (S.D.N.Y. May 14, 2013).

¹⁵³*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007).

¹⁵⁴*Perfect 10, Inc. v. Visa Int’l Service Ass’n*, 494 F.3d 788 (9th Cir. 2007), *cert. denied*, 553 U.S. 1079 (2008).

to control even though they had contracts with third-party infringing sites for advertisements in *Amazon.com* and payment processing services in *VISA*. The courts in those cases distinguished the ability to terminate a contract from the right and ability to control whether infringing material was on the third-party sites they serviced.

Courts in practice have thus far construed “financial interest” and “right and ability to control” narrowly under section 512(c)(1)(B) although in some cases this construction may reflect discomfort with the application of the vicarious liability doctrine to legitimate service providers.¹⁵⁵

¹⁵⁵For example, as previously noted, in *CoStar Group Inc. v. LoopNet, Inc.*, 164 F. Supp. 2d 688, 704 (D. Md. 2001), *aff’d on other grounds*, 373 F.3d 544 (4th Cir. 2004), the court wrote that section 512(c)(1)(B) codified the vicarious liability standard, but then proceeded to apply it without reference to vicarious liability case law. The court instead relied on *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001), a DMCA case, for the proposition that the right and ability to control infringing activity under the DMCA cannot simply mean the ability of a service provider to remove or block access to materials posted on its website or stored in its system. See also *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1098, (C.D. Cal. 2004) (following the district court’s analysis in *CoStar* on this point and further holding that where a defendant’s right and ability to control infringing activity is limited to disconnecting access to the defendant’s service, such control is insufficient under the DMCA to deny a defendant the benefit of the DMCA safe harbor), *aff’d in relevant part on different grounds*, 488 F.3d 1102, 1117–18 (9th Cir.) (finding no financial interest; holding that “‘direct financial benefit’ should be interpreted consistent with the similarly worded common law standard for vicarious copyright liability.”), *cert. denied*, 522 U.S. 1062 (2007); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1109–10 (W.D. Wash. 2004) (ruling that Amazon.com satisfied the requirements of section 512(c) because “[o]utside of providing the zShops platform, Amazon did not have the right or ability to control vendor sales. Amazon is never in possession of the products sold by zShops vendors Amazon does not preview the products prior to their listing, does not edit the product descriptions, does not suggest prices, or otherwise involve itself in the sale”; “While Amazon does provide transaction processing for credit card purchases, that additional service does not give Amazon control over the sale.”).

Hendrickson did not purport to apply vicarious liability case law in reaching this interpretation of section 512(c)(1)(B). By contrast, the Ninth Circuit in *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001), a vicarious liability case which the *LoopNet* court cited earlier in its opinion, held that, for purposes of vicarious liability, the ability of an Internet service provider to block access “for any reason whatsoever is evidence of the right and ability to supervise infringing conduct.” *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001); see generally *supra* § 4.11[9][F]. The Ninth Circuit also found a reservation of

In reality, as courts blur the lines between DMCA and common law case law, some courts effectively may apply a lower standard in cases such as *Napster* that involved massive piracy on a site that plainly had sought to monetize third-party acts of infringement than in cases such as *Elision* that involve legitimate commercial services where the only issue is whether the service provider may be held liable for particular acts of user misconduct. The particular test applied in effect may be outcome-determinative.

Whether the standard for financial interest is coextensive with or narrower than the common law test for vicarious liability, case law to date generally provides that the financial interest prong requires a showing that “the infringing activity constitutes a draw for subscribers, not just an added

rights in posted terms and conditions to evidence an ability to control user infringement. *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001); see also *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117–18 (9th Cir.) (holding that “the relevant inquiry [to establish vicarious liability] is ‘whether the infringing activity constitutes a draw for subscribers, not just an added benefit’” but finding no financial interest under the *Napster* standard in that case), *cert. denied*, 522 U.S. 1062 (2007).

The district court in *LoopNet* likewise interpreted the financial interest prong narrowly, concluding that the defendant did not have a financial interest in the infringement because users were not charged a fee. See 164 F. Supp. 2d at 704–05. Yet in *Napster*, the Ninth Circuit rejected this analysis in the context of a vicarious liability claim, ruling that a “[f]inancial benefit exists where the availability of infringing material ‘acts as a draw’ for customers.” *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1023 (9th Cir. 2001); see also *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117–18 (9th Cir.) (holding that “the relevant inquiry is ‘whether the infringing activity constitutes a draw for subscribers, not just an added benefit’” but finding no financial interest under the *Napster* standard in that case), *cert. denied*, 522 U.S. 1062 (2007). The district court in *LoopNet* noted in *dicta* that the financial benefit prong of the DMCA’s user storage safe harbor, as set forth in section 512(c)(1)(B), could not be met where a service provider charged the same flat fee to all users. 164 F. Supp. 2d at 704–05 (citing the proposed committee report to an earlier version of the DMCA); see also *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 748 (S.D.N.Y. 2012) (holding that defendants did not have a financial interest where Kodak charged a flat fee for reprints, regardless of the nature of the reprint, users selected what images to have reprinted, and Photobucket had no knowledge of what images in fact were sent to Kodak), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014). Once again, this narrow view is inconsistent with vicarious liability case law on this same point. See, e.g., *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 263 (9th Cir. 1996); see generally *supra* §§ 4.11[4], 4.11[8][C].

benefit.’ ”¹⁵⁶

4.12[7] Information Location Tools

A service provider that otherwise meets the general threshold prerequisites described in section 4.12[3] may limit its liability for infringement for linking or referring users to infringing material or activity by using “information location tools, including a directory, index, reference, pointer, or hypertext link.”¹ None of these terms are defined in the Act. Given how quickly technology and business models change in cyberspace, Congress presumably intended the term “information location tools” to be broad enough to encompass future tools which would be akin to “a directory, index, reference, pointer, or hypertext link.” Although no court has yet ruled on the issue, linked content made available via frames, in-line links or embedded links, should be entitled to protection under the broad statutory definition of *information location tools*.²

To qualify for the information location tools limitation, a

¹⁵⁶*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1117–18 (9th Cir.), cert. denied, 522 U.S. 1062 (2007); *Ellison v. Robertson*, 357 F.3d 1072, 1079 (9th Cir. 2004) (quoting legislative history); see also *Hempton v. Pond5, Inc.*, Case No. 3:15-cv-05696-BJR, 2016 WL 6217113, at *9 (W.D. Wash. Oct. 25, 2016) (granting summary judgment for the service provider, which had received between \$192.95 and \$2,000 in revenue from a user’s alleged infringement of plaintiff’s works, because there was no evidence that customers were drawn to Pond5 for infringing content); *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 748 (S.D.N.Y. 2012) (holding that the defendants did not have a financial interest directly attributable to infringing activity within the meaning of section 512(c)(1)(B) because there was no evidence that either Photobucket or the Kodak defendants “capitalizes specifically because a given image a user selects to print is infringing . . . , [t]he Defendants’ profits are derived from the service they provide, not a particular infringement . . . [and] Photobucket has no knowledge of which images users may select to send to the Kodak Defendants to be printed, and, as such, Photobucket has no ability to control whether users request that infringing material be printed.”), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014).

[Section 4.12[7]]

¹17 U.S.C.A. § 512(d).

²One court suggested in *dicta* that the DMCA safe harbor could be potentially applicable to a case involving embedded links to a photo posted by a third party on Twitter. See *Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 596 (S.D.N.Y. 2018). Embedded links and other types of links (including frames and in-line links) are addressed in section 9.03 to 9.04 in chapter 9.

service provider must meet three of the requirements of the user storage limitation discussed in section 4.12[6]. Specifically, (1) a service provider must not have actual knowledge or awareness of the infringement or, if it has either, it must promptly remove or disable access to the infringing material; (2) where a service provider has the right and ability to control the infringing activity, it must not “receive a benefit financially directly attributable to the infringing activity”; and (3) the service provider must remove or disable access to infringing material upon receipt of substantially complying notification (as described below in section 4.12[9][B]).³ These requirements are addressed in greater detail in connection with the user storage liability limitation in section 4.12[6].

Through inartful drafting, the statute appears not to compel the designation of an agent. Section 512(d), by its terms, restates the requirements of section 512(c)(1) (notice, knowledge or awareness and financial interest/right and ability to control) and incorporates by reference section 512(c)(3) (elements of a notification) modified expressly to refer to links, rather than user content, but excludes section 512(c)(2) (designation of an agent). Subsection (c)(3), however, provides that “a notification of claimed infringement must be a written communication *provided to the designated agent* of a service provider . . .,” and therefore appears to implicitly compel compliance with subsection (c)(2), governing designation of an agent.⁴ Alternatively, since subsection 512(c)(2) is not deemed applicable to the information location tools liability limitation of section 512(d), it is possible that the term *designated agent* for purposes of section 512(d) merely refers to a designated agent to receive notifications, rather than an agent formally designated pursuant to section 512(c)(2) through a notice filed with the U.S. Copyright Office.

While a copyright owner plainly must serve a notification on a service provider to compel it to disable access to or remove a link or other information location tool, and a ser-

³17 U.S.C.A. § 512(d); *see also Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1046–47 (9th Cir. 2013) (holding the operator of BitTorrent tracker sites ineligible for the information location tools safe harbor where the defendant was aware of facts and circumstances from which infringing activity was apparent, received a direct financial benefit from infringing activity and had the right and ability to control such activity); *see generally supra* § 4.12[6] (analyzing these factors).

⁴*See infra* § 4.12[9][A].

vice provider in turn must respond expeditiously to the notification to benefit from the liability limitation, the provisions governing counter notifications have no applicability to the information location tools safe harbor, even though some courts have erroneously concluded that they are applicable.⁵

Section 512(g) provides a broad exemption to service providers from liability to “any person for any claim based on the service provider’s good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.” For purposes of the user storage liability limitation only, this exemption does not apply if material is removed in response to a notification if the affected subscriber timely served a counter notification, in which case the service provider must comply with the requirements for counter notifications to enjoy the exemption. The DMCA is unambiguous, however, that this exception only applies for removal for material stored at the direction of a subscriber.⁶ Service providers are exempt from liability to anyone for any claim based on disabling access to or removing an information location tool and need to comply with procedures for counter notifications.⁷

The liability limitation for information location tools, by its terms, applies to a directory, index, reference, pointer or hypertext link. It is not necessary that a service provider maintain a large number of links or connections to other locations to benefit from this limitation.⁸

Absent DMCA protection, however, the risk of copyright liability for linking generally is low (and typically lower than for material stored at the direction of a user, which is the

⁵See *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004) (*dicta*); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1179 (C.D. Cal. 2002).

⁶See 17 U.S.C.A. § 512(g)(2).

⁷See 17 U.S.C.A. § 512(g)(1); see generally *infra* § 4.12[9][C].

⁸See *Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1097–98 (C.D. Cal. 2004) (rejecting the argument that because a defendant “merely links to a relatively small universe of websites with whom it has in place contractual relationships and established review procedures, it is not entitled to the protection under § 512(d)), *aff’d in part on other grounds*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

safe harbor more frequently litigated).⁹ Simply because a service provider does not satisfy the limitation created for information location tools does not necessarily mean that it may be held liable for linking. A link does not create a “copy” within the meaning of *MAI Systems Corp. v. Peak Computer, Inc.*,¹⁰ but merely constitutes an instruction to a browser to go to a different location. Hence, most courts that have considered the issue have held that the act of linking does not create a “copy,” although it may facilitate the creation of a “copy,”¹¹ in a user’s screen RAM.¹² At most, the creation of a link therefore potentially could expose the linking party to

⁹See *supra* § 4.12[6].

¹⁰*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994).

¹¹See, e.g., *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1156, 1162 (9th Cir. 2007) (applying the server test in holding that Google could not be held directly liable for violating the display or distribution rights of the plaintiff by creating links to photographs on third-party locations on the Internet because the content that was linked to was not located on Google’s own servers; “Google simply provides HTML instructions directing a user’s browser to access a third-party website. . . . [I]t is the website publisher’s computer, rather than Google’s computer, that stores and displays the infringing image.”); *Flava Works, Inc. v. Gunter*, Case No. 17 C 1171, 2018 WL 620035, at *2, 4 (N.D. Ill. Jan. 30, 2018) (dismissing plaintiff’s claim for direct infringement for offering a video bookmarking service because the defendant could not be held directly liable where it was the user, not the service, that clicked on a thumbnail link to access embedded content, and dismissing claims for secondary infringement because the plaintiff could not plausibly identify any myVidster users that in fact infringed one of plaintiff’s works—to serve as an underlying act of direct infringement—merely by reference to DMCA notices reproducing alleged links); *Microsoft Corp. v. Softicle.com*, Civil Action No. 16–2762, 2017 WL 5517379, at *2 (D.N.J. Sept. 29, 2017) (dismissing a claim for direct copyright infringement based on a link to infringing material; “Providing a link to a website containing infringing material does not, as a matter of law, constitute direct copyright infringement.”); *Pearson Education, Inc. v. Ishayev*, 963 F. Supp. 2d 239, 251 (S.D.N.Y. 2013) (holding that the defendant was not liable for distributing infringing content by merely linking to it on a different site; “A hyperlink does not itself contain any substantive content; in that important sense, a hyperlink differs from a zip file. Because hyperlinks do not themselves contain the copyrighted or protected derivative works, forwarding them does not infringe on any of a copyright owner’s five exclusive rights under § 106.”); *MyPlayCity, Inc. v. Conduit Ltd.*, No. 10 Civ. 1615(CM), 2012 WL 1107648, at *12–14 (S.D.N.Y. Mar. 30, 2012) (granting summary judgment for the defendant on plaintiff’s claim for direct copyright infringement for distribution of plaintiff’s videogames by including a link on a toolbar it distributed following the termination of a license; “Because the actual transfer of a file between computers must occur, merely providing a ‘link’ to a site contain-

liability for inducement, contributory infringement or in limited circumstances (if the linking party derived a financial benefit from the link) vicarious liability.¹³ Some district courts, however, have found embedded links or frames, in contrast to ordinary links, to create potential direct liability for public displays of photographs¹⁴ or the public performance

ing copyrighted material does not constitute direct infringement of a holder's distribution right.”); *see also* *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 760 (7th Cir. 2012) (holding that a video bookmarking site could not be held liable for contributory copyright infringement; “The direct infringers in this case are the uploaders; myVidster is neither a direct nor a contributory infringer—at least of Flava’s exclusive right to copy and distribute copies of its copyrighted videos.”); *Batesville Services, Inc. v. Funeral Depot, Inc.*, No. 1:02-CV-01011-DFH-TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004) (explaining that hyperlinking “does not itself involve a violation of the Copyright Act (whatever it may do for other claims) since no copying is involved.”); *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1202 n.12 (N.D. Cal. 2004) (stating in *dicta* that “[a]lthough hyperlinking *per se* does not constitute direct copyright infringement because there is no copying . . . in some instances there may be a tenable claim of contributory infringement or vicarious liability.”); *see generally* *infra* §§ 9.03, 9.04 (analyzing linking in greater detail).

¹²*See supra* § 4.03.

¹³*See, e.g., Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007) (discussing in-line linking and potential liability); *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp. 2d 1290 (D. Utah 1999) (finding secondary liability based on active encouragement); *Batesville Services, Inc. v. Funeral Depot, Inc.*, 1:02-CV-01011-DFH-TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004) (holding that links under the unusual facts of the case could provide a basis for secondary liability); *Arista Records, Inc. v. MP3Board, Inc.*, No. 00 CIV. 4660(SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002) (denying defendant’s motion for summary judgment on plaintiffs’ claim for copyright infringement because its provision of an “automated system devoted to searching for, aggregating, and organizing links” to infringing works presented a triable issue of fact); *supra* § 4.10[1] (fair use); *infra* §§ 9.03 to 9.06 (analyzing linking law). *But see* *Live Nation Motor Sports, Inc. v. Davis*, 35 Media L. Rep. (BNA) 1209, 81 U.S.P.Q.2d 1826, 2007 WL 79311 (N.D. Tex. Jan. 9, 2007) (holding that a link to a streamed live webcast constituted a public performance). In contrast to ordinary links, in-line links or frames may create greater risks of liability. *See supra* § 4.10[1]; *infra* §§ 9.03, 9.04. An entity creating an in-line link, which reproduces a portion of content from another location, would likely have difficulty qualifying for the liability limitation, which requires an absence of knowledge or awareness. On the other hand, a Web host or other third party potentially could benefit from the limitation if, for example, it merely provided access to a site or service that created the in-line link.

¹⁴*See, e.g., Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *3-5 (S.D.N.Y. 2021) (denying defendant’s motion

of streaming media,¹⁵ subject of course to defenses that may apply including the DMCA (and fair use¹⁶ or implied

to dismiss plaintiff's copyright infringement claim, holding that plaintiff stated a claim that Sinclair's placement of an embedded link to plaintiff's video of a starving polar bear (which plaintiff had uploaded to Instagram and Facebook), in an article describing how the video "went 'viral,'" constituted an unauthorized public display, and that Sinclair's fair use defense could not be resolved on a motion to dismiss); *Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585 (S.D.N.Y. 2018) (holding that an image displayed via embedded links in various publications, from the Twitter feed where it had been posted, constituted a public display under the Copyright Act; granting partial summary judgment to the plaintiff); *The Leader's Institute, LLC v. Jackson*, Civil Action No. 3:14-CV-3572-B, 2017 WL 5629514, at *10 (N.D. Tex. Nov. 22, 2017) (denying plaintiff's motion for summary judgment on defendant's counterclaim for copyright infringement, holding that plaintiff publicly displayed copyrighted content from defendant's website by framing it on its own website; distinguishing framing from ordinary linking); see generally *infra* §§ 9.03, 9.04 (analyzing these cases and potential liability for links in greater detail).

These cases directly conflict with *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1156, 1162 (9th Cir. 2007) (applying the server test in holding that Google could not be held directly liable for violating the public display or distribution rights of the plaintiff by creating links to photographs on third-party locations on the Internet because the content that was linked to was not located on Google's own servers; "Google simply provides HTML instructions directing a user's browser to access a third-party website. . . . [I]t is the website publisher's computer, rather than Google's computer, that stores and displays the infringing image."); see generally *infra* §§ 9.03, 9.04.

¹⁵See *Live Nation Motor Sports, Inc. v. Davis*, 81 U.S.P.Q.2d 1826, 2007 WL 79311 (N.D. Tex. Jan. 9, 2007) (holding that a link to a stream of a live webcast of motor races that were shown in real time constituted a public performance or display because those terms encompass "each step in the process by which a protected work wends its way to the audience"); see generally *infra* §§ 9.03, 9.04 (analyzing these cases and potential liability for links in greater detail).

¹⁶See, e.g., *Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 6393010 (E.D.N.Y. Nov. 2, 2020) (dismissing, as fair use, a photographer's copyright infringement claim against a sports news publisher, which had included an embedded link to an Instagram post by professional tennis player Caroline Wozniacki, announcing her retirements (which included a low-resolution, cropped version of a photograph taken by the plaintiff), in an article it published about Wozniacki's career, which also quoted the text of the Instagram post); *Walsh v. Townsquare Media, Inc.*, 464 F. Supp. 3d 570 (S.D.N.Y. 2020) (entering judgment on the pleadings, based on fair use, on a Paparazzi photographer's copyright infringement claim, brought against the publisher of *XXL* magazine, which had embedded a link to an Instagram post by hip hop artist Cardi B, which included a photograph taken by plaintiff of Cardi B at a Tom Ford fashion show, in an article entitled *Cardi B Partners with Tom Ford for*

license¹⁷).¹⁸ Direct liability also may be found when links are

New Lipstick Shade, which was focused on the event and referenced the Cardi B Instagram post which featured the photograph); *see also Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 7625222 (E.D.N.Y. Dec. 22, 2020) (denying reconsideration). *Cf. Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *5-7 (S.D.N.Y. 2021) (denying defendant's motion to dismiss plaintiff's copyright infringement claim, premised on Sinclair's placement of an embedded link to plaintiff's video of a starving polar bear in an article describing how the video "went 'viral,'" because Sinclair's fair use defense could not be resolved on a motion to dismiss based solely on the allegations of the complaint, despite finding that the use was transformative); *McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 604-09 (S.D.N.Y. 2020) (holding, in an opinion decided before *Boesen* and *Walsh*, that, on the facts of that case, fair use could not be established as a matter of law at the pleadings stage, in a case where plaintiff posted a photograph of an ephemeral lake on March 13, 2019, and the very next day Newsweek allegedly published an article about the ephemeral lake, embedding plaintiff's Instagram post about the lake, as part of the article).

¹⁷*See, e.g., McGucken v. Newsweek LLC*, 19 Civ. 9617 (KPF), 2020 WL 6135733, at *1-3 (S.D.N.Y. Oct. 19, 2020) (affirming, in denying reconsideration, that "while Instagram's Terms of Use clearly granted Instagram a license to sublicense Plaintiff's publicly posted content, there was insufficiently clear language to support, in the context of a Rule 12(b)(6) motion, the existence of a sublicense between Instagram and Defendant."); *Sinclair v. Ziff Davis, LLC*, 18-CV-790 (KMW), 2020 WL 3450136, at *1-2 (S.D.N.Y. June 24, 2020) (adhering to its previous holding that, "by agreeing to Instagram's Terms of Use, Plaintiff authorized Instagram to grant API users, such as Mashable, a sublicense to embed her public Instagram content, as set forth in Instagram's Platform Policy" but granting reconsideration, and revising its previous decision, by holding "that the pleadings contain insufficient evidence to find that Instagram granted Mashable a sublicense to embed Plaintiff's Photograph on its website."); *McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 603-04 (S.D.N.Y. 2020) (denying Newsweek's motion to dismiss, holding that while Instagram's Terms of Use "unequivocally grant Instagram a license to sublicense Plaintiff's publicly posted content . . . , and the Privacy Policy clearly states that 'other Users may search for, see, use, or share any of your User Content that you make publicly available through' Instagram . . . , " the court could not dismiss plaintiff's claims; "Although Instagram's various terms and policies clearly foresee the possibility of entities such as Defendant using web embeds to share other users' content . . . , none of them expressly grants a sublicense to those who embed publicly posted content. Nor can the Court find, on the pleadings, evidence of a possible implied sublicense. . . . While the Court acknowledges that it may be possible to read Instagram's various terms and policies to grant a sublicense to embedders, the Court's role on a Rule 12(b)(6) motion is to 'draw all reasonable inferences in Plaintiff's favor.'").

¹⁸*See Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 596 (S.D.N.Y. 2018) (suggesting in *dicta* the potential availability of these

created in connection with other directly infringing activity, for which the DMCA safe harbor would not provide protection.¹⁹

4.12[8] Exemption from Liability to Subscribers for Removing or Disabling Access to Material Believed to be Infringing

A service provider that otherwise has met the threshold requirements set forth in section 512(i)¹ may be entitled to a broad exemption from liability under any theory of recovery for any good faith act to disable access to or remove material believed to be infringing (even where a formal notification has not been submitted). The Act immunizes service providers from liability

to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts and circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.²

This provision, by its terms, contemplates actions undertaken by a service provider “based on facts and circumstances from which infringing activity is apparent . . . ,” and is not limited to acts undertaken in response to formal notifications. Thus, service providers may act on their own initiative or in response to customer or other third-party complaints to remove or disable access to content believed to be infringing.

Unlike the four liability limitations set forth in subsec-

defenses). Licenses and implied licenses are addressed in section 4.05[7]. Fair use is analyzed in section 4.10[1].

¹⁹See *Batesville Services, Inc. v. Funeral Depot, Inc.*, No. 1:02-CV-01011-DFH-TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004) (holding that a triable issue of fact existed on the issue of defendant's potential direct or contributory liability for creating links to unauthorized photographs of plaintiff's products, and for designing, creating and paying for the pages that it linked to, after having been warned to stop displaying the pictures itself on its own website); see generally *infra* §§ 9.03, 9.04 (analyzing links in greater detail).

[Section 4.12[8]]

¹See *supra* § 4.12[3].

²17 U.S.C.A. § 512(g)(1). Although other provisions limit a service provider's liability, subsection (g)(1) creates a broad exemption (rather than merely a liability limitation) from liability “to any person for any claim.”

tions (a) through (d), the exemption created by subpart 512(g)(1) provided for removing or disabling access to content applies to “any claim”—not merely to copyright infringement claims. Indeed, the types of claims which conceivably could be brought against a service provider for removing or blocking access would not arise under the Copyright Act. In all likelihood, any cause of action for disabling access to or removing content would arise under state contract or tort law. In order to be effective (given the type of claims likely to be asserted), the exemption presumably will be construed to preempt state law.³

There is one exception to the broad exemption provided for removing or blocking access to content. If a service provider receives a notification about allegedly infringing material stored at the direction of a *subscriber*,⁴ it must comply with the requirements of subparts (c)(3) and (g)(2) governing notifications and counter notifications (which are discussed in sections 4.12[9][B] and 4.12[9][C]) to both limit its liability to the copyright owner for infringement and to its subscriber for removing or disabling access to its content. Specifically, a service provider would have to satisfy the requirements of subpart (c)(3) to limit its potential liability to the copyright owner for infringement and comply with subpart 512(g)(2) to avoid any liability to its subscriber for disabling access to or removing content in response to a notification. Stated differently, if a service provider removes or disables access to content belonging to a subscriber (as opposed to other content) in response to a notification directed at content stored at the direction of a user, the service provider may not benefit from the broad exemption created by subpart 512(g)(1) and instead must comply with the provisions of subpart 512(g)(2) governing counter notifications in order to claim the exemption.

Whether content is removed or access blocked pursuant to

³See, e.g., *English v. General Elec. Co.*, 496 U.S. 72, 79 (1990).

⁴A *subscriber* is not defined under the Act but should be understood as someone who necessarily is also a *user* (which is also not a defined term). Not all users, however, are necessarily subscribers. Based on the statutory scheme created by Congress, a subscriber is a person whose content has been removed (or access to its disabled) by a service provider in response to a formal notification pursuant to the user storage limitation. A subscriber presumably also has a contractual relationship with the service provider given the use of the word “subscriber,” as opposed to “user.” See *infra* § 4.12[9].

the requirements for subscriber content under subpart 512(g)(2) or under the broad exemption afforded by subpart 512(g)(1) in other circumstances, the safe havens created by subpart 512(g) apply regardless of whether the removed or disabled material ultimately is found to be infringing.⁵ The Act therefore encourages service providers to err on the side of protecting copyright owners.

Although subsection (g) creates incentives for service providers to monitor and block content, they are not required to do so or to seek facts indicating infringing activity, except to the extent consistent with a “standard technical measure.”⁶ In addition, nothing in the DMCA shall be construed to condition eligibility to the DMCA liability limitations (sections 512(a) through 512(d)) on a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.⁷

Depending on the facts of the case, a service provider sued for disabling access to or removing content also may be able to benefit from subpart 2 of the Good Samaritan exemption created by the Telecommunications Act of 1996.⁸ The Good Samaritan exemption (also referred to as the Communications Decency Act or CDA) provides broad exemptions to an “interactive computer service” (which, as defined, would include a service provider) for content that originates with a third party and for “any action voluntarily taken in good faith to restrict access to or [the] availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.”

The Good Samaritan exemption preempts most inconsistent state laws, but not any law pertaining to intellectual property,⁹ among other things. Where a service provider removes material on its own initiative, it therefore may be able to rely on the Good Samaritan exemption in defense of any state law claim brought based on the removal of content, to the extent that the service provider acted in good faith,

⁵17 U.S.C.A. § 512(g)(1).

⁶17 U.S.C.A. § 512(m)(1). *Standard technical measures* are discussed above in § 4.12[3][C].

⁷17 U.S.C.A. § 512(m)(2).

⁸*See* 47 U.S.C.A. § 230(c); *see generally infra* § 37.05.

⁹*See infra* § 37.05[5][B].

voluntarily, to restrict access to or the availability of material deemed “otherwise objectionable.”¹⁰ Where it removes material but fails to comply with the requirements of subpart 512(g)(2) after being served with a notification, however, the service provider may not be able to rely on the CDA to trump the express requirements of a federal statute pertaining to intellectual property.

4.12[9] Agent Designation, Notification, Counter Notification and Sanctions Under the System Caching, User Storage and Information Location Tools Limitations

4.12[9][A] Designation of an Agent

The caching, user storage, and arguably the information location tools limitations¹ compel service providers to designate an agent to receive notifications. For the user storage liability limitation only, an agent also must transmit notifications to subscribers and receive and process counter notifications if a service provider seeks to benefit from the exemption from any liability which otherwise could be imposed for removing or disabling access to subscriber content set forth in subpart 512(g)(2).² The exemption otherwise is available for service providers that disable ac-

¹⁰See 47 U.S.C.A. § 230(c)(2); *see generally infra* § 37.05.

[Section 4.12[9][A]]

¹Whether a DMCA agent (as opposed to merely a designated agent to receive notifications) is required under the information location tools safe harbor is addressed in section 4.12[7].

²The requirement for designating an agent to receive notifications is set forth in subsection 512(c), which addresses information residing on systems or networks at the direction of a user. Subpart (2) of that subsection requires designation of an agent, while subpart (3) sets forth the information that must be set included in a notification.

To benefit from the information location tools limitation created by subsection 512(d), subpart (d)(3) compels a service provider to respond to notifications as described in subpart (c)(3). Although subsection (d) expressly incorporates by reference only subpart (3) of subsection (c) (which describes the procedures for notifications), subpart (c)(3) itself incorporates by reference subpart (c)(2) (compelling designation of an agent) by providing that “[t]o be effective . . . , a notification of claimed infringement must be a written communication provided to the designated agent of a service provider.” 17 U.S.C.A. § 512(c)(3)(A). Thus, although hardly a model of clarity, the information location tools limitation appears to compel a service provider to designate an agent to receive notifications if the service provider intends to benefit from the limitation.

cess to or remove material pursuant to the other liability limitations, without complying with the provisions governing counter notifications.³

Service providers must designate an agent to receive notification of claimed acts of infringement and make available certain contact information about the designated agent on their websites “in a location accessible to the public” and in a required filing with the U.S. Copyright Office.⁴ The contact information must include “substantially” the following information: the name, address,⁵ phone number and

Service providers also must have an agent to receive notifications to fully benefit from the system caching limitation set forth in subsection 512(b). Subpart (b)(2)(E) provides that if a third-party places material online without the authorization of the copyright owner, the service provider must respond expeditiously to remove or disable access to the material alleged to be infringing in response to a notification described in subpart (c)(3) if: (1) the material was previously removed from the originating site or access to it has been disabled (or a court has entered an order compelling that result); or (2) the notification includes a statement confirming these facts. The caching limitation therefore compels a service provider to designate an agent to receive notifications in this one limited circumstance where stale material has been cached. An agent need not be designated to benefit from the other circumstances set forth in subsection 512(b) when the caching limitation might apply or to benefit from the routing limitation created by subsection 512(a).

A service provider must have an agent to receive counter notifications to qualify for the exemption from liability when subscriber content is removed (or access to it disabled) set forth in subpart 512(g)(2). An agent need not be designated to take advantage of the broad exemption set forth in subpart 512(g)(1).

The limitation for Nonprofit Educational Institutions set forth in subsection 512(e) specifically addresses conduct by university faculty members or graduate students. To the extent a Nonprofit Educational Institution seeks to benefit from the system caching, user storage and information location tools limitations, or the exemption created by subsection 512(g)(2), it also must designate an agent.

³17 U.S.C.A. § 512(g).

⁴17 U.S.C.A. § 512(c)(2).

⁵The Copyright Office’s Interim Regulations provide that the address listed for an agent must be “[t]he full address, including a specific number and street name or rural route.” 37 C.F.R. § 201.38(a)(4). A post office box “will not be sufficient except where it is the only address that can be used in that geographic location.” 37 C.F.R. § 201.38(a)(4). This requirement may be problematic for certain consumer services where, for safety reasons, the service does not wish to reveal its exact street address. This concern undoubtedly was not considered in 1998 when the regulations were promulgated. Ten years later, the FTC issued more enlightened regulations defining a “valid physical postal address” under the federal

email address of the designated agent, as well as any other information that the Register of Copyrights may require (including a registration fee to cover the cost of publishing and maintaining a current directory of agents, which must be made available in both hard copy and electronic formats and made available over the Internet).⁶ While the statute requires provision of “substantially” the information enumerated in the statute (name, address, phone number and email address of the agent), the interim regulations specify that all of this information must be provided.⁷ The interim regulations, unlike the statute, further require that a facsimile number be provided.⁸

The interim regulations were issued on November 3, 1998 and remained in effect through November 30, 2016.⁹ In September 2011, the Copyright Office solicited comments on proposed rulemaking to update the regulations for designat-

CAN-SPAM Act, 15 U.S.C.A. §§ 7701 to 7713; *see generally infra* § 34.03 (analyzing the CAN-SPAM Act). Under that statute, a “valid physical postal address” means the sender’s current street address, a post office box that the sender has accurately registered with the U.S. Postal Service, or a private mailbox that the sender has accurately registered with a commercial mail receiving agency that is established pursuant to U.S. Postal Service regulations. 16 C.F.R. § 316.2(p). The rationale for this broader definition is because it recognizes the privacy and security concerns of individuals who work from home or are fearful of publishing their street address for other reasons. *See* Definitions and Implementation Under the CAN-SPAM Act, 73 Fed. Reg. 29654, 29668 (May 21, 2008).

⁶17 U.S.C.A. § 512(c)(2); 73 Fed. Reg. 29654, 29668 (May 21, 2008).

⁷In *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 748–49 (S.D.N.Y. 2012), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014), the court held that Photobucket met the statutory requirement where it “substantially” complied with the requirement by providing the following information (but no name or telephone number):

Copyright Agent Photobucket.com, Inc. PO Box 13003 Denver, CO 80201
mailto:abuse@photobucket.com

Id. at 749. Similarly, in *Rosen v. eBay, Inc.*, No. CV-13-6801 MWF (Ex), 2015 WL 1600081, at *10 (C.D. Cal. Jan. 16, 2015), the court held that eBay substantially complied with the requirements of section 512(c)(2) where “[i]n numerous places on its website eBay provided facsimile, telephone, email and mail contact information to parties interested in submitting infringement notices” but omitted the name of its agent (who was disclosed in its agent designation filing with the U.S. Copyright Office).

⁸37 C.F.R. § 201.38(c)(5).

⁹*See* Designation of Agent to Receive Notification of Claims Infringement, 63 Fed. Reg. 59233 (Nov. 3, 1998).

ing agents¹⁰ and in December 2016 it issued new regulations requiring electronic registration of agent designation forms, which must be renewed every three years.¹¹ Agent designations made between November 3, 1998 and November 30, 2016, were deemed lapsed if not renewed by December 31, 2017.¹² In addition, agent designation forms now must be filed electronically.

In *BWP Media USA Inc. v. Hollywood Fan Sites LLC*,¹³ Judge J. Paul Oetken of the Southern District of New York held that the designation of a DMCA agent by a parent company did not extend to the company's subsidiary. In that case, the court held that there was nothing in the earlier designation filing with the U.S. Copyright Office that could be interpreted as referring to the subsidiary. Judge Oetken held that the DMCA did "not contemplate that a service provider entity can be shielded by the safe harbor where that entity has no presence at all" in the U.S. Copyright Office's directory of service providers.¹⁴ He explained that "[i]t is implausible that parties attempting to find a provider's DMCA agent designation, using the USCO's database, are expected to have independent knowledge of the corporate structure of a particular service provider."¹⁵ Judge Oetken also questioned whether a single designation could apply to multiple entities given the language used in the Copyright Office's interim regulations.¹⁶ In its 1998 interim regulations, the Copyright Office provided that:

For purposes of these interim regulations, related companies (e.g., parents and subsidiaries) are considered separate service providers who would file separate Interim Designations. When it considers final regulations, the Office will solicit comments

¹⁰See Notice of Proposed Rulemaking, 76 Fed. Reg. 59,953 (Sept. 28, 2011).

¹¹See 37 CFR § 201.38. Service providers must register their agents online at <https://dmca.copyright.gov/osp/login.html>. Paper registrations are no longer accepted.

¹²37 CFR § 201.38(e).

¹³*BWP Media USA Inc. v. Hollywood Fan Sites LLC*, 115 F. Supp. 397 (S.D.N.Y. 2015).

¹⁴*BWP Media USA Inc. v. Hollywood Fan Sites LLC*, 115 F. Supp. 397, 402 (S.D.N.Y. 2015).

¹⁵*BWP Media USA Inc. v. Hollywood Fan Sites LLC*, 115 F. Supp. 397, 402 (S.D.N.Y. 2015).

¹⁶*BWP Media USA Inc. v. Hollywood Fan Sites LLC*, 115 F. Supp. 397, 403 (S.D.N.Y. 2015).

as to whether related companies (e.g., parent and subsidiary companies) should be permitted to file a single Designation of Agent to Receive Notifications of Claimed Infringement.¹⁷

As noted above, the Copyright Office has yet to issue final regulations.

It is not clear, however, that interim administrative regulations for filings with the Copyright Office should necessarily control in evaluating the substantive law question of whether DMCA protection applies. In an analogous context, defects in copyright applications and compliance with the deposit requirement for obtaining copyright registration have held to be harmless errors that do not affect entitlement to copyright protection.¹⁸ In addition, the DMCA, on its face, only requires substantial compliance with its requirements.

District courts have also held that the user storage safe harbor is unavailable to a service provider if the alleged acts of infringement pre-date the time the service provider registered its DMCA agent with the U.S. Copyright Office.¹⁹

¹⁷Designation of Agent to Receive Notification of Claimed Infringement, 63 Fed. Reg. 59233, 59234 (Nov. 3, 1998).

¹⁸See *supra* § 4.08[2]; *infra* § 4.19.

¹⁹See, e.g., *Atlantic Recording Corp. v. Spinrilla, LLC*, 506 F. Supp. 3d 1294, 1320 (N.D. Ga. 2020) (holding that Spinrilla could not invoke the DMCA safe harbor prior to the time it registered its DMCA agent with the Copyright Office); *Werner v. Evolve Media, LLC*, 2:18-cv-7188-VAP-SKx, 2020 WL 3213808, at *8 (C.D. Cal. Apr. 28, 2020) (granting summary judgment for the copyright owner on Evolve's DMCA defense where the image at issue had been uploaded before Evolve had registered its DMCA agent with the U.S. Copyright Office); *BWP Media USA Inc. v. Hollywood Fan Sites LLC*, 115 F. Supp. 397, 400–01 (S.D.N.Y. 2015) (citing *Oppenheimer* approvingly for the proposition that “[a] service provider cannot retroactively qualify for the safe harbor for infringements occurring before the proper designation of an agent under the statute” and holding that “§ 512(c) makes clear that it contemplates two parallel sources—the provider’s website and the USCO directory—where each service provider’s DMCA agent information is readily available to the public. For a service provider to fulfill only one of these two requirements is insufficient.”); *Oppenheimer v. Allvoices, Inc.*, No. C 14–00499 LB, 2014 WL 2604033, at *6 (N.D. Cal. June 10, 2014) (holding the DMCA inapplicable to conduct that pre-dated the defendant’s registration of its DMCA agent with the U.S. Copyright Office, in ruling on a motion to dismiss); *Nat’l Photo Group, LLC v. Allvoices, Inc.*, No. C–13–03627 JSC, 2014 WL 280391, at *4 (N.D. Cal. Jan. 24, 2014) (denying in part defendant’s motion to dismiss, noting that “Plaintiff’s claims predate Defendant’s DMCA protection since Defendant’s allegedly infringing activity began a number of weeks or months prior to Defendant’s DMCA registration”); *Perfect 10, Inc. v.*

In *Perfect 10, Inc. v. Yandex, N.V.*,²⁰ for example, Judge William Alsup of the Northern District of California held that overseas entities were not entitled to DMCA safe harbor protection for notices sent prior to the time that they registered their DMCA agents with the U.S. Copyright Office, over objections that the service providers had received and processed DMCA notices without having a registered agent and substantially complied with the requirements of the statute. The court reasoned that 17 U.S.C.A. § 512(c)(2) provides that the DMCA safe harbor applies “*only if* the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, . . .” the name and contact information of the agent.²¹

The *Yandex* court, however, did not thoroughly consider whether submission of information to the Copyright Office, as opposed to designation of an agent, necessarily must oc-

Yandex, N.V., No. C 12-01521, 2013 WL 1899851, at *7 (N.D. Cal. May 7, 2013) (granting partial summary judgment for the plaintiff on Yandex’s ineligibility for the DMCA user storage safe harbor for alleged infringement that occurred prior to the date Yandex registered its DMCA agent with the U.S. Copyright Office); *Datatech Enterprises LLC v. FF Magnat Ltd.*, No. C 12-04500 CRB, 2012 WL 4068624, at *4 (N.D. Cal. Sept. 14, 2012) (granting a preliminary injunction based in part on the finding that the operator of an offshore file sharing cloud storage service was not likely to prevail on its DMCA defense with respect to 12,000+ alleged violations that occurred prior to June 15, 2011, which was the date it registered its DMCA agent with the U.S. Copyright Office, and because it failed to enforce its repeat infringer policy).

In *Datatech Enterprises*, the court subsequently held that factual issues surrounding the defendant’s designation of a DMCA agent precluded the plaintiff from obtaining partial summary judgment on the issue of the defendant’s entitlement to the DMCA safe harbor but declined to dissolve its preliminary injunction order based on new evidence regarding agent designation where the record showed that the defendant had ignored copyright holders’ requests to remove specifically identified repeat infringers, including one individual who uploaded 1,600 separate copies of an infringing work. District Court Judge Charles Breyer accordingly reiterated that, independent of the issue of registration, the defendant was unlikely to prevail on its DMCA defense based on its failure to implement its repeat infringer policy. *Datatech Enterprises LLC v. FF Magnat Ltd.*, No. C 12-04500 CRB, 2013 WL 1007360, at *5–6 (N.D. Cal. Mar. 13, 2013).

²⁰*Perfect 10, Inc. v. Yandex, N.V.*, No. C 12-01521, 2013 WL 1899851, at *7 (N.D. Cal. May 7, 2013).

²¹17 U.S.C.A. § 512(c)(2) (emphasis added).

cur as a precondition to eligibility for the safe harbor. The DMCA statute refers to *designation*, not registration, as a precondition to safe harbor eligibility. If a service provider designates an agent to receive DMCA notifications on its website and begins substantial compliance with the DMCA so that copyright owners may submit DMCA notifications to the agent to have infringing works removed, but the service provider does not notify the Copyright Office until some time later, the conclusion that DMCA protection is only available as of the date notice is provided to the Copyright Office, and not prior to that time when an agent was identified on the service provider's website (where most people look to see if a service provider has designated an agent) is not necessarily compelled by the plain terms of the statute.

Even if designation requires identification of the agent on both the service provider's website and with the U.S. Copyright Office, it does not necessarily follow that when both steps have been completed protection does not relate back to the initial act of designation. Section 512(c)(2) uses the terminology "only if" not "only when" in describing the preconditions for safe harbor protection. By analogy, the Copyright Act generally requires registration of a copyright as a precondition to filing suit, but allows a copyright owner to sue for infringement that pre-dates registration, but only after a copyright has been registered.²² It does not necessarily follow that if the technical requirements for designation of an agent occur at different times, protection is only available as of the last date when the last of the requirements set forth in section 512(c)(2) have been met—especially given that notice to the Copyright Office arguably is the least important of the specific requirements set forth in section 512(c)(2).

In *Disney Enterprises, Inc. v. Hotfile Corp.*,²³ Judge Kathleen M. Williams of the Southern District of Florida followed *Yandex* in ruling, as alternative grounds for denying safe harbor protection to Hotfile, an overseas file storage site adjudged ineligible for failing to reasonably implement its repeat infringer policy, that Hotfile would have been ineligible for the safe harbor for any acts of infringement that occurred on Hotfile prior to May 2010, which was the date on

²²See *infra* § 4.19[1].

²³*Disney Enterprises, Inc. v. Hotfile Corp.*, Case No. 11-20427-Civ, 2013 WL 6336286 (S.D. Fla. Sept. 20, 2013).

which it published its DMCA agent's contact information on its website. In *Hotfile*, the service provider had an "abuse report" form on its website and provided an email address for users to report infringing content for many years, but did not register a DMCA agent with the Copyright Office until December 2009 and did not identify the agent on its website until May 2010. Judge Williams conceded that the statute "focuses on whether someone with an infringement complaint would be able to contact the company . . .," but nonetheless followed *Yandex* in holding that DMCA protection was unavailable until the agent was both identified in a Copyright Office filing and on the defendant's website.

Yandex and *Hotfile* underscore a potential conundrum faced by foreign website owners and service providers that potentially could comply with the DMCA but may not otherwise be doing business in the United States. If a foreign site registers a DMCA agent with the U.S. Copyright Office, this act could be viewed as evidencing purposeful availment of the privileges and benefits of doing business in the United States and/or targeting the U.S. market, which could increase the chance that of being found subject to personal jurisdiction in the United States.²⁴ On the other hand, if the entity does not register its agent with the U.S. Copyright Office and otherwise is held subject to personal jurisdiction in the United States, under *Yandex* and *Hotfile* it could be deprived of any safe harbor defense even if it substantially complies with the requirements of the statute.

4.12[9][B] Notifications (and Service Provider Obligations in Response to Notifications)

A notification must be "a written communication" directed to the service provider's designated agent. This requirement may be satisfied by an email message since the signature requirement (discussed below) allows for electronic, as well as physical, signatures.¹

In response to a notification, a service provider's obliga-

²⁴See *infra* chapter 53 (analyzing personal jurisdiction over U.S. and foreign entities).

[Section 4.12[9][B]]

¹17 U.S.C.A. § 512(c)(3)(A). Since the time the DMCA was enacted, Congress passed the federal e-SIGN statute, which significantly liberalized the standards for electronic signatures. See 15 U.S.C.A. §§ 7001 *et seq.*; *infra* § 15.02[2].

tions will vary depending on the type of infringement alleged. A service provider must *expeditiously* remove or disable access to allegedly infringing material that has been cached, but only if the material first was removed from the originating site (or access to it was blocked).² A service provider likewise must respond *expeditiously* to remove or disable links or similar information location tools³ or material stored on its system or network at the direction of a user.⁴

There is little case law on what constitutes an *expeditious* response. In *Long v. Dorset*,⁵ Judge Hamilton of the Northern District of California, in granting a motion to dismiss a complaint that alleged that Facebook was not entitled to DMCA safe harbor protection, ruled that Facebook acted expeditiously in removing over 100 images (and also responding to plaintiff's demand that his rights as an administrator be restored) within five business days, where "Facebook promptly responded to plaintiff's initial email and, over the next several days, continued to exchange emails with plaintiff to resolve the issue." In *Capitol Records, LLC v. Vimeo, LLC*,⁶ Judge Ronnie Abrams of the Southern District of New York held that Vimeo was not obligated to disable access to or remove material in response to notices that were not substantially complying but in any case expeditiously removed videos where it took down material on the same day on two occasions and within three and a half weeks in response to a notice that covered 170 videos. It is unclear whether other courts would agree that three and a half weeks represents an *expeditious* response, even to a notice that identifies 170 videos, although the inadequacy of notice and speed of removing at least some of the videos may have come into play. Other courts have approved shorter response times as expeditious without suggesting that longer time periods would not have been permissible.⁷ By contrast, a two month delay in removing material was found not to be

²See 17 U.S.C.A. § 512(d)(2)(E).

³See 17 U.S.C.A. § 512(d)(3).

⁴17 U.S.C.A. § 512(c)(3).

⁵*Long v. Dorset*, 369 F. Supp. 3d 939, 944-47 (N.D. Cal. 2019).

⁶*Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 535-36 (S.D.N.Y. 2013), *aff'd in part on other grounds*, 826 F.3d 78 (2d Cir. 2016).

⁷See, e.g., *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 732-34, 746-47 (S.D.N.Y. 2012) (holding that Photobucket was protected by the safe harbor where it disabled access to material identified in substantially complying notifications within five days or less, finding

expeditious.⁸ An 18 to 23 day turnaround for removing infringing items was likewise found to not be expeditious, in an unreported opinion finding other grounds to deny DMCA safe harbor protection to a defendant, where the defendant initially assured the copyright owner that it would act within 24 hours, plaintiff made test purchases of items bearing the infringing images during the period of delay, and the defendant falsely represented that no sales had taken place.⁹

Where a notification relates to material stored at the direction of a user who is also a subscriber and the service provider seeks to benefit from the exemption set forth in subpart 512(g)(2), the service provider also must take reasonable steps to *promptly* inform its subscriber (i.e., the alleged infringer) that it has removed or disabled access to the material described in the notification¹⁰ and comply with the more complex rules governing counter notification,¹¹ which are discussed below in section 4.12[9][C]. A service provider

notifications that did not include URLs to be noncomplying and holding that Photobucket had no ongoing obligation to proactively search for other copies of the same works identified in the earlier DMCA notices), *aff'd mem.*, 569 F. App'x 51 (2d Cir. 2014).

⁸See *Rosen v. Global Net Access, LLC*, No. 10-2721-DMG (E), 2014 WL 2803752, at *4–5 (C.D. Cal. June 20, 2014) (holding that a delay in removing photographs identified in a DMCA notice for more than two months, until after the defendant was served with a copy of the complaint in the lawsuit, was not *expeditious* within the meaning of the DMCA).

⁹See *Feingold v. RageOn, Inc.*, 472 F. Supp. 3d 94, 102 (S.D.N.Y. 2020) (granting summary judgment for the plaintiff-photographer on her claim for copyright infringement, writing that “[i]n this context—and, particularly, in light of Defendant’s initial assurance that it would act within 24 hours—Defendant’s efforts to remove the infringing items cannot be considered expeditious.”).

¹⁰17 U.S.C.A. § 512(g)(2)(A) (emphasis added).

¹¹See 17 U.S.C.A. § 512(g)(2). Subpart (g)(2)—which imposes potentially burdensome requirements on service providers to transmit notifications to certain alleged infringers and accept and process counter notifications in order to enjoy an exemption from liability—applies where content residing at the direction of a subscriber is removed (or access to it is blocked) based on a service provider’s good faith belief that the material in question is infringing. The subscriber content removed will be material stored at the direction of a user within the meaning of the user storage limitation set forth in subpart (c)(3). It is possible, however, that a service provider, to limit its potential liability for copyright infringement in response to a notification, could remove user content that was not stored by a subscriber within the meaning of subpart (g)(2), in which case the service provider would not need comply with the requirements of subpart (g)(2) in order to be exempt from any liability for removing or disabling ac-

that fails to comply with these additional requirements may still enjoy limited liability for copyright infringement under section 512(c) for material stored at the direction of a user even though it would not be exempt from potential liability to its subscriber under subpart 512(g)(2) for removing or disabling access to material which in good faith is believed to be infringing.

In *Hendrickson v. Amazon.com, Inc.*,¹² Judge Hatter of the Central District of California ruled in a case of first impression that a notification is only effective with respect to material on a site “at the time the ISP receives the notice” and cannot impose a continuing obligation on the recipient-service provider to monitor its location for future acts of infringement. In *Amazon.com, Inc.*, the plaintiff sent a substantially complying notification to *Amazon.com* on Jan. 28, 2002, stating that as copyright owner he had never authorized a DVD release of the movie *Manson*. He subsequently sued *Amazon.com, Inc.*, for a third-party listing of a DVD version of *Manson* that he noticed on the Amazon site on Oct. 21, 2002—almost nine months after the time he sent the notification. Judge Hatter ruled that although the January 2002 notice was “adequate for the listings then on Amazon,” “there is a limit to the viability of an otherwise adequate notice.” The January 2002 notification could not “be deemed adequate notice for subsequent listings and sales, especially, as here, when the infringing item was posted for sale nine months after the date of notice.”¹³ Citing legislative history, Judge Hatter wrote:

The DMCA places the burden on the copyright owner to moni-

cess to such content. Although the terms are not defined, *subscribers* should be thought of potentially as a subset of a service provider’s users. Except where subscriber content is removed (or access to it disabled) in response to a formal notification (in which case the requirements of subpart (g)(2) must be met to benefit from the exemption), service providers are exempt pursuant to subpart (g)(1) from any liability for removing or disabling access to material believed in good faith to be infringing. Thus, where a service provider acts on its own initiative, in response to a third-party complaint or in response to a notification that does not involve subscriber content stored by a user within the meaning of subpart (c)(3), it will be exempt, pursuant to subpart (g)(1), from any liability for removing or disabling access to content believed in good faith to be infringing.

¹²*Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914 (C.D. Cal. 2003).

¹³*Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 917 (C.D. Cal. 2003).

tor the Internet for potentially infringing sales. “[A] service provider need not monitor its service or affirmatively seek facts indicating infringing activity.” House Report No. 551(II), 105th Congress, 2d Session 1998, H.R. at 53. To allow a plaintiff to shift its burden to the service provider would be contrary to the balance crafted by Congress. “The goal of § 512 (c)(3)(A)(iii) is to provide the service provider with adequate information to find and examine the allegedly infringing material expeditiously.” H.R. at 55.¹⁴

¹⁴*Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 916 (C.D. Cal. 2003); *see also EMI Christian Music Group, Inc. v. MP3Tunes, LLC*, 844 F.3d 79, 89 (2d Cir. 2016) (“the DMCA explicitly relieves service providers from having to affirmatively monitor their users for infringement”); *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 94, 98 (2d Cir. 2016) (“§ 512(m) makes clear that the service provider’s personnel are under no duty to ‘affirmatively seek[]’ indications of infringement.”); “§ 512(m) relieves the service provider of obligation to monitor for infringements posted by users on its website.”); *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 35 (2d Cir. 2012) (“Section 512(m) is explicit: DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider. For that reason, § 512(m) is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that infringement may be occurring.”); *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 603 (9th Cir. 2018) (“The Digital Millennium Copyright Act places the burden of policing infringement on the copyright owner, not on the person or firm storing and hosting the material.”); *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1022 (9th Cir. 2013) (holding that the burden of policing for infringement is on the copyright owner; “Copyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers like Veoh, who cannot readily ascertain what material is copyrighted and what is not.”); *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir.) (“The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright.”), *cert. denied*, 522 U.S. 1062 (2007); *Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 733, 746–47 (S.D.N.Y. 2012) (rejecting plaintiff’s contention that the defendant was required to proactively search for copies of the same work in the future once a notification is sent), *aff’d mem.*, 569 F. App’x 51 (2d Cir. 2014).

In *Hendrickson*, Judge Hatter concluded that because the language of the statute is in the present tense, “it clearly indicates that Congress intended for the notice to make the service provider aware of the infringing activity that is occurring at the time it receives the notice.” *Hendrickson v. Amazon.com, Inc.*, 298 F. Supp. 2d 914, 917 (C.D. Cal. 2003). Moreover, he wrote:

The purpose behind the notice is to provide the ISP with adequate information to find and examine the allegedly infringing material expeditiously. H.R. at 55. If the infringing material is on the website at the time the ISP receives the no-

Under the statute, a notification must include:

- (i) A physical or electronic signature of a person authorized to act on behalf of the copyright owner or exclusive licensee.
- (ii) Identification of the copyrighted work claimed to be *infringed*. If a notice refers to multiple works posted at a single location, it is sufficient to include a representative list of works infringed at the site.
- (iii) Identification of the material claimed to be *infringing* together with “information reasonably sufficient to permit the service provider to locate the material.” For purposes of the information location tools limitation, the notification must also identify the reference or link to the material or activity claimed to be infringing and information “reasonably sufficient” to permit the service provider to locate the reference or link.
- (iv) Information “reasonably sufficient” to permit the service provider to contact the complaining party. Such information may include the complaining party’s address, telephone or email address.
- (v) A statement that the complaining party believes, in good faith,¹⁵ that the copyrighted material identified is being used in a manner that is not authorized¹⁶ by “the copyright owner, its agent, or the law.”

tice, then the information, that all Manson DVD’s are infringing, can be adequate to find the infringing material expeditiously. However, if at the time the notice is received, the infringing material is not posted, the notice does not enable the service provider to locate infringing material that is not there, let alone do it expeditiously.

Hendrickson v. Amazon.com, Inc., 298 F. Supp. 2d 914 (C.D. Cal. 2003).

¹⁵In *Rossi v. Motion Picture Ass’n of America Inc.*, 391 F.3d 1000 (9th Cir. 2004), *cert. denied*, 544 U.S. 1018 (2005), the Ninth Circuit ruled that the “good faith belief” requirement in § 512(c)(3)(A)(v) encompasses a subjective, rather than an objective, standard.

¹⁶In *Lenz v. Universal Music Corp.*, 815 F.3d 1145 (9th Cir. 2016), the Ninth Circuit held that section 512(c)(3)(A)(v) requires a copyright owner to consider fair use in formulating a good faith belief that “use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.” The court ruled that a copyright owner need only have a subjective good faith belief that the material at issue in a DMCA notice is not entitled to fair use, but a copyright owner faces liability if it knowingly misrepresents in a takedown notice that it had formed a good faith belief that the material was not authorized by law without considering fair use. As explained by the court in *Lenz*, “[t]his in-

- (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.¹⁷

All six requirements do not necessarily have to be met for a particular notification to be considered valid. The Act merely requires that “substantially” all of the six categories of information be provided.¹⁸ While Congress did not specifically define what would constitute substantial compliance, a notification that only satisfies the second, third and fourth requirements apparently is not sufficient, based on a later provision of the Act which refers to a notice that “fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii) and

quity lies not in whether a court would adjudge the video as a fair use, but whether Universal formed a good faith belief that it was not.” *Id.* at 1153. The majority further explained that if

a copyright holder forms a subjective *good faith* belief the allegedly infringing material does not constitute fair use, we are in no position to dispute the copyright holder’s belief even if we would have reached a different conclusion. A copyright holder who pays lip service to the consideration of fair use by claiming it formed a good faith belief when there is evidence to the contrary is still subject to § 512(f) liability.

Id. at 1154.

The Ninth Circuit further clarified that liability could be imposed based on willful blindness if a copyright owner (1) subjectively believed there was a high probability that the subject of a DMCA notice constituted a fair use, and (2) took deliberate action to avoid learning of this fair use. *Id.* at 1155, citing *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754 (2011); see generally *supra* § 4.11[6][A] (analyzing the case in greater detail in the context of liability for copyright infringement); *infra* § 4.12[6][C] (analyzing *SEB* and willful blindness in the context of knowledge or awareness that could disqualify a service provider from DMCA safe harbor protection).

Where liability may be found, the Ninth Circuit held that even if an affected user has incurred no monetary loss the user may recover nominal damages for a knowing material misrepresentation under section 512. *Id.* at 1156–57 (discussing nominal awards in tort cases). The appellate court declined, however, to decide the scope of recoverable damages, including “whether she may recover expenses following the initiation of her § 512(f) suit or *pro bono* costs and attorneys’ fees, both of which arose as a result of the injury incurred.” *Id.* at 1157; see *infra* §§ 4.12[9][D], 4.12[9][F] (discussing the case at greater length).

¹⁷17 U.S.C.A. § 512(c)(3)(A) (emphasis added).

¹⁸See 17 U.S.C.A. § 512(c)(3).

(iv).¹⁹ Congress thus apparently believed that some level of authentication was required in order for a notification to be in substantial compliance since elements (i), (v) and (vi) relate, respectively, to the requirements for a signature, a good faith statement that the material in question is infringing, verification of the accuracy of the notification and certification under penalty of perjury that the person lodging the notification is authorized to do so.²⁰

A notification that is not a “written communication provided to the designated agent of a service provider” would be defective, although it is unclear whether a notice complying with all six content requirements would be found to be in substantial compliance if it were directed to someone other than the designated agent. Presumably, Congress would not have required agent designation and the publication of lists of designated agents if the requirement that notice be provided to *a designated agent* had not been considered important. Failure to submit notification to the designated agent therefore may make a notification fatally defective (at least absent evidence of actual receipt by the service provider).

In *ALS Scan, Inc. v. RemarQ Communities, Inc.*,²¹ the Fourth Circuit ruled that ALS Scan, the owner of copyrights in adult content, substantially complied with the notification requirement of the DMCA when it sent RemarQ a notification that (1) identified two Usenet groups—alt.als and alt.binaries.pictureserotica.als—that it alleged had been created solely for the purpose of publishing ALS Scan’s copyrighted works, (2) asserted that virtually all of the images on the two sites constituted infringing copies of its

¹⁹17 U.S.C.A. § 512(c)(3)(B)(ii).

²⁰Although the issue was not thoroughly or carefully considered, the court in *Brave New Films 501(c)(4) v. Weiner*, 626 F. Supp. 2d 1013 (N.D. Cal. 2009) wrote that no authority had been presented by a defendant to suggest that a letter that otherwise met the requirements of a DMCA notification was not substantially complying merely because it did not include a statement that the sender had a good faith belief that the defendant’s use of plaintiff’s work was unauthorized. The issue of substantial compliance, although decided by the court, in fact was not relevant to the question of whether the plaintiff had stated a claim for misrepresentation under section 512(f), which does not in fact require that a notification be substantially compliant to be actionable. *See generally infra* § 4.12[9][D] (discussing the case in the context of section 512(f)).

²¹*ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001).

copyrighted photographs (and noted that material could be identified as ALS Scan's material because the images included reference to ALS Scan's name and/or copyright symbol), and (3) referred RemarQ to two URLs where RemarQ could find pictures of ALS Scan's models and obtain copyright information.²² Although the district court had ruled that the notice was deficient, the Fourth Circuit concluded that it substantially complied with the notification requirement of providing a "representative list" of potentially infringing material²³ as well as information "reasonably sufficient"²⁴ to enable RemarQ to locate the infringing material.²⁵ Accordingly, the court ruled that RemarQ had been given notice of infringement and failed to act, and was therefore not entitled to the DMCA's liability limitations.²⁶

²²RemarQ had responded to the notification by advising that it would eliminate individual infringing items if ALS Scan identified them "with sufficient specificity." ALS Scan objected that over 10,000 copyrighted images belonging to ALS Scan had been included in the newsgroups over a period of several months.

²³As previously noted, 17 U.S.C.A. § 512(c)(3)(A)(ii) provides that "[i]f a notice refers to multiple works posted at a single location, it is sufficient to include a representative list of works infringed at the site."

²⁴See 17 U.S.C.A. § 512(c)(3)(A)(iii) (providing that a notification must include "information reasonably sufficient to permit the service provider to locate the material.").

²⁵*ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 625 (4th Cir. 2001). RemarQ had argued that the notice was insufficient to identify the infringing works because the Usenet groups in question also included text commentaries and appeared to include non-ALS Scan photographs, in addition to works owned by ALS Scan. The two newsgroups at issue, however, included ALS Scan's name, which ALS Scan cited in arguing that the groups had been created solely for the purpose of publishing and exchanging ALS Scan images (which ALS Scan did not license for this purpose). *ALS Scan, Inc. v. RemarQ Communities, Inc.* is perhaps best understood as a case involving allegations of infringement on a massive scale, where the very names of the Internet locations betrayed that they had been created for the purpose of infringing plaintiff's works. Although not directly relevant, the Fourth Circuit may also have been influenced by the fact that America Online, Erol's and Mindspring apparently responded to equivalent notices by blocking access to the two Usenet groups. See *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619, 621 (4th Cir. 2001). The decision was not well received by some service providers, because RemarQ was not actually hosting the newsgroups. Unlike websites, newsgroups do not reside on a single server. The DMCA, however, does not distinguish between hosts, content providers or access providers in its treatment of service providers.

²⁶See *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619 (4th

In *Perfect 10, Inc. v. CCBill, LLC*,²⁷ the Ninth Circuit found notifications sent by Perfect 10 to a Web host and payment processor did *not* substantially comply with the requirements of the DMCA. Perfect 10 had argued that it met the requirements for substantially complying notifications through a combination of three sets of documents: (1) a 22,185-page bates-stamped production that included pictures with URLs of Perfect 10 models allegedly posted on the websites of defendants' clients, but which did not contain a statement submitted under penalty of perjury that the complaining party was authorized to act; (2) a spreadsheet identifying the Perfect 10 models revealed in the first set of documents, which was sent approximately nine months later; and (3) interrogatory responses that incorporated by reference the spreadsheet and which was signed under penalty of perjury approximately two and a half months later. The Ninth Circuit ruled that each document was defective because section 512(c)(3) contemplates " 'a written communication' Permitting a copyright holder to cobble together adequate notice from separately defective notices . . . unduly burdens service providers."²⁸ The court emphasized that "[t]he DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright. We decline to shift a substantial burden from the copyright owner to the provider; Perfect 10's separate communications are

Cir. 2001) ("The DMCA's protection of an innocent service provider disappears at the moment the service provider loses its innocence, i.e., at the moment it becomes aware that a third party is using the system to infringe."). The Fourth Circuit reversed and remanded the case, reinstating ALS Scan's claim against RemarQ for direct infringement. Although the court ruled that RemarQ was not entitled to the protections afforded by the DMCA's safe harbor provisions and reversed the lower court's entry of summary judgment for RemarQ, it declined to reverse the lower court's order denying summary judgment for ALS Scan, and instead remanded the case for further proceedings, finding that ALS Scan's contentions that the sole purpose of the newsgroups, and that "virtually all" of the images posted on the newsgroups are infringing, constituted disputed facts that precluded the entry of summary judgment.

²⁷*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

²⁸*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1112-13 (9th Cir.) (emphasis in original), cert. denied, 522 U.S. 1062 (2007).

inadequate.”²⁹

In a later Ninth Circuit case, *Luvdarts, LLC v. AT&T Mobility, LLC*,³⁰ the court held that mobile phone carriers could not be held secondarily liable for copyright infringement for user text messages that allegedly attached infringing copies of plaintiff’s works where the notices sent to the carriers failed to qualify as proper notifications under the DMCA. In *Luvdarts*, the notices were 150-page long lists of copyrighted works owned by the plaintiff along with a request for “accountability” for unauthorized distribution of those titles for the period from May 2008 to November 2009, which did not identify “which of these titles were infringed, who infringed them, or when the infringement occurred.”³¹ In short, they “failed to notify the Carriers of any meaningful fact.”³²

In *Wolk v. Kodak Imaging Network, Inc.*,³³ Judge Robert Sweet of the Southern District of New York held that notifications sent to Photobucket that did not include URLs did not comply with the requirements of the statute.³⁴ Subsequently, the Ninth Circuit implied, without expressly

²⁹*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1113 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

³⁰*Luvdarts, LLC v. AT&T Mobility, LLC*, 710 F.3d 1068 (9th Cir. 2013).

³¹*Luvdarts, LLC v. AT&T Mobility, LLC*, 710 F.3d 1068, 1073 (9th Cir. 2013).

³²*Luvdarts, LLC v. AT&T Mobility, LLC*, 710 F.3d 1068, 1072 (9th Cir. 2013).

³³*Wolk v. Kodak Imaging Network, Inc.*, 840 F. Supp. 2d 724, 746–47 (S.D.N.Y. 2012), aff’d mem., 569 F. App’x 51 (2d Cir. 2014).

³⁴In an unreported decision, *Perfect 10, Inc. v. Yandex, N.V.*, No. C 12-01521, 2013 WL 1899851 (N.D. Cal. May 7, 2013), a court approved of the sufficiency of DMCA notices that provided only truncated URLs, where the full URLs could be manually extracted by the service provider by right clicking on PDF files provided. The opinion, however, does not cite to *Wolk* or any of the many other cases addressing the sufficiency of DMCA notices, other than *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1112–13 (9th Cir.), cert. denied, 522 U.S. 1062 (2007), which, ironically, is cited for the proposition that a DMCA notice may not be proper if it requires a service provide to “take substantial time to piece together the relevant information for each instance of claimed infringement.” See *Perfect 10, Inc. v. Yandex, N.V.*, No. C 12-01521, 2013 WL 1899851, at *3 (N.D. Cal. May 7, 2013). Given that Perfect 10 has a long history of sending notices to service providers that are intended to make it difficult for the service provider to easily locate and remove material, as detailed in various court opinions, the court in *Yandex* should have at least given more serious consideration to whether Perfect 10’s provision of truncated URLs (which are impossible

holding, that URLs satisfied the requirement for “information reasonably sufficient to permit the service provider to locate the material” within the meaning of 17 U.S.C.A. § 512(c)(3)(A)(iii), where the service at issue hosted more than a half-million videos and the videos at issue did not contain information identifying the plaintiff as the copyright owner.³⁵

In *Hendrickson v. eBay, Inc.*,³⁶ the plaintiff’s failure to authenticate a notification sent to eBay by including a written statement under penalty of perjury substantiating the accuracy of the notification (section 512(c)(3)(A)(vi)) or certifying that he had “a good faith belief that use of the material in the manner complained of” was not authorized (section 512(c)(3)(A)(v)) rendered it defective.

The court in *Hendrickson* also found the plaintiff’s notification insufficient under section 512(c)(3)(A)(iii) to identify the various listings that purportedly offered pirated copies of his work. In response to plaintiff’s notice, eBay had asked for the specific item number(s) to facilitate locating them. The court wrote that it recognized that “there may be instances where a copyright holder need not provide eBay with specific numbers to satisfy the identification requirement.”³⁷ It concluded, however, that specific items numbers were neces-

to use to locate a web page) was intended to thwart the service provider’s efforts at locating and removing the allegedly infringing material and cause it to “take substantial time to piece together relevant for information for each instance of claimed infringement.” The court ruled that section 512(c)(3) does not require any particular format for DMCA notices and likely was influenced by the fact that Perfect 10’s notices in *Yandex* improved upon the abysmal notices rejected by the Ninth Circuit in *CCBill*. Nevertheless, the *Yandex* court should have considered the context in which truncated URLs were provided in evaluating whether the notices satisfied *ccBill*. In light of the plaintiffs’ record of sending deficient notices, the fact that it was on notice about what was required based on its prior experience litigating the sufficiency of DMCA notices and given that it could easily have provided a list of complete URLs, the sufficiency of Perfect 10’s notice in *Yandex* at a minimum deserved closer scrutiny.

³⁵See *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 612 (9th Cir. 2018) (holding that a service provider acted expeditiously in removing video clips where the plaintiff provided no advance notice before filing suit and initially ignored a request from the service provider to provide URLs, where the service provider removed files on the same day that the copyright owner eventually provided the URLs).

³⁶*Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001).

³⁷As an example, the court wrote that “if a movie studio advised eBay that all listings offered to sell a new movie (e.g., “Planet X,”) that has not

sary in this case to allow eBay to identify the problematic listings.³⁸ It also rejected the argument that information allegedly communicated orally to eBay was relevant, since a notification must be in writing.

In *UMG Recordings, Inc. v. Veoh Networks, Inc.*,³⁹ the court held that a notice from the RIAA that identified UMG artists, but not their works, and not the files on Veoh's site that allegedly infringed those works, was deficient. In that case, UMG had relied on *dicta* from *Hendrickson v. eBay, Inc.*, in which the court had hypothesized that "if a movie studio advised eBay that all listings offering to sell a new movie . . . are unlawful, eBay could easily search its website using the title . . . and identify the offensive listings."⁴⁰ Judge Matz, however, held that UMG's "reliance on this *dictum*" was misplaced.⁴¹ "Here, the RIAA's notices did not identify titles of infringing videos. Nor did they advise Veoh that all videos by a certain artist, let alone all videos that would turn up in a search of an artist's name on Veoh's system, were infringing."⁴² Although not specifically discussed in the context of notice, the court, elsewhere in its opinion, had noted that at least some of the artists identified in RIAA notices as UMG artists also recorded music for Sony-BMG, which had licensed its music videos to Veoh.

In *Viacom Int'l Inc. v. YouTube, Inc.*,⁴³ Judge Stanton of the Southern District of New York followed *Veoh* in rejecting Viacom's argument that YouTube was not entitled to DMCA

yet been released in VHS or DVD format are unlawful, eBay could easily search its website using the title "Planet X" and identify the offensive listings.

³⁸Among other things, the court noted that the plaintiff had never explained what distinguished an infringing copy from a genuine one.

³⁹*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1110 (C.D. Cal. 2009), *aff'd on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁴⁰*Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1090 (C.D. Cal. 2001).

⁴¹*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1110 (C.D. Cal. 2009), *aff'd on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁴²*UMG Recordings, Inc. v. Veoh Networks Inc.*, 665 F. Supp. 2d 1099, 1110 n.14 (C.D. Cal. 2009), *aff'd on other grounds sub nom. UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013).

⁴³*Viacom Int'l Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010), *aff'd in relevant part on other grounds*, 676 F.3d 19 (2d Cir. 2012).

protection because it removed only the specific clips identified in DMCA notices, rather than other clips that also infringed the same works. The court held that a copyright owner, in meeting the statutory requirement for providing “information reasonably sufficient to permit the service provider to locate the material,” must provide specific information, such as a copy or description of the material and a URL, rather than merely a generic description.

In *Perfect 10, Inc. v. Giganews, Inc.*,⁴⁴ Judge Audrey Collins of the Central District of California denied plaintiff’s summary judgment motion based on the insufficiency of the five DMCA takedown notices that plaintiff had sent to the defendant, which were comprised of search instructions, thumbnail images and screen shots of Usenet posts. The court found these notices to be inadequate because the results lists did not specifically identify infringing items (as opposed to merely search results) and because material accessible through the Usenet is in a constant state of flux the images and search instructions did not meet the requirements of section 512(c)(3)(A)(iii). The notices likewise did not provide “information reasonably sufficient to permit the service provider to locate the material” In contrast to providing Message IDs, which would have allowed Giganews to locate the material at issue, Judge Collins characterized plaintiff’s practice as a “Rube Goldberg method of locating messages”⁴⁵

A lower standard for substantial compliance may exist for notifications relating to information location tools, which as a practical matter may be easier for a service provider to identify and locate than certain types of material stored by

⁴⁴*Perfect 10, Inc. v. Giganews, Inc.*, 993 F. Supp. 2d 1192 (C.D. Cal. 2014).

⁴⁵*Perfect 10, Inc. v. Giganews, Inc.*, 993 F. Supp. 2d 1192, 1201 (C.D. Cal. 2014). The Ninth Circuit ultimately applied the same rationale in affirming summary judgment for Giganews on Perfect 10’s claim for contributory infringement, holding that plaintiff could not show a *material contribution* (or *actual* knowledge that *specific* infringing material was available using its system) where Perfect 10 had failed to provide machine readable Message—IDs and instead proposed that Giganews search the Usenet manually, which the court characterized as “onerous and unreasonably complicated.” *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 671 (9th Cir. 2017); see generally *supra* § 4.11[3][B].

users. In *Arista Records, Inc. v. MP3Board, Inc.*,⁴⁶ for example, a district court in New York held that a letter that named particular artists and songs, which was accompanied by printouts of screen shots of the defendant's service where relevant links had been highlighted and marked with an asterisk, was sufficient even though plaintiffs did not actually provide the specific URLs of the pages connected via the links.⁴⁷ Unlike the notices at issue in *Veoh*, the notifications in MP3Board at least identified the material alleged to be infringing.

If a notification is defective, it generally may not be cited as evidence that the service provider had knowledge or awareness of the infringement for purposes of the user storage limitation.⁴⁸ If, however, the notification at least includes substantially complying details of the allegedly infringed and infringing works and contact information to allow the service provider to contact the complainant,⁴⁹ the provider must disable access to or remove the material to benefit from this provision.⁵⁰

As a practical matter, the substantial compliance standard encourages service providers to respond even to defective notices in order to avoid a later judicial determination that a nonconforming notice nonetheless was in substantial compliance. A court generally may not consider whether a defective notice—which fails to comply substantially with the requirements of the Act—gave a service provider actual notice or awareness within the meaning of the user storage

⁴⁶*Arista Records, Inc. v. Mp3Board, Inc.*, No. 00 CIV. 4660(SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002).

⁴⁷An earlier letter that merely identified ten artists whose works had been infringed was deemed not to be substantially complying. See *Arista Records, Inc. v. Mp3Board, Inc.*, No. 00 CIV. 4660(SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002). For further discussion of this case, see *infra* § 4.12[9][F].

⁴⁸See 17 U.S.C.A. § 512(c)(3)(B)(i) (a notification that is not substantially complying “shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or if aware of facts or circumstances from which infringing activity is apparent”); see generally *supra* § 4.12[6][C].

⁴⁹These three requirements are set forth in sections 512(c)(3)(A)(ii), 512(c)(3)(A)(iii) and 512(c)(3)(A)(iv).

⁵⁰See 17 U.S.C.A. § 512(c)(3)(B)(ii); see generally *supra* § 4.13[6][B].

or information location tools limitations.⁵¹

Where a defective notice provided to a service provider's designated agent substantially complies with requirements (ii), (iii) and (iv), however, the notice may be cited as evidence that the service provider had knowledge of the infringement unless, upon receipt of the defective notice, the service provider promptly attempted to contact the person who submitted it "or takes other reasonable steps" to obtain notification that substantially complies with the statutory requirements.⁵² Where it does so, and the copyright owner refuses to provide the requested information, the service provider will not have liability for failing to act⁵³ (assuming that it was not mistaken in the first instance in concluding that additional information was required).

To avoid a finding that a service provider had actual knowledge or awareness based on a defective notice, service providers may find it easier simply to remove or block access to content reasonably described in a defective notice. If they do so, however, and if a notification relating to content stored at the direction of a user is later held to be substantially complying, they may run afoul of the requirements of subpart 512(g)(2) if they fail to serve a copy of the notification on a subscriber and thereby deny that party the ability to file a counter notification.⁵⁴ Thus, on balance, service providers may be best advised to respond to all defective notices by promptly notifying the complainant of the specific defects in the notification and urging prompt resubmission.

Service providers or affected users may publish notifications on the Internet. Google, for example, forwards copies of all notifications to *chillingeffects.org* (now *lumendatabase.org*), a site that publishes and archives legal

⁵¹17 U.S.C.A. § 512(c)(3)(B)(i).

⁵²17 U.S.C.A. § 512(c)(3)(B)(ii).

⁵³See *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1090–91 (C.D. Cal. 2001) (finding no liability where the plaintiff failed to cure defects in its notification to eBay, even after have been asked to do so by eBay).

⁵⁴As a practical matter, service providers may be able to limit their exposure to subscribers and account holders by contract in their subscriber agreements, ISP service agreement, Terms of Use or similar contracts. If a service provider will comply with the procedures for counter notifications, it is prudent to disclose in both the privacy policy and DMCA policy (or copyright section of Terms of Use) that copies of notifications will be sent to users accused of infringing activity. The sample DMCA policy found in the Appendix to this chapter includes such a provision.

notices.

Material misrepresentations in notifications may lead to liability under section 512(f) of the DMCA⁵⁵ or other theories of law.⁵⁶ The contents of notifications, however, may be protected against tort or other claims based on state law litigation privileges.⁵⁷

What it means to disable access to or remove material is addressed in section 4.12[6][C].

4.12[9][C] Counter Notification

Upon receipt of a notification, a service provider generally will be exempt from liability for removing or disabling access to allegedly infringing content in good faith.¹ However, this exemption will only apply with respect to material residing at the direction of a subscriber (i.e., material stored at the direction of a user which is removed in response to a notification sent pursuant to section 512(c)), where the user is also a subscriber under section 512(g)(2)), if the service provider “take[s] reasonable steps *promptly* to notify the subscriber that it has removed or disabled access to the material” and thereby allows the alleged infringer to respond to the notification. An accused infringer’s response is referred to in the statute as a “counter notification.”

There is no *obligation* to comply with the procedures for counter notification with respect to material removed pursuant to any other liability limitation, including information location tools.² Nor is there an obligation to comply with the procedures for counter notifications unless the material stored at the direction of a user was removed pursuant to a

⁵⁵See *infra* § 4.12[9][D].

⁵⁶See *infra* § 4.12[9][F].

⁵⁷See, e.g., Cal. Civil Code § 47(b) (statements made in judicial proceedings); *Maponics, LLC v. Wahl*, No. C07–5777 BZ, 2008 WL 2788282 (N.D. Cal. July 18, 2008) (discussing the potential applicability of California Civil Code section 47(b) to DMCA notices as “reasonably relevant” to “achieve the objects of the litigation,” but concluding that the emails at issue in that case did not meet the requirements of section 512(c)(3)(A) and “seem more like an attempt . . . to gain business from a customer by charging a competitor with theft, than an attempt to mitigate a customer’s damages.”).

[Section 4.12[9][C]]

¹17 U.S.C.A. § 512(g)(1).

²See *supra* § 4.12[7].

notification (as opposed to in response to the service provider's knowledge or red flag awareness), and even then only if the user is also a subscriber. Indeed, restoring access to material pursuant to counter notification procedures except where expressly authorized by the DMCA for material stored by a subscriber who submits a counter notification in accordance with the rules set forth in section 512(g)—could result in a service provider being held liable for copyright infringement.

Counter notification procedures nevertheless provide a service provider with a useful mechanism to avoid getting embroiled in user complaints. Users upset that their material has been removed are given a procedure to lodge a complaint (subject to sanctions for misrepresentations), while service providers who comply with procedures can deflect criticism if their removal and restoration decisions are dictated by statute, rather than discretion. Suits by users against service providers for material taken down typically are precluded by a service provider's Terms of Service contract or other user agreement.³ Nevertheless, compliance with counter notification procedures can be helpful for good

³*See, e.g., Darnaa, LLC v. Google LLC*, 756 F. App'x 674 (9th Cir. 2018) (affirming dismissal of plaintiff's suit arising out of YouTube's removal of plaintiff's music video from YouTube, based on YouTube's Terms of Service provision foreclosing damages from interruption or cessation of services); *Caraccioli v. Facebook, Inc.*, 700 F. App'x 588, 590 (9th Cir. 2017) (affirming dismissal of plaintiff's breach of contract and unfair competition claims against Facebook, where Facebook's Terms of Service agreement expressly disclaimed responsibility for content published by third parties on its social network), *aff'g*, 167 F. Supp. 3d 1056, 1064 (N.D. Cal. 2016); *Domen v. Vimeo, Inc.*, 433 F. Supp. 3d 592, 603-04 (S.D.N.Y. 2020) (dismissing plaintiff's claim for removing content, allegedly in bad faith, where the court found that removal pursuant to Vimeo's Terms of Service negated any conclusory allegation of bad faith, and therefore entitled Vimeo to Good Samaritan immunity under 47 U.S.C.A. § 230(c)(2)(A), for taking any action in good faith to restrict access to or the availability of particular types of content), *aff'd on other grounds*, No. 20-616-cv, 2021 WL 4352312 (2d Cir. Sept. 24, 2021); *King v. Facebook, Inc.*, Case No. 19-cv-01987-WHO, 2019 WL 6493968 (N.D. Cal. Dec. 3, 2019) (dismissing plaintiff's amended claim for retaliatory breach of contract because Facebook's Terms of Service agreement placed restrictions on users' behavior, but did not create affirmative obligations on Facebook, and gave it the right to terminate users "for any reason" and "in its sole discretion"); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1037-38 (N.D. Cal. 2019) (dismissing claims for breach of contract, breach of implied contract, breach of the implied covenant of good faith and fair dealing, quasi contract, and breach of confidence, where Facebook's Terms of Service included a limitation-of-liability clause); *Young v. Facebook, Inc.*, No. 5:10–

customer relations.

Like a notification, a counter notification, to be considered proper, must be “a written communication provided to the service provider’s designated agent” and satisfy certain content requirements. Specifically, a counter notification must include:

- (1) A physical or electronic signature of the alleged infringer;
- (2) Identification of the material that was removed or disabled by the service provider and the location where the material appeared before it was removed or access to it was disabled;
- (3) A statement under penalty of perjury that the alleged infringer has a good faith belief that the material at issue was mistakenly removed or misidentified; and
- (4) The alleged infringer’s name, address, and telephone number and a statement that the alleged infringer consents to the jurisdiction of the federal district court for the judicial district in which the address it provides is located and that it will accept service of process from the person who provided the original notification. If the alleged infringer is located outside the United States, the alleged infringer must include a statement that it consents to the jurisdiction of any U.S. federal district court in which the service provider may be found.⁴

As noted above, an internet user who submits a counter notification must consent to jurisdiction of a federal district court (pursuant to section 512(g)(3)), even though a copyright owner who submits a notification is not similarly

cv–03579–JF/PVT, 2010 WL 4269304, at *3, (N.D. Cal. Oct. 25, 2010) (dismissing plaintiff’s breach of contract claim); *Lewis v. YouTube, LLC*, 244 Cal. App. 4th 118, 125-26, 197 Cal. Rptr. 3d 219 (6th Dist. 2015) (sustaining YouTube’s demurrer without leave to amend, holding that the limitation of liability clause in YouTube’s terms of service contract precluded the plaintiff from establishing the damages element of her breach of contract claim and further holding that YouTube’s TOS did not require it to continue displaying comments or an accurate view count for user’s videos); *see generally infra* § 22.05[2][F] (analyzing the enforceability of liability limitations and other provisions in internet and mobile Terms of Service agreements).

⁴17 U.S.C.A. § 512(g)(3).

required to consent to jurisdiction.⁵

The purpose for this requirement is to put teeth in the process for seeking restoration of material taken down in response to a DMCA notification. A user must not only certify to its good faith belief that the material at issue was mistakenly removed or misidentified, under penalty of perjury and threat of sanctions under 17 U.S.C.A. § 512(f) for misrepresentations, but it must consent to jurisdiction so that a copyright owner can easily file suit if it chooses to do so, to prevent the material from being put back up.

A counter notification—like a notification—need only “substantially” include the information required by the statute.⁶

Upon receipt of a counter notification, a service provider must promptly provide the original complainant with a copy of the counter notification and notice that it will replace the removed material or cease disabling access to it within ten (10) business days. The original complainant must then file suit within the ten day period to obtain an order restraining the subscriber from engaging in infringing activity if it wants to prevent access to the material from being restored. Absent evidence that a lawsuit has been filed “seeking a court order to restrain the subscriber from engaging in infringing activity . . .” a service provider is required by the Act to “replac[e] the removed material and cease disabling access to it not less than ten, nor more than fourteen, business days following receipt of the counter notice.”⁷ It is noteworthy that the statute merely requires notice of a court action being filed—rather than evidence that litigation has commenced or the entry of a court order—in order to trigger the service provider’s obligation to maintain its blocking of the material.

Pursuant to the Copyright Alternative in Small-Claims Enforcement Act of 2020—known colloquially as the CASE Act¹—infringement claims or counterclaims initiated with the Copyright Claims Board may also suffice to meet the

⁵See 17 U.S.C.A. § 512(c)(3); *Doe v. Geller*, 533 F. Supp. 2d 996, 1011 (N.D. Cal. 2008) (“That difference must be viewed as intentional If that result seems asymmetrical and unfair, then the problem should be resolved by Congress, not this court.”) (dismissing plaintiff’s claim arising out of a notification, for lack of personal jurisdiction).

⁶See 17 U.S.C.A. § 512(g)(3).

⁷17 U.S.C.A. § 512(g)(2).

¹See 17 U.S.C.A. §§ 1501 to 1511.

requirement under section 512(g) that a copyright owner file an action to keep material down in response to a counter notification, in lieu of filing a federal court lawsuit. For copyright owners, this may be a lower cost and lower risk alternative to filing suit in federal court, to prevent material from being restored by a service provider in response to a DMCA counter notification. To qualify, a claim or counterclaim brought before the Copyright Claims Board must allege copyright infringement of the material identified in the notification that caused the material to be taken down and must be provided to the service provider before it replaces the material following the waiting period mandated by section 512(g), in response to a counter notification.²

This provision of the CASE Act potentially could be abused by owners of registered copyrights (or merely applicants for registration, who would not yet even be able to file suit in federal court³ but who could initiate a claim or counterclaim before the Copyright Claims Board and hold it in abeyance potentially for a year or more⁴) to keep material offline for an extended period of time. While the CASE Act provides for sanctions for bad faith, those typically are limited to \$5,000 except in exceptional circumstances.⁵

CASE Act claims initiated with the Copyright Claims Board would not help copyright owners responding to DMCA counter notifications if the party that sent the counter notification is a foreign national. The CASE Act does not permit claims to be asserted against a person or entity residing outside the United States (although if such a person or entity brings a claim, a counterclaim may be asserted against that person or entity).⁶ While a user who submits a counter notification to a service provider to restore access to material taken down in response to a DMCA notification must assent to jurisdiction in a U.S. court,⁷ that user need not consent to proceedings before the Copyright Claims Board. Moreover, copyright owners or service providers could not seek to have users waive these requirements in Terms of Service or other

²See 17 U.S.C.A. § 1507(d).

³See *supra* § 4.08[2].

⁴See 17 U.S.C.A. § 1505; see generally *supra* § 4.08[8] (explaining this provision and analyzing the CASE Act).

⁵See 17 U.S.C.A. § 1506(i).

⁶See 17 U.S.C.A. § 1504(d)(4).

⁷See 17 U.S.C.A. § 512(g)(2)(C).

contracts.⁸

The time frame for filing suit or bringing a CASE Act complaint before the Copyright Claims Board may work to the potential disadvantage of complainants if they are not expecting a counter notification and fail to react in “Internet time.”⁸ Although there is no specific time period mandated for an alleged infringer to file a counter notification, once one is filed, service providers must notify complainants “promptly” of receipt of the counter notification, and must in any event restore access to the content within ten to fourteen business days absent receipt of notice from the original complainant that a lawsuit has been filed. Since the time period runs from the time a service provider *receives* the counter notification—rather than the time the counter notification is sent to or received by the original complainant—a service provider’s delay in “promptly” transmitting the counter notification could be detrimental to a copyright owner. Complainants anxious to have infringing content removed therefore should act through their litigation counsel or otherwise be prepared to initiate litigation within days of receiving a copy of a counter notification.

Material misrepresentations in counter notifications may lead to liability under section 512(f) of the DMCA⁹ or other theories of law.¹⁰

The procedures set forth in the DMCA for notification and counter notification relieve service providers of any obligation to evaluate the merits of a dispute. Service providers that seek to benefit from all of the protections afforded by the Act need only mechanically evaluate whether notifications or counter notifications substantially comply with the requirements of the statute and then automatically disable access to or remove offending content and/or restore access to or replace the content within the strict time frames established by the law.

⁸See 17 U.S.C.A. § 1504(a) (providing that the rights, remedies, and limitations set forth in that section “may not be waived except in accordance with this chapter.”).

⁸See *supra* § 1.06.

⁹See *infra* § 4.12[9][D].

¹⁰See *infra* § 4.12[9][F].

**4.12[9][D] Section 512(f) Liability, Injunctive
Relief and Sanctions for
Misrepresentations in Notifications and
Counter Notifications**

Both copyright owners and accused infringers who are *subscribers* within the meaning of the statute must be honest in their representations in notifications and counter notifications for the DMCA's system of notice and takedown to work properly, since service providers are required to mechanically comply with substantially complying notifications and counter notifications, rather than investigate the merits of the assertions of ownership or rights asserted in these notices. To minimize the risk of fraudulent notifications or counter notifications being filed, Congress provided in 17 U.S.C.A. § 512(f) that both copyright owners and accused infringers may be subject to liability if they make material misrepresentations in notifications or counter notifications¹ (although oddly a party's statement of the merits of its position is only required to be submitted under penalty of perjury in a counter notification).² The Ninth Circuit has further extended this statutory obligation to hold that copyright

[Section 4.12[9][D]]

¹Although it goes without saying that remedies under section 512(f) apply only to misrepresentations in connection with DMCA notifications and counter notifications, the Eleventh Circuit held in one case that a claim under section 512(f) may not be premised on allegedly false notices of trademark infringement. *See Mandala v. Tire Stickers, LLC*, 829 F. App'x 896, 902 (11th Cir. 2020) (affirming dismissal).

Likewise, “[i]t is self-evident that a statement cannot be a ‘misrepresentation’ for purposes of 17 U.S.C. § 512(f) if it is factually accurate.” *Hosseinzadeh v. Klein*, 276 F. Supp. 3d 34, 47 (S.D.N.Y. 2017) (granting summary judgment for defendant Klein on plaintiff's 512(f) claim where Klein's use was found to be a fair use and “even if this Court held the Klein video [wa]s not fair use, the Court would still dismiss Claim II because defendants clearly had a subjective “good faith belief” that their video did not infringe plaintiff's copyrights.”). “[T]he same is of course true for statements that are legally accurate.” *Hughes v. Benjamin*, 437 F. Supp. 3d 382, 394-95 (S.D.N.Y. 2020) (dismissing plaintiff's section 512(f) claim, in a dispute between YouTubers, where the defendant represented in a counter notification that her use was a fair use and “highly transformative,” where the court ultimately concluded that the use was indeed fair and the assertion that defendant's video was “highly transformative” was merely hyperbole and not legally significant).

²*See* 17 U.S.C.A. § 512(g)(3)(C). A notification must include merely a statement of the merits made “in good faith” and a statement of its accuracy, although the certification that the complaining party is authorized to act on behalf of an owner of an exclusive right must be made under

owners also may be held liable for misrepresenting their rights under the DMCA if they fail to make a good faith subjective determination that the material at issue in a given DMCA notification is not a fair use before submitting a takedown notice under the DMCA.³

Claims under section 512(f) for damages and, if applicable, attorneys' fees, may be brought in court or—subject to a \$30,000 cap for damages and \$5,000 cap for attorneys' fees and costs— before the Copyright Claims Board, pursuant to the Copyright Alternative in Small-Claims Enforcement (CASE) Act of 2020,⁴ which is separately analyzed in section 4.08[8]. CASE Act dispute resolution generally is only available when brought against U.S. residents (unless a non-resident itself initiates a claim, in which case a counterclaim could be brought).⁵

Suits for sanctions under section 512(f) are sometimes joined with common law claims for relief, which are separately analyzed in section 4.12[9][F]. Those claims, however, could not be joined in a section 512(f) proceeding before the Copyright Claims Board. Thus, copyright owners, service providers, and users, who seek to take action for misrepresentations in a DMCA notification or counter notification must select between potentially asserting a broader range of claims, without damage limitations, in federal court, or pursuing a potentially less expensive administrative remedy for a section 512(f) claim only. For many, pursuing a section 512(f) claim before the Copyright Claims Board will be the preferred route.

Today, many DMCA notifications are sent by automated

penalty of perjury. *See* 17 U.S.C.A. §§ 512(c)(3)(A)(v), 512(c)(3)(A)(vi). It is possible that this reflects a drafting error and that Congress intended that both the certification and the statement of accuracy included in the notification be made under penalty of perjury (which would then parallel the obligation imposed on subscribers when signing counter notifications), but for purposes of statutory construction courts must assume that this difference was intentional. *See Doe v. Geller*, 533 F. Supp. 2d 996, 1011 (N.D. Cal. 2008) (writing, in connection with the lack of parallel structure between notifications and counter notifications with respect to submission to jurisdiction, “[t]hat difference must be viewed as intentional.”; citation omitted).

³*See Lenz v. Universal Music Corp.*, 815 F.3d 1145 (9th Cir. 2016).

⁴*See* 17 U.S.C.A. §§ 1501 to 1511.

⁵*See* 17 U.S.C.A. § 1504(d); *see generally supra* § 4.08[8] (analyzing the CASE Act in greater detail).

processes and may include errors or omissions.⁶ Mere errors or omissions, however, may not justify relief under section 512(f) (although they potentially could be actionable under other theories of law). Where automated notices are repeatedly sent without human verification, at least one court has held that a plaintiff could state a 512(f) claim.⁷

Section 512(f) provides that any person who “knowingly materially misrepresents” that “material or activity” is infringing or was removed or disabled “by mistake or misidentification” may be held liable for damages, including costs and attorneys’ fees, in an action brought by an alleged infringer, a copyright owner or authorized licensee or a service provider injured by a service provider’s reliance on the misrepresentation.⁸ As explained by one court, a section 512(f) claim requires allegations that a defendant (1) knowingly and materially misrepresented that copyright infringe-

⁶According to one study of 3,000,000 takedown notices and more than 80,000,000 takedown complaints served on Google between 2011 and 2015, at least 5.5% omitted copyright work descriptions and at least 9.8% had empty takedown requests, misidentified the infringing site or provided inactive URLs. See Daniel Seng, *Copyrighting Copywrongs: An Empirical Analysis of Errors with Automated DMCA Takedown Notices*, 37 Santa Clara High Tech. L.J. 119 (2021).

⁷See *Enttech Media Group LLC v. Okularity, Inc.*, Case No. 2:20-cv-06298 RGK (Ex), 2020 WL 6888722 (C.D. Cal. Oct. 2, 2020) (dismissing plaintiff’s RICO claim but denying defendant’s motion to dismiss plaintiff’s DMCA 512(f) claim arising out of 48 automated takedown notices sent by the defendant to Instagram, which resulted in Instagram disabling the Instagram page of *Paper* magazine, holding that plaintiff stated a claim by alleging that Okularity used software that scanned the Internet for potentially infringing images on its clients’ behalf, automatically generating DMCA takedown notices against purported infringers without considering potential non-infringing use of images, including fair use, thereby causing Enttech to lose revenue from Instagram); see also *ENTTech Media Group LLC v. Okularity, Inc.*, Case No. 2:20-cv-06298-JWH-Ex, 2021 WL 916307, at *6 (C.D. Cal. Mar. 10, 2021) (denying Okularity’s subsequent motion to dismiss because “to plead a claim under § 512(f), it is enough for ENTtech to allege that Defendants did not consider fair use (sufficiently or at all) before issuing the takedown notices.”).

Enttech alleged that Okularity typically waited until notices accumulated to the point when a social media platform would disable access to the target’s account before contacting the purported infringer to initiate settlement negotiations, demanding \$1,010,000 in this case. Enttech requested copies of the DMCA notifications sent to Instagram, but Okularity’s agent refused to provide them unless Enttech agreed to sign a nondisclosure agreement. Enttech filed suit instead.

⁸17 U.S.C.A. § 512(f). Section 512(f) reads in full:

ment occurred, (2) that a service provider relied on the misrepresentation, and (3) that plaintiff was injured as a result.⁹ It is a complete defense to a claim under section 512(f), however, if the party that issued the takedown notice had a subjective good faith belief that the use in question was not authorized (including, for example, because of reliance on counsel).¹⁰

Relief under section 512(f) may be sought by an affirmative claim.¹¹ To state a claim under section 512(f) in federal

Misrepresentations.—Any person who knowingly materially misrepresents under this section—

- (1) that material or activity is infringing, or
- (2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

⁹*Enttech Media Group LLC v. Okularity, Inc.*, Case No. 2:20-cv-06298 RGK (Ex), 2020 WL 6888722, at *5 (C.D. Cal. Oct. 2, 2020).

¹⁰*See, e.g., Johnson v. New Destiny Christian Center Church, Inc.*, 826 F. App'x 766, 772 (11th Cir. 2020) (affirming summary judgment for New Destiny Christian Center Church and Paula White, where they relied on counsel in sending a DMCA takedown notice to YouTube, seeking removal of videos of New Destiny Christian Center Church sermons that had been uploaded by Johnson and which included her critique of the sermons, and thus had a good faith belief that the videos uploaded by Johnson were not a fair use); *see also Makeup Blowout Sale Group, Inc. v. All that Glowz, Inc.*, Civil Action No. 20-20906-Civ-Scola, 2020 WL 5535533, at *2-3 (S.D. Fla. Sept. 15, 2020) (applying *Johnson* in denying a motion to dismiss where the counterclaim plaintiffs alleged that Makeup Blowout did not have a subjective good faith belief that the use in question was unauthorized where Beauty Pop-up alleged that Makeup Blowout's owner showed it how to use the images, consented to their display, referred to it as a "sister company" in a Facebook post and introduced Beauty Pop-up to Makeup Blowout owner's girlfriend to help manage the Beauty Pop-up Facebook account).

¹¹*See, e.g., Curtis v. Shinsachi Pharmaceutical Inc.*, 45 F. Supp. 3d 1190 (C.D. Cal. 2014) (entering a default judgment under section 512(f) where a seller alleged that between 2011 and 2013 defendants, who were her competitors, submitted 30 false Notices of Claimed Infringement to eBay, resulting in the removal of at least 140 listings and causing eBay to issue strikes against her selling account, as well as allegedly false notices to Google, PayPal and Serversea); *T.D. Bank, N.A. v. Hill*, Civil No. 12-7188 (RBK/JS), 2014 WL 413525, at *7-8 (D.N.J. Feb. 3, 2014) (denying motion to dismiss a claim under section 512(f)).

court, however, a plaintiff must have suffered an injury to meet the requirements of Article III standing and assert claims that “fall within the zone” of interests protected by section 512(f).¹² Article III standing need not be shown, however, to bring a 512(f) claim before the Copyright Claims Board under the CASE Act.

The statutory remedy focuses on *misrepresentations* that were relied upon by a service provider in disabling access to or restoring access to a work. It therefore does not matter whether the misrepresentation in fact was made in a substantially complying notification or counter notification or merely some other form of takedown notice.¹³

Where a mistake is made in a DMCA notification or counter notification, even if it rises to the level of a misrepresentation, the mistake will not be actionable under section 512(f) unless it was acted upon. A representation that particular works are protected and should be removed will not rise to the level of a material misrepresentation under section 512(f), and a user will not be deemed to have suffered any injury, if the service provider did not act on them.¹⁴

¹²*Handshoe v. Perret*, 270 F. Supp. 3d 915 (S.D. Miss. 2018) (holding that a website publisher had Article III standing to sue the owners of creative works that had sent takedown requests to his service providers but dismissed several of his claims as falling outside the zone of protection afforded by section 512(f)).

¹³In *Brave New Films 501(c)(4) v. Weiner*, 626 F. Supp. 2d 1013 (N.D. Cal. 2009), the court denied a defendant’s motion to dismiss a misrepresentation claim brought under section 512(f) over the defendant’s objection that the letter at issue, which had resulted in plaintiff’s videos being removed by YouTube, was not a substantially complying notification because it did not include a statement that the sender had a good faith belief that the defendant’s use of plaintiff’s work was unauthorized. While relevant to the question of whether a service provider must disable access to or remove the material or activity described in the notice (*supra* § 4.12[9][B]), whether a notification (or counter notification) in fact is substantially complying, as noted above in the text, should not be relevant in assessing whether a party has stated a claim under section 512(f) based on a misrepresentation.

¹⁴*See, e.g., Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 704–05 (D. Md. 2011) (granting judgment for the defendant on plaintiff’s section 512(f) claim where the service party that received the takedown notice responded by advising that it no longer hosted the website that was the subject of the notice; “Even assuming that Wilson acted knowingly, a fact not established by the record, his conduct did not violate the statute because it did not provoke a response from A1–Hosting and did not result in any harm to Plaintiffs.”); *Capitol Records, Inc. v.*

In *Rossi v. Motion Picture Association of America, Inc.*,¹⁵ the Ninth Circuit construed the scope of section 512(f) narrowly, writing that:

In section 512(f), Congress included an expressly limited cause of action for improper infringement notifications, imposing liability only if the copyright owner's notification is a knowing misrepresentation. A copyright owner cannot be liable simply because an unknowing mistake is made, even if the copyright owner acted unreasonably in making the mistake. See § 512(f). Rather, there must be a demonstration of some actual knowledge of misrepresentation on the part of the copyright owner.

Juxtaposing the “good faith” requirement of the DMCA¹⁶ with the “knowing misrepresentation” provision of that same statute reveals an apparent statutory structure that predicated the imposition of liability upon copyright owners only for knowing misrepresentations regarding allegedly infringing websites. Measuring compliance with a lesser “objective reasonableness” standard would be inconsistent with Congress's apparent intent that the statute protect potential violators from subjectively improper actions by copyright owners.

Rossi involved the operator of a website that advertised “Full Length Downloadable Movies” and posted graphics for copyrighted motion pictures. In response, the MPAA sent DMCA notices to Rossi's ISP. Rossi sued the MPAA for tortious interference, arguing in effect that the MPAA should be held liable for taking Rossi at his word based on what he advertised to be available on his website, when in fact his representations were untrue and users could not download motion pictures from his site. Based on both the facts and the law, the Ninth Circuit concluded that the MPAA could not be held liable based on the MPAA's subjective belief that

MP3tunes, LLC, 611 F. Supp. 2d 342, 346–47 (S.D.N.Y. 2009) (dismissing defendant's DMCA counterclaim with prejudice where, notwithstanding plaintiffs' representation that all links to its copyrighted recordings were infringing, the service provider only removed songs on a representative list, and did not disable access to or remove the links that were alleged to lead to five songs that allegedly were authorized for free download).

¹⁵*Rossi v. Motion Picture Ass'n of America Inc.*, 391 F.3d 1000 (9th Cir. 2004), *cert. denied*, 544 U.S. 1018 (2005).

¹⁶The Ninth Circuit also ruled in *Rossi* that the requirement of section 512(c)(3)(A)(v) that notifications include a statement that the complaining party believes, in good faith, that the copyrighted material identified is being used in a manner that is not authorized by the copyright owner, its agent or the law, encompasses a subjective, rather than objective, standard. See *generally supra* § 4.12[9][B].

infringing material was available on Rossi's site, rejecting Rossi's argument that a "reasonable investigation" would have shown that users could not download motion pictures from the site.¹⁷ The Ninth Circuit held that the DMCA's "interpretive case law and statutory structure support the conclusion that the 'good faith belief requirement in § 512(c)(3)(A)(v) encompasses a subjective, rather than objective standard.'"¹⁸ District courts in other circuits have applied this same standard.¹⁹

In *Online Policy Group v. Diebold Election Systems, Inc.*,²⁰ a case decided shortly before *Rossi* by a district court in the Ninth Circuit, Judge Jeremy Fogel of the Northern District of California held that the defendant in a declaratory judgment action was liable for monetary relief, including attorneys' fees and costs, pursuant to section 512(f), for sending notifications to service providers for an email database that included material subject to the fair use defense—even though the defendant in fact never filed a copyright infringement suit and the plaintiff's complaint for declaratory relief was dismissed as moot based on a finding that the defendant did not intend to initiate litigation. The plaintiffs had alleged that they had posted and linked to a database of Diebold's internal company emails to inform the public about problems associated with Diebold's electronic voting machines.

In holding that Diebold knowingly materially misrepresented that plaintiffs had infringed its copyright interest, the court reasoned that:

The misrepresentations were material in that they resulted in removal of the content from websites and the initiation of the present lawsuit. The fact that Diebold never actually brought suit against any alleged infringer suggests strongly that Diebold sought to use the DMCA's safe harbor provisions—which were designed to protect ISPs, not copyright holders—as

¹⁷*Rossi v. Motion Picture Ass'n of America Inc.*, 391 F.3d 1000, 1003 (9th Cir. 2004), *cert. denied*, 544 U.S. 1018 (2005).

¹⁸*Rossi v. Motion Picture Ass'n of America Inc.*, 391 F.3d 1000, 1004 (9th Cir. 2004), *cert. denied*, 544 U.S. 1018 (2005).

¹⁹*See, e.g., Cabell v. Zimmerman*, No. 09 CIV. 10134(CM), 2010 WL 996007, at *4–5 (S.D.N.Y. Mar. 12, 2010); *Third Educational Group, Inc. v. Phelps*, 675 F. Supp. 2d 916, 927 (E.D. Wis. 2009); *Dudnikov v. MGA Entertainment, Inc.*, 410 F. Supp. 2d 1010, 1013 (D. Colo. 2005).

²⁰*Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property.

The court construed *material* to mean “that the misrepresentation affected the ISP’s response to the DMCA letter.”

While the *Diebold* court’s analysis of materiality remains potentially relevant, its analysis of what constitutes a material misrepresentation is no longer good law. Citing Black’s law dictionary, Judge Fogel had construed *knowingly* to mean “that a party actually knew, or should have known if it acted with reasonable care or diligence, or would have had no substantial doubt had it been acting in good faith, that it was making misrepresentation.” This standard, however, is too strict in light of the Ninth Circuit’s subsequent ruling in *Rossi* that subjective, not objective intent is relevant under section 512(f).

In *Lenz v. Universal Music Corp.*²¹—colloquially referred to as the “Dancing Baby Case”—the Ninth Circuit further held that a copyright owner faces liability under section 512(f) if it knowingly misrepresents in a takedown notification that it has formed a good faith belief that the material identified in a DMCA notification was not authorized by law because the copyright owner failed to consider a user’s potential fair use of the material before sending the DMCA notification. *Lenz* was brought by a YouTube user who claimed that Universal Music Group failed to act in good faith when it sent a DMCA notification to YouTube alleging that a video that she posted on the service was infringing, because UMG failed to consider fair use. The video at issue was a twenty-nine second clip of plaintiff’s son dancing. For twenty seconds, Prince’s song “Let’s Go Crazy” could be heard playing in the background. At the behest of Prince, UMG had sent a DMCA notice to YouTube, which removed the video. In response, Lenz sent a counter notification. Because UMG did not file suit for copyright infringement, the video was reposted to the site. Lenz sued, however, seeking damages and attorneys’ fees from UMG pursuant to section 512(f) and for tortious interference with her contract with YouTube. In allowing the suit to proceed based on the allegation that UMG had acted in bad faith by issuing a takedown notice without proper consideration of fair use, Northern District of California Judge Jeremy Fogel ruled that section 512(c)(3)(A)(v) requires a copyright owner to

²¹*Lenz v. Universal Music Corp.*, 815 F.3d 1145 (9th Cir. 2016).

consider fair use in formulating a good faith belief that “use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.”²²

Seven years later, in 2015, the Ninth Circuit affirmed, holding that section 512(c)(3)(A)(v) requires a copyright owner to consider fair use in formulating a good faith belief that “use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.” The court ruled that a copyright owner need only have a subjective good faith belief that the material at issue in a DMCA notice is not entitled to fair use, but a copyright owner faces liability if it knowingly misrepresents in a takedown notice that it had formed a good faith belief that the material was not authorized by law without considering fair use. As explained by the majority, “[t]his inquiry lies not in whether a court would adjudge the video as a fair use, but whether Universal formed a good faith belief that it was not.”²³ The majority further explained that if

a copyright holder forms a subjective *good faith* belief the allegedly infringing material does not constitute fair use, we are in no position to dispute the copyright holder’s belief even if we would have reached a different conclusion. A copyright holder who pays lip service to the consideration of fair use by claiming it formed a good faith belief when there is evidence to the contrary is still subject to § 512(f) liability.²⁴

The Ninth Circuit clarified that liability could be imposed based on willful blindness if a copyright owner (1) subjectively believed there was a high probability that the subject of a DMCA notice constituted a fair use, and (2) took deliberate action to avoid learning of this fair use.²⁵

The subjective standard articulated by the Ninth Circuit does not necessarily mean that a copyright owner must manually review material before sending a DMCA notice, although that certainly is a best practice where it is feasible to

²²*Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150 (N.D. Cal. 2008), *aff’d* 815 F.3d 1145 (9th Cir. 2016).

²³*Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1153 (9th Cir. 2016).

²⁴*Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1154 (9th Cir. 2016).

²⁵*Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1155 (9th Cir. 2016), *citing* *Global-Tech Appliances, Inc. v. SEB S.A.*, 563 U.S. 754 (2011); *see generally supra* § 4.11[6][A] (analyzing the case in greater detail in the context of liability for copyright infringement); *infra* § 4.12[6][C] (analyzing *SEB* and willful blindness in the context of knowledge or awareness that could disqualify a service provider from DMCA safe harbor protection).

do so. For popular works, the volume of unauthorized infringement may be too great to manually check every file. Artificial intelligence, bots (or intelligent agents), algorithms and scripts frequently are used by copyright owners to search for and identify allegedly infringing material. In dicta in *Lenz*, which was subsequently removed in a revised version of the opinion, the Ninth Circuit had noted, “without passing judgment, that the implementation of computer algorithms appears to be a valid and good faith middle ground for processing a plethora of content while still meeting the DMCA’s requirements to somehow consider fair use.”²⁶ This portion of the court’s original 2015 opinion was deleted when it was subsequently replaced with an amended opinion in 2016. Nevertheless, although the propriety of using automated notifications to comply with the DMCA was not specifically at issue in *Lenz*, under the Ninth Circuit’s flexible standard, the use of algorithms or artificial intelligence to search for and identify content should be appropriate where a copyright owner either manually confirms that a file is infringing or sets the search parameters in such a way that the copyright owner has a good faith subjective basis to believe that material identified through automated search techniques is infringing and not a fair use.²⁷

Where liability may be found, the Ninth Circuit held that even if an affected user has incurred no monetary loss the

²⁶*Lenz v. Universal Music Corp.*, 801 F.3d 1126, 1135 (9th Cir. 2015), *amended and replaced by*, 815 F.3d 1145 (9th Cir. 2016). In this subsequently deleted portion of its opinion, the court cited *Disney Enterprises, Inc. v. Hotfile Corp.*, No. 11-cv-20427, 2013 WL 6336286, at *47 (S.D. Fla. Sept. 20, 2013) (“The Court . . . is unaware of any decision to date that actually addressed the need for human review, and the statute does not specify how belief of infringement may be formed or what knowledge may be chargeable to the notifying entity.”). In the withdrawn opinion, the Ninth Circuit further elaborated that, as an example,

consideration of fair use may be sufficient if copyright holders utilize computer programs that automatically identify for takedown notifications content where: “(1) the video track matches the video track of a copyrighted work submitted by a content owner; (2) the audio track matches the audio track of that same copyrighted work; and (3) nearly the entirety . . . is comprised of a single copyrighted work.” Brief for The Org. for Transformative Works, Public Knowledge & Int’l Documentary Ass’n as Amici Curiae Supporting Appellee at 29–30 n. 8 (citing the Electronic Frontier Foundation website (link unavailable)).

Lenz v. Universal Music Corp., 801 F.3d 1126, 1135–36 (9th Cir. 2015), *amended and replaced by*, 815 F.3d 1145 (9th Cir. 2016). While this example seems reasonable, it is also likely that less exacting search criteria would satisfy the Ninth Circuit’s subjective good faith test.

²⁷The *Lenz* court explained that

user may recover nominal damages for a knowing material misrepresentation under section 512.²⁸ The appellate court

if a copyright holder ignores or neglects our unequivocal holding that it must consider fair use before sending a takedown notification, it is liable for damages under § 512(f). If, however, a copyright holder forms a subjective good faith belief the allegedly infringing material does not constitute fair use, we are in no position to dispute the copyright holder's belief even if we would have reached the opposite conclusion. A copyright holder who pays lip service to the consideration of fair use by claiming it formed a good faith belief when there is evidence to the contrary is still subject to § 512(f) liability. *Cf. Disney Enters., Inc. v. Hotfile Corp.*, No. 11-cv-20427, 2013 WL 6336286, at *48 (S.D. Fla. Sept. 20, 2013) (denying summary judgment of § 512(f) counterclaim due to "sufficient evidence in the record to suggest that [Plaintiff] Warner intentionally targeted files it knew it had no right to remove"); *Rosen v. Hosting Servs., Inc.*, 771 F. Supp. 2d 1219, 1223 (C.D. Cal. 2010) (denying summary judgment of § 512(f) counterclaim where the takedown notification listed four URL links that did not contain content matching the description of the purportedly infringed material); *Online Policy Grp. v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1204-05 (N.D. Cal. 2004) ("[T]here is no genuine issue of fact that Diebold knew—and indeed that it specifically intended—that its letters to OPG and Swarthmore would result in prevention of publication of that content. . . . The fact that Diebold never actually brought suit against any alleged infringer suggests strongly that Diebold sought to use the DMCA's safe harbor provisions—which were designed to protect ISPs, not copyright holders—as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property.").

Lenz v. Universal Music Corp., 815 F.3d 1145, 1154-55 (9th Cir. 2016). Thus, so long as search criteria is reasonable to allow a copyright owner to form a subjective good faith belief that material identified is infringing and not a fair use, the Ninth Circuit's test should be satisfied even without human review.

In an unreported opinion pre-dating *Lenz*, *Ouellette v. Viacom Int'l, Inc.*, No. CV 10-133-M-DWM-JCL, 2012 WL 850921, at *5 (D. Mont. Mar. 13, 2012), *report and recommendation adopted*, No. CV 10-133-M-DWM-JCL, 2012 WL 1435703 (D. Mont. Apr. 25, 2012), *aff'd*, 671 F. App'x 972 (9th Cir. 2016), the lower court granted Viacom's motion for judgment on the pleadings against a pro se plaintiff's section 512(f) claim, where Viacom had submitted automated DMCA takedown notices leading to the removal of plaintiff's videos because, among other things, the plaintiff advanced "no factual matters suggesting it is plausible that Viacom had actual knowledge of the software's alleged deficiencies." *See* 2012 WL 850921, at *5. In that case, the plaintiff had complained that Viacom used "scanning software" without human oversight, which he claimed was necessary to prevent the software from mis-identifying fair use videos. *See* 2012 WL 850921, at *4. The district court adopted the Magistrate Judge's recommended ruling finding, among other things, that Ouellette failed to plead facts supporting his assertion that Viacom knew that its scanning software was improperly flagging Ouellette's protected, "fair use" videos as infringing. *See* 2012 WL 1435703, at *4. The Ninth Circuit affirmed the lower court's entry of judgment on the pleadings without leave to amend. *Ouellette v. Viacom Int'l, Inc.*, 671 F. App'x 972 (9th Cir. 2016).

²⁸*Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1156 (9th Cir. 2016) (discussing nominal awards in tort cases).

declined, however, to decide the scope of recoverable damages, including “whether she may recover expenses following the initiation of her § 512(f) suit or *pro bono* costs and attorneys’ fees, both of which arose as a result of the injury incurred.”²⁹

The Ninth Circuit’s opinion in *Lenz* left section 512(f) claims as potentially viable but likely not lucrative, except in rare circumstances. While Judge Fogel’s 2008 lower court decision in the same case initially led to a flurry of complaints (mostly by *pro se* plaintiffs) and expressions of concern on the part of copyright owners, a later decision in the case defining the type of damages recoverable under section 512(f) substantially scaled back enthusiasm for seeking sanctions under the DMCA. In early 2010, Judge Fogel held that a plaintiff’s damages under section 512(f) must be “proximately caused by the misrepresentation to the service provider and the service provider’s reliance on the misrepresentation.”³⁰ In reaching this conclusion, based on the statute, legislative history and similar statutory language, Judge Fogel rejected both plaintiffs urging that more broadly any damages “but for” the misrepresentation could be recovered and UMG’s argument that only substantial economic damages were recoverable. Judge Fogel observed that a “but for” test would allow any plaintiff to satisfy the damage element of their claims merely by hiring an attorney and filing suit, which could not be justified based on either the language of the statute or the statutory goal of deterrence. At the same time, he conceded that “[i]t may be that the combination of the subjective bad faith standard and the proximate causation requirements will lead many potential § 512(f) plaintiffs to refrain from filing suit unless they have suffered substantial economic harm or other significant inconvenience. However, . . . this result is not necessarily at odds with what Congress intended.”³¹

Judge Fogel likewise narrowly construed the term “fees and costs,” which are an element of recoverable damages

²⁹*Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1157 (9th Cir. 2016).

³⁰*Lenz v. Universal Music Corp.*, 94 U.S.P.Q.2d 1344, 2010 WL 702466 (N.D. Cal. 2010) (emphasis in original omitted).

³¹*Lenz v. Universal Music Corp.*, 94 U.S.P.Q.2d 1344, 2010 WL 702466 (N.D. Cal. 2010), *citing* Laura Quilter & Jennifer M. Urban, Efficient Process or “Chilling Effects”? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act, 22 Santa Clara Computer & High Tech. L.J. 621, 631 (2006).

under section 512(f). He ruled that fees and costs incurred in responding to a takedown notice or otherwise prior to the institution of a lawsuit are recoverable under section 512(f), but fees and costs incurred *after* suit is filed are not automatically recoverable. Judge Fogel noted that the Copyright Act authorizes a court to award reasonable attorneys' fees in its discretion to the prevailing party and full costs in its discretion by or against any party other than the United States (or an officer of the United States).³² Lenz's argument that post-suit fees and costs could be claimed as an element of damage under section 512(f), he wrote, "would remove the Court's discretion to award (or not award) fees to plaintiffs, force the Court to treat prevailing plaintiffs and defendants differently with regard to fees, and contradict the application of § 505 to 'any action under' Title 17." For the same reason that Congress "did not intend to allow plaintiffs to establish the damage element under § 512(f) merely by hiring an attorney and filing suit" Judge Fogel concluded that it there was no indication that Congress intended fees and costs incurred in filing suit to be an element of damage under section 512(f).

With respect to damages, the Ninth Circuit majority in *Lenz* held that Lenz was not limited to actual monetary loss. The majority explained that section 512(k) defines *monetary relief* as "damages, costs, attorneys['] fees, and any other form of monetary payment." The term *monetary relief* is used in sections 512(a), 512(b)(1), 512(c)(1) and 512(d), which outline the four DMCA safe harbors that potentially may insulate a service provider from *monetary relief*. The majority deemed it significant that this term was "notably absent from § 512(f)." In fact, it is reasonable that Congress would broadly define the range of monetary relief from which a service provider would be insulated by the DMCA safe harbors. Nevertheless, the court deemed it significant that Congress used the term "any damages" in section 512(f), which it concluded evidenced an intent to depart from the common law presumption that a misrepresentation plaintiff must have suffered a monetary loss. A more likely explanation, when the different purposes for the references to monetary relief and damage in the safe harbor provisions, on the one hand, and misrepresentation section, on the other, are considered, is that Congress wanted to broadly protect

³²See 17 U.S.C.A. § 505; *infra* § 4.15.

eligible service providers by the safe harbor and allow recovery of damages, if any, for misrepresentations. The Ninth Circuit's assumption that *any damages* was intended to be broader than the defined term *monetary relief* is simply unsupportable when the purpose for each section is considered.

In *Tuteur v. Crosley-Corcoran*,³³ Judge Richard G Stearns of the District of Massachusetts held that a blogger adequately stated a claim under section 512(f) by alleging that the defendant made “a knowing and material misrepresentation” in a DMCA notice, but rejected the argument that a copyright owner is required to verify that it had explored an alleged infringer’s affirmative defenses prior to sending a DMCA notice, noting that even the *Lenz* court, “in its most recent iteration (denying cross-motions for summary judgment) . . . substantially retreated from its ruling, acknowledging that ‘in light of *Rossi*,’ the ‘mere failure to consider fair use *would be insufficient* to give rise to liability under § 512(f), and that a plaintiff must show that the defendant ‘had some actual knowledge that its Takedown Notice contained a material misrepresentation.’ ”³⁴ Judge Stearns found “[m]ore compelling . . . the fact that, in enacting the DMCA, Congress did not require that a notice-giver verify that he or she had explored an alleged infringer’s possible affirmative defenses prior to acting, only that she affirm a good faith belief that the copyrighted material is being used without her or her agent’s permission.”³⁵ Judge Stearns added that there was reason for this statutory scheme: “To have required more would have put the takedown procedure at odds with Congress’s express intent of creating an ‘expeditious,’ ‘rapid response’ to ‘potential infringement’ on the Internet.”³⁶

Tuteur arose out of the personal animosity of two bloggers

³³*Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 333 (D. Mass. 2013).

³⁴*Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 333, 343 (D. Mass. 2013), quoting *Lenz v. Universal Music Corp.*, No. 5:07-cv-03783-JF, 2013 WL 271673, at *6 (N.D. Cal. Jan. 24, 2013).

³⁵*Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 333, 343-44 (D. Mass. 2013).

³⁶*Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 333, 344 (D. Mass. 2013), citing 17 U.S.C. § 512(c)(i)(A)(iii); S. Rep. 105-190, at 21. In response to the policy arguments presented by amici, Judge Stearns added:

Undoubtedly abuses will occur—as is the case with almost any system that permits legal self-help (although EFF and DMLP point to but a handful of

towards one another. The defendant, Gina Crosley-Corcoran, was a doula who advocated home birthing methods on her blog, *TheFeministBreeder*, which the plaintiff, Amy Tuteur, a former OBGYN, disagreed with in a scathing critique on her blog, *The Skeptical OB*. After a heated exchange, the doula briefly posted a photo of herself giving the OBGYN “the finger”³⁷ with the caption that she was giving Tuteur “something else to go back to her blog and obsess about.” Crossley-Corcoran eventually thought better of the exchange and took down the photo but not before Tuteur had copied it and posted it on *The Skeptical OB*, without Crossley-Corcoran’s permission. Crossley-Corcoran sent Tuteur a cease and desist letter and sent Tuteur’s ISP a DMCA takedown notice. The ISP warned Tuteur to remove the photo, but she instead filed a counter notice and, when her ISP, in the court’s words, “washed its hands of the snowballing disputation and notified Tuteur and Crosley-Corcoran that it was up to either or both of them to ‘pursue legal action’” Tuteur switched ISPs and reposted the photo, which led to another round of DMCA notifications and counter notifications and an exchange of legal letters between Tuteur’s husband, the chair of Foley & Lardner’s litigation practice in Boston, and counsel retained by the doula. Tuteur then sued the doula in a lawsuit in which multiple amici, including the Motion Picture Association of America (which was the defendant in *Rossi*) and the Electronic Frontier Foundation (*pro bono* counsel to the plaintiff in *Lenz*) filed amicus briefs on the issue of the proper interpretation of section 512(f).³⁸

examples). For these abuses Congress provided a remedy in section 512(f). If experience ultimately proves that the remedy is weighted too heavily in favor of copyright owners at the expense of those who seek to make “fair use” of another’s intellectual property, the resetting of the balance is for Congress and not a court to strike.

961 F. Supp. 2d at 344.

³⁷In an earlier opinion, Judge Stearns described the photograph as involving Crosley-Corcoran “making a graphic gesture with her middle finger that is often associated with an unrealized ambition of French soldiers at the Battle of Agincourt.” *Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 329, 330 (D. Mass. 2013).

³⁸The court also ruled on the question of whether sending a DMCA notice to Tuteur’s ISP in Utah subjected Crosley-Corcoran, a resident of Illinois, to jurisdiction in Massachusetts (concluding that it did based on the facts of this case). *See Tuteur v. Crosley-Corcoran*, 961 F. Supp. 2d 333, 338-40, (D. Mass. 2013); *see generally infra* § 53.04[5][F] (analyzing jurisdiction based on DMCA and other takedown notices and discussing the

In *Automattic Inc. v. Steiner*,³⁹ a website owner and student blogger obtained sanctions by default judgment against a UK resident who was alleged to have knowingly misrepresented that plaintiffs violated his copyright. In so ruling, Judge Phyllis J. Hamilton, adopting the recommendations of Magistrate Judge Joseph C. Spero, held that plaintiffs were entitled to damages for the time and resources spent dealing with the improper notice, but not for any reputational damage.

The cumulative effect of these rulings is that users aggrieved by an allegedly wrongful takedown notice may bring suit to recover damage, but the cost of litigation may deter anyone from doing so except where there is a substantial economic loss (for example, where a company sends a false DMCA notice to a service provider to have a competitor's website shut down during Cyber Monday, the Christmas holiday season or an annual sale) or in cases like *Lenz* where counsel is willing to represent the plaintiff on a *pro bono* basis, or *Tuteur* where the plaintiff's spouse is a litigator. In *Lenz*, the district court had found that the plaintiff had established damages based on "time spent reviewing counter notice procedures, seeking the assistance of counsel, and responding to the takedown notice." These types of damages, however, are likely to be *de minimis* in cases such as *Lenz* where a mother's home video of her child was off-line for 10 days. If courts allow broad recovery of *any damages*, including attorneys' fees as consequential damages, as suggested as a possibility by the Ninth Circuit majority in *dicta* in *Lenz*, there will be an explosion of section 512(f) litigation brought by users and contingent fee counsel who would have no incentive to resolve, and every incentive to litigate section 512(f) disputes. If Judge Fogel's analysis and the analysis of other district courts to date is accurate, then most potential plaintiffs likely will think twice before filing suit to recover *de minimis* damages where attorneys' fees may only be recovered in the discretion of the court (and some courts may consider the *de minimis* amount at issue as grounds for denying a fee request, even where a plaintiff prevails).⁴⁰

By contrast, in cases involving unfair competition between commercial entities or competitors, *Lenz* underscores that

court's ruling on personal jurisdiction in greater detail).

³⁹*Automattic Inc. v. Steiner*, 82 F. Supp. 3d 1011 (N.D. Cal. 2015).

⁴⁰*See infra* § 4.15.

the DMCA authorizes potentially potent remedies. For example, if a competitor were to send a fraudulent takedown notice directed at another company's online storefront or seasonal sales promotion on December 17, hoping to keep a competitor offline during the Christmas shopping season, the aggrieved party could recover damages and potentially attorneys' fees.

Remedies for improper notices may be granted pursuant to judge's general equitable authority. In one case, for example, Judge Denny Chin, while still a district court judge in the Southern District of New York, granted summary judgment in favor of the copyright owner on a defendant's counterclaim for sending two DMCA notices for material that was found not be infringing, but retained jurisdiction over the case so that the defendants could turn to the court for relief if any further notices were served, writing that plaintiffs would have no good faith basis for serving new DMCA notices based on the dismissal of their copyright infringement claims.⁴¹

Some courts have also relied on section 512(f) of the DMCA to enjoin a competitor from sending improper takedown notices.⁴² Although an affected party may serve a counter notification in response to a notification to have material put

⁴¹See *Biosafe-One, Inc. v. Hawks*, 639 F. Supp. 2d 358, 369–70 n.3 (S.D.N.Y. 2009).

⁴²See, e.g., *Beyond Blond Productions, LLC v. Heldman*, 479 F. Supp. 3d 874 (C.D. Cal. 2020) (preliminarily enjoining defendants from submitting takedown notices for edited versions of public domain product design logos, which the court held were not covered by defendants' copyright registration); *Design Furnishings, Inc. v. Zen Path, LLC*, 97 U.S.P.Q.2d 1284, 2010 WL 5418893 (E.D. Cal. Dec. 23, 2010) (enjoining the defendant from sending takedown requests to eBay directed at the plaintiff's wicker products, specifically "from notifying eBay that defendant has copyrights in the wicker patio furniture offered for sale by plaintiff and that plaintiff's sales violate those copyrights."); see also *Amaretto Ranch Breedables, LLC v. Ozimals, Inc.*, 790 F. Supp. 2d 1024 (N.D. Cal. 2011) (allowing claims for unfair competition and copyright misuse to proceed, but dismissing tortious interference and section 512(f) claims where no takedown in fact occurred). The court in *Amaretto Ranch* reaffirmed its earlier unreported preliminary injunction order (issued pursuant to plaintiff's claim for declaratory relief) requiring the defendant to withdraw all DMCA takedown notifications sent to Second Life and send no further notifications. *Amaretto Ranch* was a suit between business competitors that sold virtual animals in Second Life. In an earlier ruling, the court had entered an ex parte TRO enjoining Second Life from taking down plaintiff's works in response to the defendant's takedown notices although Linden Labs, as the service provider, should not have been enjoined under

back online,⁴³ ten days or more may elapse before wrongfully removed material is restored.⁴⁴ In addition, absent injunctive relief, an unethical party potentially could serve multiple takedown notices to harass a competitor or interfere with a legitimate business. Both declaratory and injunctive relief potentially may be available in cases involving abuse of the DMCA notice and takedown system.

Absent some evidence of abuse, injunctive relief generally could be difficult to obtain.⁴⁵ Moreover, merely because a defendant prevails in litigation does not mean that sanctions necessarily should be awarded against a copyright owner for sending a DMCA notice that ultimately is found to have lacked merit. In *UMG Recordings, Inc. v. Augusto*,⁴⁶ for example, Judge James Otero of the Central District of California granted summary judgment to UMG on a defendant's counterclaim for damages and attorneys' fees under section 512(f) in a case involving the defendant's sale of promotional CDs over eBay. In that case, UMG had sent a DMCA notice to eBay asking that defendant's listings for Promo CDs be removed. eBay stopped the auctions and temporarily suspended the defendant as a seller. UMG subsequently sued the defendant for copyright infringement. On the

the DMCA (and the preliminary injunction that subsequently issued in fact was directed at the competitor, not the service provider). See *Amaretto Ranch Breedables v. Ozimals, Inc.*, 97 U.S.P.Q.2d 1664, 2010 WL 5387774 (N.D. Cal. Dec. 21, 2010) (entering an ex parte TRO). The court subsequently ruled that DMCA-related state law claims were preempted by section 512(f). See *Amaretto Ranch Breedables, LLC v. Ozimals, Inc.*, No. C 10-05696 CRB, 2011 WL 2690437 (N.D. Cal. July 8, 2011); see generally *infra* § 4.12[9][F].

⁴³See *supra* § 4.12[9][C].

⁴⁴See *supra* § 4.12[9][C].

⁴⁵See, e.g., *Flynn v. Siren-Bookstrand, Inc.*, No. 4:13-CV-3160, 2013 WL 5315959 (D. Neb. Sept. 20, 2013) (declining to grant a TRO in a suit by a book author brought against the publisher of some but not all of her books seeking a TRO to prevent the publisher from sending further DMCA notices to Amazon.com for two books that the plaintiff claimed to have self-published in ebook and paper format, which had been suspended by Amazon.com in response to DMCA notices sent by the publisher, because section 512(f) did not expressly authorize injunctive relief and the plaintiff had not demonstrated a sufficient threat of irreparable harm that could not be ameliorated with money damages); see generally *infra* § 4.13 (equitable remedies in copyright cases).

⁴⁶*UMG Recordings, Inc. v. Augusto*, 558 F. Supp. 2d 1055 (C.D. Cal. 2008), *aff'd on other grounds*, 628 F.3d 1175 (9th Cir. 2011) (affirming that the promotional CDs were transferred, not licensed).

merits, the court ruled for the defendant, holding that under the first sale doctrine UMG had given away, rather than licensed, the promotional CDs to music industry insiders, who then lawfully resold them to Augusto.⁴⁷ Judge Otero nonetheless held that UMG had acted with subjective good faith in sending a DMCA notice to eBay alleging that the defendant was infringing its copyrights because UMG believed it could enforce the licensing language stamped on promo CDs, had carefully documented the defendant's conduct, and was aware that the defendant had previously entered into a consent judgment where he admitted to selling promo CDs and admitted that this act violated the owner's copyright. The court ruled that defendant's argument that UMG should have known better did not raise a genuine issue of material fact "given the uncertainty of the law in this area."⁴⁸

In perhaps the first case decided under section 512(f)—*Arista Records, Inc. v. MP3Board, Inc.*⁴⁹—a court in the Southern District of New York ruled that section 512(f) did not authorize liability for a notification that was merely insufficient, in the absence of evidence that the copyright owner or its agents knowingly materially misrepresented the material or activity that was infringing.⁵⁰

A copyright owner's claim under section 512(f) over an alleged misrepresentation in a counter notification likewise will be dismissed where the defendant had a good faith basis for submitting the notice.⁵¹

On balance, the risk of an award of damages and attorneys'

⁴⁷That aspect of the court's decision is discussed in section 16.02 in the context of the first sale doctrine and ultimately was affirmed on appeal.

⁴⁸558 F. Supp. 2d at 1064.

⁴⁹*Arista Records, Inc. v. Mp3Board, Inc.*, No. 00 CIV. 4660(SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002).

⁵⁰This ruling is discussed further in § 4.12[9][F].

⁵¹*See, e.g., Hosseinzadeh v. Klein*, 276 F. Supp. 3d 34, 37 (S.D.N.Y. 2017) (dismissing the copyright owner's section 512(f) DMCA claim where the defendant's use of plaintiff's video, in the work that was the subject of the plaintiff's takedown notice, was a fair use and, even if it wasn't, the defendant had a subjective good faith belief that his use was permitted as a fair use); *see also, e.g., Hughes v. Benjamin*, 437 F. Supp. 3d 382, 394-95 (S.D.N.Y. 2020) (dismissing plaintiff's section 512(f) claim, in a dispute between YouTubers, where the defendant represented in a counter notification that her use was a fair use and "highly transformative," where the court ultimately concluded that the use was indeed fair and the assertion that defendant's video was "highly transformative" was merely hyperbole

fees creates an incentive for responsible copyright owners to think twice before sending a notice in cases like the “Dancing Baby” suit where their position may be questionable, while allowing meaningful relief where substantial injuries could result from misrepresentations and deterring frivolous suits for damages in cases where honest mistakes are made by copyright owners.

Sanctions for misrepresentations under section 512(f) must be based on misrepresentations under section 512. Other alleged misrepresentations involving claims other than copyright infringement are not actionable under this section⁵²—although they potentially could support other causes of action, as discussed later in this chapter in section 4.12[9][F].⁵³ Some district courts, however, have held that state law claims arising from DMCA takedown notices are preempted by the DMCA under the principle of field preemption.⁵⁴ These issues are addressed in greater detail in section 4.12[9][F].

and not legally significant).

⁵²See *Twelve Inches Around Corp. v. Cisco Systems, Inc.*, No. 08 Civ. 6896 (WHP), 2009 WL 928077 (S.D.N.Y. Mar. 12, 2009) (granting summary judgment for the defendant on a claim alleging misrepresentation about trademark ownership in a takedown notice sent to a service provider).

⁵³See, e.g., *Flava Works, Inc. v. Gunter*, No. 10 C 6517, 2013 WL 4734002 (N.D. Ill. Sept. 3, 2013) (denying plaintiff’s motion to dismiss the defendant’s counterclaim for tortious interference with contract and misrepresentation of intellectual property infringement (pursuant to 17 U.S.C.A. § 512(f)) based on alleged misrepresentations about the extent of allegedly infringing material available on the myVidster.com website made to defendant’s service providers and in DMCA notifications); see generally *infra* § 4.12[9][F].

⁵⁴See, e.g., *Tine Bak LLC v. Selkatz, Inc.*, CV 20-5065 DSF (SK), 2020 WL 9074806, at *4-6 (C.D. Cal. Nov. 30, 2020) (dismissing plaintiff’s claim for tortious interference, premised on a false takedown notice, as preempted by the DMCA); *Beyond Blond Productions, LLC v. Heldman*, CV 20-5581 DSF (GSJx), 2020 WL 4772796, at *2-3 (C.D. Cal. Aug. 17, 2020) (dismissing claims for tortious interference, unfair competition, and trade libel, as preempted by the DMCA, to the extent they depended on alleged misrepresentations in DMCA takedown notices); *Furnituredealer.net, Inc. v. Amazon.com, Inc.*, Civil No. 18-232 (JRT/HB), 2019 WL 3738622, at *3-5 (D. Minn. Aug. 8, 2019) (dismissing with prejudice, as preempted by the online service provider provisions of the DMCA, common law claims of tortious interference with existing business relationships and prospective economic advantage, after plaintiff brought actions for the alleged appearance of copyrighted marketing content on defendant’s e-commerce website); *Stardock Systems, Inc. v. Reiche*, Case No: C 17-

Jurisdiction based on DMCA and takedown notices is separately analyzed in chapter 53 and in particular in section 53.04[5][F].

4.12[9][E] Subpoenas to Identify Infringers

Section 512(h) of the DMCA authorizes copyright owners to obtain a special subpoena to compel a service provider to

07025 SBA, 2019 WL 8333514, at *4-8 (N.D. Cal. May 14, 2019) (dismissing, as preempted by the DMCA, claims of tortious interference with prospective economic advantage and contractual relations, arising out of allegedly bad-faith takedown notices submitted to videogame platforms and distributors involving the “Star Control” franchise); *Complex Media, Inc. v. X17, Inc.*, Case No. CV 18-07588 SJO (AGRx), 2019 WL 2896117, at *4-6 (C.D. Cal. Mar. 4, 2019) (granting defendant’s anti-SLAPP motion and dismissing with prejudice plaintiff’s claim for interference with contract (and awarding attorneys’ fees to the defendant under the anti-SLAPP statute) in a suit brought by a copyright owner under section 512(f) (and for related state claims) alleging that the defendant repeatedly sent unjustified DMCA takedown notices to YouTube, jeopardizing its entitlement to use that platform); *infra* § 37.02[3] (analyzing the case in connection with anti-SLAPP motions); *Amaretto Ranch Breedables, LLC v. Ozimals, Inc.*, No. C 10-05696, 2011 WL 2690437, at *4 (N.D. Cal. July 8, 2011) (holding preempted Amaretto’s interference with contract claim, as well as “any other state law claim to the extent such claim is based on Ozimals’s DMCA Takedown Notifications” in a suit alleging that DMCA takedown notices were wrongfully sent, even though the material addressed in the notices was not actually removed); *Lenz v. Universal Music Corp.*, No. C 07-03783, 2008 WL 962102, at *4 (N.D. Cal. Apr. 8, 2008) (dismissing plaintiff’s claim for intentional interference with contractual relations based on field preemption, but allowing leave to amend “because it is possible that Lenz may be able to allege that the take down notice was based on YouTube’s Terms of Use policy rather than the DMCA”); *Online Policy Group v. Diebold*, 337 F. Supp. 2d 1195, 1205-06 (N.D. Cal. 2004) (dismissing plaintiff’s claim for tortious interference with contractual relations based on field preemption; “Even if a copyright holder does not intend to cause anything other than the removal of allegedly infringing material, compliance with the DMCA’s procedures nonetheless may result in disruption of a contractual relationship: by sending a letter, the copyright holder can effectuate the disruption of ISP service to clients. If adherence to the DMCA’s provisions simultaneously subjects the copyright holder to state tort law liability, there is an irreconcilable conflict between state and federal law.”); *see also Rock River Communications, Inc. v. Universal Music Group, Inc.*, No. CV08–635 CAS (AJWx), 2011 WL 1598916, at *13-16 (C.D. Cal. Apr. 27, 2011) (granting summary judgment for the defendants on plaintiff’s section 512(f) claim because the cease and desist letter at issue was not a DMCA notice and accordingly holding that plaintiff’s tortious interference claim arising out of the cease and desist letter was not preempted by the DMCA); *see generally infra* § 4.12[9][F] (analyzing field preemption of state law claims arising out of allegedly unjustified DMCA takedown notices).

disclose the identity of an alleged infringer prior to the initiation of litigation.¹

Where applicable, a copyright owner or person authorized to act on the owner's behalf may request the clerk of "any United States district court"² to issue a subpoena to a service provider requiring identification of an alleged infringer.³ An application must include a copy of a notification, a proposed subpoena, and a sworn declaration stating that the copyright owner will only use the information obtained from the subpoena for protecting its rights under the Copyright Act.⁴

If a request for a subpoena contains each of these elements and the notification substantially meets the statutory requirements, a subpoena will issue.⁵ A DMCA subpoena "shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose . . . information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider."⁶ Upon receiving a subpoena, a service provider must expeditiously disclose the information required by it, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.⁷ To "the greatest extent practicable . . .," the procedures for issuing, delivering and enforcing service provider subpoenas are to be governed by those provisions of the Federal Rules of Civil Procedure governing the issuance, service and enforcement of a subpoena *duces tecum*.

[Section 4.12[9][E]]

¹17 U.S.C.A. § 512(h); *see generally* *Signature Management Team, LLC v. Automattic, Inc.*, 941 F. Supp. 2d 1145 (N.D. Cal. 2013) (denying a blogger's motion to quash a section 512(h) subpoena on First Amendment grounds); *In re Subpoena Issued Pursuant to the Digital Millennium Copyright Act to: 43SB.com, LLC*, No. MS07-6236-EJL, 2007 WL 4335441 (D. Idaho Dec. 7, 2007) (denying motion to quash where the requirements for a section 512(h) subpoena had been met, but quashing the subpoena to the extent directed at comments critical of the plaintiff and not copyright infringement).

²It is unclear whether Congress meant by this language to authorize national jurisdiction. *See infra* chapter 53.

³17 U.S.C.A. § 512(h)(1).

⁴17 U.S.C.A. § 512(h)(2).

⁵17 U.S.C.A. § 512(h)(4).

⁶17 U.S.C.A. § 512(h)(3).

⁷17 U.S.C.A. § 512(h)(5).

The special subpoena contemplated by section 512(h) could issue in any federal case, including a lawsuit brought against the alleged infringer (either to obtain injunctive relief if a counter notification were filed or strictly for damages if no objection were raised to the original notification). An unidentified infringer potentially could be sued by its fictitious or pseudonymous Internet identification. Upon the service provider's compliance with the terms of the subpoena, the copyright owner could then serve the alleged infringer and, if appropriate, amend its complaint to properly identify the alleged infringer.⁸

When challenged through a motion to quash, a subpoena may not issue, or may issue subject to conditions, where plaintiff's claim appears weak or impinges upon First Amendment or fair use rights.⁹

While section 512(h) in theory should provide a quick, easy, inexpensive mechanism for copyright owners to expeditiously identify pseudonymous infringers at the outset of a dispute, in practice courts have limited the reach of section 512(h) in cases involving peer-to-peer file sharing. Several courts have held that section 512(h), which by its terms authorizes the issuance of a subpoena upon submission of a substantially complying notification, potentially could only apply to cases involving user storage and information location tools (and at least some forms of caching)—which are the only safe harbors for which notifications apply—and therefore does not authorize the issuance of a subpoena to a service provider acting solely as a conduit for communications not actually stored on its own servers (since there is no provision for notifications where the relevant liability limitation is for the transitory digital network communications¹⁰ safe harbor).¹¹

Hence, in cases involving peer-to-peer file sharing where

⁸For more information on suing anonymous and pseudonymous Internet actors, see *infra* §§ 37.02, 50.06, 57.03.

⁹See, e.g., *In re DMCA Subpoena to Reddit, Inc.*, 441 F. Supp. 3d 875 (N.D. Cal. 2020) (quashing a subpoena seeking the identity of an anonymous poster on the Jehovah's Witness forum on Reddit, holding that its use of a Jehovah's Witness chart and advertisement on Reddit was a fair use).

¹⁰17 U.S.C.A. § 512(a).

¹¹See, e.g., *Recording Industry Ass'n of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229, 1233–37 (D.C. Cir. 2003), *cert denied*, 543 U.S. 924 (2004); *In re Charter Communications, Inc., Subpoena*

copyright owners have sought to compel service providers to produce identifying information for pseudonymous infringers, these courts have quashed subpoenas, holding that, by virtue of the nature of peer-to-peer communications, allegedly infringing material was not actually stored on the servers of the service provider to which the DMCA was directed.

While other courts may adopt a broader interpretation of the scope of section 512(h),¹² these cases present formidable potential obstacles to copyright owners seeking to take advantage of the special subpoena provision of the DMCA in cases that do not involve material stored on a service provider's servers or links or other information location tools (or in limited circumstances, cached content removed from the original location that remains on a service provider's servers).

In one unreported case, a magistrate judge extended the rationale of cases holding that section 512(h) subpoenas

Enforcement Matter, 393 F.3d 771, 775–77 (8th Cir. 2005); *In re Subpoena To University of North Carolina at Chapel Hill*, 367 F. Supp. 2d 945, 949 (M.D.N.C. 2005).

In *dicta*, the majority in *In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771 (8th Cir. 2005) raised without deciding the possibility that section 512(h) “may unconstitutionally invade the power of the judiciary by creating a statutory framework pursuant to which Congress, via statute, compels a clerk of a court to issue a subpoena, thereby invoking the court’s power.” *Id.* at 777–78. The majority also wrote in *dicta* that Charter Communications had “at least a colorable argument that a judicial subpoena is a court order that must be supported by a case or controversy at the time of its issuance.” *Id.* at 778.

In the *Chapel Hill* case, the court also quashed the subpoena because it had called for production of information in Raleigh, which was outside of the Middle District of North Carolina. In so ruling, the court held that Rule 45—which allows for service within 100 miles of the place of a deposition, hearing, trial, production, or inspection specified in a subpoena was inapplicable to pretrial subpoenas issued pursuant to § 512(h).

¹²See, e.g., *In re Charter Communications, Inc., Subpoena Enforcement Matter*, 393 F.3d 771, 778–86 (8th Cir. 2005) (Murphy, J., dissenting) (arguing forcefully that the majority had “focus[ed] too narrowly in its reading of the DMCA, overlook[ed] certain plain language used by Congress, and fail[ed] to give effect to the statute as a whole” where section 512(h) on its face does not limit a copyright owner’s ability to obtain a subpoena based on the function performed by a service provider).

In one case, *Fatwallet, Inc. v. Best Buy Enterprise Services, Inc.*, Copy. L. Rep. (CCH) ¶ 28,799 (N.D. Ill. Apr. 12, 2004), a court ruled that a service provider lacked standing to object to a DMCA subpoena on behalf of anonymous posters.

could not apply when the basis for a service provider's connection to an alleged infringer was the transitory digital network communications safe harbor, to quash a subpoena served with a DMCA notice and affidavit for material stored at the direction of a user, where the material at issue had been removed from the defendant's blog prior to the time the notice and subpoena issued. In *Maximized Living, Inc. v. Google, Inc.*,¹³ Magistrate Judge Elizabeth LaPorte granted the motion to quash of a pseudonymous blogger, ruling that section 512(h) does not authorize issuance of a subpoena to obtain identifying information for past infringement that has ceased and thus can no longer be removed or disabled and is limited to information about currently infringing activity. In so ruling, Judge LaPorte relied on the language of section 512(c) which, in describing the information required to be included in a DMCA notification, is phrased in the present, rather than past tense. The plain terms of section 512(h) which governs the issuance of a DMCA subpoena, however, merely require "a copy of a notification described in subsection (c)(3)(A) . . ."¹⁴ without further qualification, a proposed subpoena and a "sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title."¹⁵ There is nothing on the face of section 512(h) that limits its application to cases involving *present* infringement. Indeed, to the contrary, section 512(h) on its face contemplates that a DMCA subpoena could issue *after* the accompanying notification. Section 512(h)(5), in setting forth the obligations of a service provider upon service of a DMCA subpoena, specifically refers to the subpoena as "either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A) . . ."¹⁶ Since service providers are required to expeditiously disable access to or remove material in response to a substantially complying notification,¹⁷ any subpoena served after a notification could well relate to material no longer on a site. There is

¹³*Maximized Living, Inc. v. Google, Inc.*, No. C 11-80061 Misc. CRB (EDL), 2011 WL 6749017 (N.D. Cal. Dec. 22, 2011).

¹⁴17 U.S.C.A. § 512(h)(2)(A).

¹⁵17 U.S.C.A. § 512(h)(2)(C).

¹⁶17 U.S.C.A. § 512(h)(5).

¹⁷17 U.S.C.A. § 512(c); see generally *supra* §§ 4.12[6][B], 4.12[9][B] (addressing service provider obligations in response to a substantially

simply no textual basis for reading into section 512(h) the requirement that infringement be ongoing for a section 512(h) subpoena to issue and *Maximized Living* should be viewed as wrongly decided.¹⁸

If a copyright owner is unable to obtain a DMCA subpoena, it may still seek a regular third-party subpoena, petition for pre-service discovery or, where available, sue a “John Doe” defendant and issue a third-party subpoena to the service provider.¹⁹

compliant DMCA notification).

¹⁸If DMCA subpoenas could only issue where infringement was ongoing, an alleged infringer could easily nullify the subpoena merely by voluntarily removing the material addressed by the accompanying notification and then moving to quash the subpoena (potentially even re-posting the material after winning the motion). A copyright owner, in turn, would be hesitant to send a DMCA notice in advance of a subpoena, even though the DMCA’s text is permeated with terms such as *expeditiously* that underscore an intent by Congress to provide for prompt remedies in recognition of the harm that may be caused by online infringement. Given that a copyright owner may sue for injunctive relief even when a defendant has voluntarily discontinued his infringing activity (*infra* § 4.13), and may sue for damages for past infringement (*infra* § 4.14), it stretches credibility to believe that Congress intended that a DMCA subpoena would be effective only for so long as material remains online. The court’s construction of section 512(h) is inconsistent with Congress’s obvious attempt to provide a fast, easy mechanism for copyright owners to identify so that they may then sue online infringers.

These concerns are underscored by the facts of *Maximized Living*. In that case, the copyright owner had originally obtained its subpoena on March 22, 2011 (when the alleged infringement was ongoing), but the subpoena was quashed for procedural irregularities and substantive challenges, with leave to re-file, on May 25, 2011. The next day, counsel for the third party notified the plaintiff that the blogger had voluntarily removed the material at issue. Hence, by the time the plaintiff served a new subpoena, the material had already been taken down—and the blogger’s lawyer then moved to quash the re-filed subpoena on that basis.

¹⁹See, e.g., *Sony Music Entertainment Inc. v. Does 1-40*, 326 F. Supp. 2d 556 (S.D.N.Y. 2004) (denying a motion to quash based on findings that (1) file sharing was not, for the most part, expression, and whatever First Amendment protection might exist did not extend to infringement of copyrights; (2) the First Amendment rights of individuals to remain anonymous were not so strong that they precluded copyright owners from using the judicial process to pursue meritorious copyright infringement actions; and (3) defendants had, at most, only a minimal expectation of privacy, which did not defeat plaintiffs’ right to conduct discovery); see also *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 119 (2d Cir. 2010) (adopting Judge Chin’s analysis in *Sony*). Under *Doe 3* and *Sony*, whether a subpoena to compel the disclosure of the identity of an anonymous file

The approach of subpoenaing customer account information to identify pseudonymous users outside of the DMCA became commonplace many years ago in suits brought by record companies against individuals accused of illegal file sharing.²⁰

In *Columbia Pictures, Inc. v. Bunnell*,²¹ the court even ordered the operators of a BitTorrent service to preserve server log data to allow identification of infringers.

At one time, some copyright owners also sought to join large numbers of BitTorrent users as Doe defendants in a single proceeding. Some courts quashed these subpoenas, severed claims, or even dismissed cases entirely where the basis for asserting a claim was merely an IP address.²²

sharer should be quashed turns on consideration of (1) the concreteness of the plaintiff's showing of a *prima facie* claim of actionable harm; (2) the specificity of the discovery request; (3) the absence of alternative means to obtain the subpoenaed information; (4) the need for the subpoenaed information to advance the claim; and (5) the objecting party's expectation of privacy. *Id.* Different considerations, however, come into play in seeking to unmask a pseudonymous defendant's identity once liability has been established. See *Signature Management Team, LLC v. Doe*, 876 F.3d 831 (6th Cir. 2017); see generally *infra* § 37.02[1] (analyzing the case and the balancing test it articulates).

²⁰See, e.g., *LaFace Records, LLC v. Does 1-5*, No. 2:07-CV-187, 2007 WL 2867351 (W.D. Mich. Sept. 27, 2007); *Warner Brothers Records, Inc. v. Does 1-4*, Copy. L. Rep. (CCH) ¶ 29,396 (D. Utah 2007); *Capitol Records, Inc. v. Doe*, Civil No. 07-cv-1570-JM (POR), 2007 WL 2429830 (S.D. Cal. Aug. 24, 2007); *Warner Bros. Records Inc. v. Does 1-20*, Civil No. 07-cv-01131-LTB-MJW, 2007 WL 1655365 (D. Colo. June 5, 2007); *Arista Records LLC v. Does 1-9*, Civil Action No. 07-cv-00628-EWN-MEH, 2007 WL 1059049 (D. Colo. Apr. 4, 2007); *Interscope Records v. Does 1-7*, 494 F. Supp. 2d 388 (E.D. Va. 2007).

²¹*Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443 (C.D. Cal. 2007).

²²See, e.g., *AF Holdings, LLC v. Does 1-1058*, 752 F.3d 990 (D.C. Cir. 2014) (vacating and remanding an order directing ISPs to comply with discovery of numerous defendants, where personal jurisdiction could not be established and joinder of the unknown individuals was improper and, among other things, "AF Holdings has provided no reason to think that the Doe defendants it named in this lawsuit were ever participating in the same swarm at the same time. Instead, it has simply set forth snapshots of a precise moment in which each of these 1,058 Does allegedly shared the copyrighted work—snapshots that span a period of *nearly five months*."); *Strike 3 Holdings, LLC v. Doe*, 331 F.R.D. 14 (E.D.N.Y. 2019) (denying plaintiff's request for expedited discovery to identify the persons associated with identified IP addresses; declining to apply the Second Circuit's *Arista Records, LLC v. Doe 3*, 604 F.3d 110 (2d Cir. 2010) test because that case involved a motion to quash, as unduly burdensome

By contrast, other courts in past years allowed BitTorrent swarm suits to proceed in a single action, at least pending discovery.²³

under Rule 45, a subpoena properly issued under Rule 26, rather than a motion under Rule 26 for expedited discovery, and the court in *Arista* acknowledged that the factors listed were the principal ones—but not the only ones—to consider); *Bicycle Peddler, LLC v. John Does 1-177*, No. 13-cv-0671-WJM-KLM, 2013 WL 1103473 (D. Colo. Mar. 15, 2013) (severing and dismissing claims against defendants 2-177); *Third Degree Films v. Does 1-47*, 286 F.R.D. 188 (D. Mass. 2012) (severing claims); *Patrick Collins, Inc. v. John Doe 1*, 288 F.R.D. 233 (E.D.N.Y. 2012) (adopting Magistrate’s recommendation to deny joinder); *CineTel Films, Inc. v. Does 1-1,052*, 853 F. Supp. 2d 545 (D. Md. 2012) (severing claims); *Media Products, Inc. v. Does 1-58*, Civil No. JFM 8:12-cv-00348, 2012 WL 1150816 (D. Md. Apr. 4, 2012); *Patrick Collins, Inc. v. Does 1-23*, Civil No. JFM 8:12-cv-00087, 2012 WL 1144918 (D. Md. Apr. 4, 2012); *Third Degrees Films, Inc. v. Does 1-131*, 280 F.R.D. 493 (D. Ariz. 2012) (severing claims); *Liberty Mutual Holdings, LLC v. BitTorrent Swarm*, 277 F.R.D. 672, 675–76 (S.D. Fla. 2011) (severing claims against 18 defendants (and dismissing all but the first defendant) where plaintiff alleged that the defendants used BitTorrent on different days and times and because of the decentralized nature of BitTorrent swarms; “Merely participating in a BitTorrent swarm does not equate to participating in the same ‘transaction, occurrence, or series of transactions or occurrences.’”); *Hard Drive Productions, Inc. v. Does 1-188*, 809 F. Supp. 2d 1150 (N.D. Cal. 2011) (granting Doe defendants’ motion to quash in a suit brought against Doe defendants from different BitTorrent swarms who did not act simultaneously); *On The Cheap, LLC v. Does 1-5011*, 280 F.R.D. 500 (N.D. Cal. 2011) (severing Doe defendants 1-16 and 18-5011); *Nu Image, Inc. v. Does 1-23,322*, 799 F. Supp. 2d 34 (D.D.C. 2011) (denying jurisdictional discovery about any defendants who reside outside the District of Columbia).

²³See *Malibu Media, LLC v. Does 1-14*, 287 F.R.D. 513 (N.D. Ind. 2012) (denying motion to sever and motion to quash); *Patrick Collins, Inc. v. Does 1-21*, 282 F.R.D. 161 (E.D. Mich. 2012) (Magistrate recommending denial of motion to quash and motion to dismiss for misjoinder); *John Wiley & Sons, Inc. v. Doe Nos. 1-30*, 284 F.R.D. 185 (S.D.N.Y. Sep. 19, 2012) (denying defendant’s motion for protective order and motion to quash subpoena served on nonparty internet service provider); *Hard Drive Productions, Inc. v. Does 1-1,495*, 892 F. Supp. 2d 334 (D.D.C. 2012) (denying motion for emergency stay and reconsideration); *Raw Films, Ltd. v. John Does 1-15*, Civil Action No. 11-7248, 2012 WL 1019067 (E.D. Pa. Mar. 26, 2012) (denying motion to quash); *Liberty Mutual Holdings, LLC v. Does 1-62*, No. 11-cv-575-MMA (NLS), 2012 WL 628309 (S.D. Cal. Feb. 24, 2012) (denying motion to quash and motion to dismiss where the defendants were alleged to be part of the same BitTorrent swarm and all of the IP addresses identified with the defendants shared the same unique hash); *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239 (S.D.N.Y. Jan. 30, 2012) (declining to sever claims at an early stage in the proceedings); *Call of the Wild Movie, LLC v. Does 1-1,062*, 770 F. Supp. 2d 332, 344–45

In some of these cases, courts expressed concern about joining large numbers of unnamed and unrepresented defendants, as a way for plaintiffs to avoid paying multiple filing fees, while other courts deemed joinder proper or deferred consideration pending discovery where plaintiffs made detailed showings of the connections between the Doe defendants and the underlying transactions. In at least one case where discovery was permitted at an early stage, the court subsequently ordered the plaintiff to use IP address lookup services to determine the presumptive location of defendants and dismiss those where jurisdiction and venue likely were improper.²⁴ Some courts expressly ruled that joinder was permissible at the outset of a case for purposes of subpoenaing an ISP to determine the identity of defendants, noting that severance could always be ordered at a

(D.D.C. 2011) (denying a motion to quash based on a finding that the claims included common questions of law or fact and that joinder would not prejudice the parties or result in needless delay and was appropriate at least at the initial stage of the proceedings in that case); *Call of the Wild Movie, LLC v. Smith*, 274 F.R.D. 334 (D.D.C. 2011) (declining to quash subpoenas issued to ISPs seeking the identifying information about five putative file sharers who allegedly downloaded and illegally distributed plaintiff's film and denying their motion to dismiss for improper joinder at the discovery stage, holding that discovery was required to determine whether the court had personal jurisdiction over the putative users); *Patrick Collins, Inc. v. Does 1-2,590*, No. C 11-2766 MEJ, 2011 WL 4407172 (N.D. Cal. Sept. 22, 2011) (holding that the plaintiff showed good cause under *Columbia Ins. Co. v. seescandy.com*, 185 F.R.D. 573, 578–80 (N.D. Cal. 1999) for *ex parte* discovery and that joinder of BitTorrent users was appropriate where "Plaintiff has at least presented a reasonable basis to argue that the BitTorrent protocol functions in such a way that peers in a single swarm downloading or uploading a piece of the same seed file may fall within the definition of 'same transaction, occurrence, or series of transactions or occurrences' for purposes of Rule 20(a)(1)(A)."); *Maverick Entertainment Group, Inc. v. Does 1-2,115*, 810 F. Supp. 2d 1 (D.D.C. 2011) (declining to quash a subpoena or dismiss putative users for misjoinder pending discovery to determine whether the court had personal jurisdiction over the putative users); *Voltage Pictures, LLC v. Does 1-5,000*, 79 Fed. R. Serv. 3d 891 (D.D.C. 2011) (ruling the same way in a companion case); *Donkeyball Movie, LLC v. Does 1-171*, 810 F. Supp. 2d 20 (D.D.C. 2011) (ruling the same way); *West Coast Productions, Inc. v. Does 1-5829*, 275 F.R.D. 9 (D.D.C. 2011) (denying defendants' motion to proceed anonymously and to quash subpoenas seeking their identities, holding that the argument that court lacked personal jurisdiction was premature, that permissive joinder was appropriate and that the defendants, as subscribers, lacked standing to make procedural objections to the subpoenas).

²⁴See *Patrick Collins, Inc. v. Does 1-2,590*, No. C 11-2766 MEJ, 2011 WL 7460101 (N.D. Cal. Dec. 7, 2011).

later stage in the proceedings.

In many instances, it is more time consuming and expensive to proceed with John Doe subpoenas than DMCA subpoenas. Both the service provider—and potentially later the individual John Does—may move to quash Doe subpoenas, causing additional time delays and expense. In addition, the practices and approaches to pre-service discovery among the different state and federal courts are not uniform.²⁵ Of course, depending on the misconduct alleged, a DMCA subpoena may not yield the contact information of a suspected infringer, for the reasons outlined earlier in this section. Even where a DMCA subpoena could yield the required information, courts nonetheless may permit expedited pre-service discovery through John Doe subpoenas, although failing to comply with the requirements for a DMCA subpoena (or show that a DMCA subpoena would not likely result in the information sought by a Doe subpoena) could weigh against issuance of the Doe subpoena.²⁶

While mainstream music services have largely discontinued efforts to sue thousands of individual users to deter file sharing, porn companies have picked up on the practice as a way to generate revenue. The rise of porn trolls—who seek premium payments from individual users accused of downloading or merely just viewing videos online—has generated a substantial number of court opinions. Courts have generally permitted copyright owners in porn troll cases to compel the disclosure of contact information associated with IP addresses—which are sought to extract settlements from individuals who may be especially sensitive to the potential

²⁵See generally *infra* §§ 37.02 (suing anonymous defendants in defamation and other state law cases), 57.03 (anonymity and pseudonymity in litigation). Unless a copyright owner has separate state claims against a Doe defendant, the subpoena would have to issue in federal court (since federal courts have exclusive jurisdiction over copyright matters).

²⁶See *Paisley Park Enterprises, Inc. v. Ziani*, Case No. 18-cv-2556 (DSD/TNL), 2018 WL 6567828 (D. Minn. Dec. 13, 2018) (granting in part plaintiffs' motion for expedited discovery, in a case brought by the Estate of Prince Rogers Nelson and others to obtain, from various online music services, the identity of people selling bootlegged copies of Prince's music, even though plaintiffs did not explain their failure to seek a DMCA subpoena, while also denying their request for the identification of financial institutions and accounts associated with the bootlegging enterprise which—while relevant to plaintiffs' claims—was unrelated to the petition's objective of allowing plaintiffs to identify the defendants and more easily effectuate service upon them).

for public embarrassment²⁷—subject to entry of a protective order “in light of the substantial risk for false positive identification [associated with an IP address] that could result in ‘annoyance, embarrassment, oppression, or undue burden of expense.’ ”²⁸

²⁷See, e.g., *Strike 3 Holdings, LLC v. Doe*, Case No. 1:18-cv-02651-AJN, 2018 WL 2229124, at *3 (S.D.N.Y. Apr. 25, 2018) (granting plaintiff leave to serve early discovery on Spectrum under the *Arista Records* standard, subject to a protective order, given the apparent lack of other means by which the plaintiff could have sought out the defendant’s identity; “while the Court is sensitive to the fact that Defendant’s viewing of these particular copyrighted works may be the source of public embarrassment, courts in this district have nonetheless concluded that ‘ISP subscribers have a minimal expectation of privacy in the sharing of copyrighted material.’ ”) (quoting *Malibu Media, LLC v. John Does 1-11*, No. 12 Civ. 3810(ER), 2013 WL 3732839, at *6 (S.D.N.Y. July 16, 2013)).

²⁸*Strike 3 Holdings, LLC v. Doe*, Case No. 1:19-cv-04840-AJN, 2019 WL 3242570, at *3 (S.D.N.Y. July 9, 2019) (allowing Strike 3 to serve a Rule 45 subpoena on Verizon, to obtain information to identify the true name and current and permanent address (but not the email address or telephone numbers) of the John Doe defendant, together with a copy of the court order, allowing Verizon 60 days to serve a copy of the subpoena and court order on its customer, the John Doe defendant, and then allowing the Doe defendant 60 days to move to quash before any information may be turned over, and outlining a notice to the defendant to be served with the order); see also, e.g., *Strike 3 Holdings, LLC v. Doe*, Nos. 1:18-cv-2674-NLH-JS, 1:18-cv-12585-NLH-JS, 1:18-cv-12586-NLH-JS, 1:18-cv-16564-NLH-JS, 1:18-cv-16565-NLH-JS, 1:18-cv-16566-NLH-JS, 1:18-cv-17594-NLH-JS, 1:18-cv-17595-NLH-JS, 1:19-cv-00894-NLH-JS, 1:19-cv-00895-NLH-JS, 1:19-cv-14014-NLH-JS, 1:19-cv-14015-NLH-JS, 1:19-cv-14016-NLH-JS, 2020 WL 3567282, at *11 (D.N.J. July 30, 2020) (remanding the matter to the magistrate judge for consideration of an appropriate protective order to enter); *Strike 3 Holdings, LLC v. Doe*, Case No. 19-cv-00723-JCS, 2019 WL 2996428 (N.D. Cal. July 9, 2019) (denying a Doe defendant’s motion to quash a subpoena, subject to the caveat that “any name or other personal identifying information of any current or proposed defendant shall be filed UNDER SEAL in all filings and not otherwise disclosed.”); *Malibu Media, LLC v. Doe*, Civil Action No. 3:19-cv-00808 (CSH), 2019 WL 2537671 (D. Conn. June 20, 2019) (authorizing a subpoena under similar conditions to the July 9, 2019 S.D.N.Y. order); *Strike 3 Holdings, LLC v. Doe*, No. 1:18-cv-2211 (PLF/GMH), 2019 WL 1778054 (D.D.C. Apr. 23, 2019) (allowing pre-service discovery, with procedural safeguards); *Malibu Media, LLC v. Doe*, Civil Action No. 3:18-cv-00355 (CSH), 2019 WL 1529956 (D. Conn. Apr. 9, 2019) (authorizing a subpoena under similar conditions); *Strike 3 Holdings, LLC v. Doe*, 1:18-CV-01490 EAW, 2019 WL 1529339 (W.D.N.Y. Apr. 4, 2019) (denying defendant’s motion to quash, but granting defendant’s motion to proceed anonymously); *Strike 3 Holdings, LLC v. Doe Subscriber Assigned IP Address 68.82.141.39*, 370 F. Supp. 3d 478 (E.D. Pa. 2019) (denying defendant’s motion to quash, but entering a protective order to safeguard

the defendant); *Strike 3 Holdings, LLC v. Doe*, No. 2:18-cv-02637-MCE-CKD, 2019 WL 935390 (E.D. Cal. Feb. 26, 2019) (denying defendant's motion to strike plaintiff's subpoena, where the court had "taken steps to protect Doe defendant's identity [so that] . . . he will not be prejudiced by allowing plaintiff to carry out the subpoena as ordered."); *Strike 3 Holdings, LLC v. Doe*, No. 19-CV-00160-EMC, 2019 WL 591459 at *2-3 (N.D. Cal. Feb. 13, 2019) (authorizing plaintiff to serve a Rule 45 subpoena on AT&T "to obtain the true name and address of the Doe Defendant at IP address 99.99.32.152" subject to a protective order; "In view of the potential implication of an innocent third party, and the sensitivity of the subject matter of the suit, the Court orders that Strike 3 Holdings shall not publicly disclose any of Defendant's identifying information until he has the opportunity to file a motion with this Court to be allowed to proceed in this litigation anonymously and that motion is ruled on by the Court. Defendant may file such a motion under seal."); *Strike 3 Holdings, LLC v. Doe*, No. 4:18-CV-04993-KAW, 2019 WL 468816 (N.D. Cal. Feb. 6, 2019) (denying motion to strike where the defendant claimed innocence, contending that the subscriber's router was not secure, that there was a 'false positive' on the IP address, and that the device with the subject IP address could not be found at the subscriber's location, because plaintiff was simply seeking to ascertain the defendant's identity and the court's *ex parte* order had required that the defendant's identity be kept confidential and out of public court filings); *Strike 3 Holdings, LLC v. Doe*, 329 F.R.D. 518 (S.D.N.Y. 2019) (authorizing a subpoena under similar conditions); *Strike 3 Holdings, LLC v. Doe*, 330 F.R.D. 552, 556-57 (D. Minn. 2019) (entering a multifaceted protective order to aid in protecting privacy interests and limit risks of embarrassment and misidentification); *Strike 3 Holdings, LLC v. Doe*, 18-CV-2648 (VEC), 2019 WL 78987, at *4 (S.D.N.Y. Jan. 2, 2019) (allowing discovery subject to a protective order permitting the defendant to proceed anonymously, ordering plaintiff not to initiate settlement negotiations until the Complaint had been properly served, and prohibiting plaintiff from obtaining any information from defendant's ISP other than defendant's name and address; "the Court is not entirely unsympathetic to Defendant's argument. As numerous district courts in this Circuit have pointed out, copyright holders such as Plaintiff are repeat litigants who have, in the past, engaged in 'abusive litigation practices,' including coercive settlement practices. . . . The Court, however, must balance Defendant's privacy right in the legitimate use of the internet against Plaintiff's interests in protecting its copyrighted material from infringement. That interest is not lessened by the salacious content of the material. . . ."); *Strike 3 Holdings, LLC v. Doe* 70.95.96.208, No. 18-CV-2720-GPC(WVG), 2018 WL 6649504, at *3 (S.D. Cal. Dec. 18, 2018) (granting plaintiff's motion for early discovery from Spectrum seeking only the true name and address of the subscriber associated with the IP address 70.95.96.208 during the time period of the allegedly infringing conduct described in plaintiff's Complaint, subject to various protections to ensure the confidentiality of the defendant's identity); *Strike 3 Holdings, LLC v. Doe*, Civil Action No. 3:18-CV-1332 (CSH), 2018 WL 4846676 (D. Conn. Oct. 5, 2018) (authorizing a subpoena on CSC Holdings, an ISP, on similar conditions as in the previously cited cases in this footnote involving Strike 3); *Malibu Media, LLC v. Doe*, No. 15-CV-4381(JFK),

Many courts have expressed concern,²⁹ and some have pushed back against this practice.³⁰ As explained by the D.C.

2015 WL 4923114, at *1 (S.D.N.Y. Aug. 18, 2015) (authorizing service of a subpoena on Verizon, subject to a protective order, but noting that “courts in this district have expressed concern . . . that disclosure of a defendant’s name or other identifying information in cases involving infringement of adult films could lead to abusive litigation through coercion.”); *In re BitTorrent Adult Film Copyright Infringement Cases*, 296 F.R.D. 80, 90 (E.D.N.Y. 2012) (allowing only limited pre-service discovery; Courts must exercise a “heightened degree of supervision” to ensure that a plaintiff is not using a barebones copyright infringement claim to “bludgeon” “hundreds of doe defendants” into “mass settlement.”).

²⁹See, e.g., *Malibu Media, LLC v. Mantilla*, No. 3:18-cv-01369 (JAM), 2020 WL 6866678, at *5 (D. Conn. Nov. 20, 2020) (granting motion for a default judgment but noting that “it appears from the sheer number of lawsuits filed by Malibu Media in this Court and across the nation that there is good reason to doubt the extent to which Malibu Media’s business model is premised on sales of copyrighted material as distinct from litigation income.”); *Malibu Media, LLC v. Doe*, 2020 WL 6043946, at *2 (N.D.N.Y. Oct. 13, 2020) (denying defendant’s motion for attorneys fees following a successful motion to dismiss, but observing: “There is certainly some merit to the chorus of criticism directed at Malibu Media by courts across the country. Here, Malibu Media appears to find it more convenient to abandon its supposedly ‘legitimate’ infringement claim rather than pursue it to vindication through the litigation process. Indeed, it could be inferred that Malibu Media declined to expend further resources and amend the Complaint after it became clear that Defendant would not simply roll over and agree to a quick settlement. Despite its objections to the contrary, Malibu Media’s action in this case appears consistent with many of the accusations levied against it by other courts, especially as it relates to strong-arming nuisance settlements under the threat of embarrassing litigation.”).

³⁰See, e.g., *AF Holdings, LLC v. Does 1-1058*, 752 F.3d 990 (D.C. Cir. 2014) (vacating and remanding an order directing ISPs to comply with discovery of numerous defendants, where the plaintiff did not have a good faith basis to believe that discovery would enable it to show that the court had personal jurisdiction over more than 1,000 defendants, joinder of the unknown individuals was improper because the plaintiff had no reason to think that the Doe defendants it named in this lawsuit were ever participating in the same swarm at the same time based on evidence it collected over a five month period, and the plaintiff’s lack of a good faith belief in the basis for suing unnamed defendants rendered the requested discovery of nonparty Doe defendants unduly burdensome); *Malibu Media, LLC v. Mullins*, No. 18-cv-06447, 2021 WL 122715 (N.D. Ill. Jan. 13, 2021) (awarding fees in a suit dismissed by the plaintiff; “Malibu has been publicly criticized for being a prolific litigant. As one court recently found, Malibu filed 7,183 cases nationwide from 2012 to 2018. . . . [T]he Court cannot consider these figures without wondering what motivates Malibu’s penchant for litigation—an interest in protecting its copyrights or using litigation as a profit center. Certainly most people who risk being identi-

fied in lawsuits as alleged porn downloaders are likely to simply settle the case as a means of avoiding public ridicule and embarrassment.”); *Malibu Media, LLC v. Duncan*, Civil Action No. 4:19-cv-02314, 2020 WL 567105 (S.D. Tex. Feb. 4, 2020) (dismissing plaintiff’s complaint and expressing concern over Malibu’s so-called “litigation-as-a-business strategy,” noting that others have labeled the company a “copyright troll”); *Strike 3 Holdings, LLC v. Doe*, 331 F.R.D. 14 (E.D.N.Y. 2019) (denying plaintiff’s request for expedited discovery to identify the persons associated with identified IP addresses; declining to apply the Second Circuit’s *Arista* factors because that case involved a motion to quash as unduly burdensome under Rule 45 a subpoena properly issued under Rule 26, rather than a motion under Rule 26 for expedited discovery, and the court in *Arista* acknowledged that the factors listed were the principal ones—but not the only ones—to consider); *Malibu Media, LLC v. Doe*, No. 15-CV-4369 (AKH), 2015 WL 4092417 (S.D.N.Y. July 6, 2015) (declining to allow pre-service discovery and characterizing Malibu Media as a copyright troll; “In light of Malibu’s history of abuse of court process and its failure to show ‘good cause,’ I decline to give it the benefit of an exception to the normal rules of discovery.”); see also *Cobbler Nevada, LLC v. Gonzalez*, 901 F.3d 1142, 1145 (9th Cir. 2018) (affirming dismissal of plaintiff’s complaint alleging infringement based on the defendant’s alleged connection to an IP address associated with acts of alleged infringement, where the IP address, while registered in the defendant’s name, was the internet service of an adult care home, where numerous residents and visitors had access to it; a defendant’s “status as the registered subscriber of an infringing IP address, standing alone, does not create a reasonable inference that he is also the infringer,” because other individuals could have used the IP address); *Malibu Media, LLC v. Park*, Civil Action No. 17-12107 (JMV) (MF), 2019 WL 2960146 (D.N.J. July 9, 2019) (relying on *Cobbler* and Judge Lamberth’s decision in *Strike 3 Holdings* in denying plaintiff’s motion for a default judgment because the court was not satisfied that the plaintiff established that the defendant was the person who committed copyright infringement based solely on connecting the defendant to an IP address); *Malibu Media, LLC v. Doe*, No. 18-C-450, 2018 WL 6446404 (N.D. Ill. Dec. 10, 2018) (dismissing plaintiff’s amended complaint against a Doe defendant identified under seal following Comcast’s compliance with a third party subpoena, because the plaintiff had not sufficiently tied Doe to the alleged infringing conduct over BitTorrent; reading *Cobbler* as not limited to situations such as an adult care home in which both residents and visitors could access the IP address); see also *Malibu Media, LLC v. Doe*, No. 15-CV-4369 (AKH), 2015 WL 4092417, at *2 (S.D.N.Y. July 6, 2015) (declining to allow pre-service discovery, noting that the late Judge Harold Baer, Jr. explained that there is a risk not only of public embarrassment for the misidentified defendant, but also that the innocent defendant may be coerced into an unjust settlement with the plaintiff to prevent the dissemination of publicity surrounding unfounded allegations); see also *Malibu Media, LLC v. Does 1–5*, 285 F.R.D. 273, 278 (S.D.N.Y. 2012) (denying defendant’s motion to sever, but acknowledging that “there is a fear that regardless of a defendant’s actual culpability, [the Defendant] may feel compelled to settle the lawsuit confidentially in order to avoid the embarrassment of being named as a defendant in a case

Circuit in one case:

Generally speaking, our federal judicial system and the procedural rules that govern it work well, allowing parties to resolve their disputes with one another fairly and efficiently. But sometimes individuals seek to manipulate judicial procedures to serve their own improper ends. This case calls upon us to evaluate—and put a stop to—one litigant’s attempt to do just that.³¹

As explained by the Ninth Circuit:

Although copyright owners can often trace infringement of copyrighted material to an IP address, it is not always easy to pinpoint the particular individual or device engaged in the infringement. Internet providers, such as Comcast or AT & T, can go so far as to identify the individual who is registered to a particular IP address (i.e., an account holder) and the physical address associated with the account, but that connection does not mean that the internet subscriber is also the infringer. The reasons are obvious—simply establishing an account does not mean the subscriber is even accessing the internet, and multiple devices can access the internet under the same IP address. Identifying an infringer becomes even more difficult in instances like this one [involving an IP address registered to an adult care home], where numerous people live in and visit a facility that uses the same internet service. While we recognize this obstacle to naming the correct defendant, this complication does not change the plaintiff’s burden to plead factual allegations that create a reasonable inference that the defendant is the infringer.³²

In *Strike 3 Holdings, LLC v. Doe*,³³ U.S. Magistrate Judge James Orenstein reasoned that the person who engaged in

about the alleged illegal trading of a pornographic film.” (internal quotation marks omitted)); *Ingenuity 13 LLC v. Doe*, No. 2:12-cv-8333-ODW (JCx), 2013 WL 1898633 (C.D. Cal. May 6, 2013) (characterizing Prenda Law as a “porno-trolling collective” and imposing sanctions on Prenda Law-affiliated attorneys; “Plaintiffs have outmaneuvered the legal system. They’ve discovered the nexus of antiquated copyright laws, paralyzing social stigma, and unaffordable defense costs. And they exploit this anomaly by accusing individuals of illegally downloading a single pornographic video. Then they offer to settle—for a sum calculated to be just below the cost of a bare-bones defense. For these individuals, resistance is futile; most reluctantly pay rather than have their names associated with illegally downloading porn. So now, copyright laws originally designed to compensate starving artists allow, starving attorneys in this electronic-media era to plunder the citizenry.”).

³¹*AF Holdings, LLC v. Does 1-1058*, 752 F.3d 990, 991 (D.C. Cir. 2014).

³²*Cobbler Nev., LLC v. Gonzales*, 901 F.3d 1142, 1146–47 (9th Cir. 2018).

³³*Strike 3 Holdings, LLC v. Doe*, 331 F.R.D. 14 (E.D.N.Y. 2019).

the allegedly infringing conduct—using BitTorrent to download plaintiff’s copyrighted porn movies and distribute them to others—“might or might not be the same person as the subscriber of internet service associated with the IP address Strike 3 has identified.”³⁴ The court found that good cause for expedited discovery had not been shown because expedited discovery would create “a risk that Strike 3 will be in a position to effectively coerce the identified subscribers into paying thousands of dollars to settle claims that may or may not have merit, so as to avoid either the cost of litigation or the embarrassment of being sued for using unlawful means to view adult material.”³⁵ The court also raised concern that expedited discovery was not being sought to actually litigate cases:

[W]hatever else Strike 3 will do with the information it secures if it prevails on these motions, it is likely that one thing it will *not* do is use the information to litigate the action in court. Strike 3 has filed 276 cases in this district since 2017. Of those, 133 remain pending, many with unresolved motions for expedited discovery. Of the 143 cases that have been resolved, Strike 3 reports that it settled 49 and voluntarily dismissed 94—28 due to the alleged infringers’ hardship, 50 due to Strike 3’s inability to satisfy itself that Doe (the service subscriber named as the defendant) was in fact the alleged infringer, and 16 for other reasons. . . . There can hardly be good cause to allow expedited discovery, particularly on an *ex parte* basis, to secure information that will not actually be used under judicial supervision to resolve the case on the merits.³⁶

The court also found that good cause had not been shown because in a third of the resolved cases (50 out of 143), Strike 3 could not satisfy itself that the named defendant was actually the alleged infringer.³⁷ The court further expressed skepticism that expedited discovery was necessary to deter copyright violations given that the outcomes of its cases were kept confidential.³⁸

In a D.C. action by the same name, *Strike 3 Holdings, LLC v. Doe*,³⁹ Judge Royce C. Lamberth sharply criticized Strike 3 as a “a copyright troll.” He explained, in an opinion

³⁴*Strike 3 Holdings, LLC v. Doe*, 331 F.R.D. 14, 16 (E.D.N.Y. 2019).

³⁵*Strike 3 Holdings, LLC v. Doe*, 331 F.R.D. 14, 18 (E.D.N.Y. 2019).

³⁶*Strike 3 Holdings, LLC v. Doe*, 331 F.R.D. 14, 19 (E.D.N.Y. 2019).

³⁷*Strike 3 Holdings, LLC v. Doe*, 331 F.R.D. 14, 19 (E.D.N.Y. 2019).

³⁸*Strike 3 Holdings, LLC v. Doe*, 331 F.R.D. 14, 19-20 (E.D.N.Y. 2019).

³⁹*Strike 3 Holdings, LLC v. Doe*, 351 F. Supp. 3d 160, 161 (D.D.C.

published in November 2018, that Strike 3's

swarms of lawyers hound people who allegedly watch their content through Bittorrent, an online service enabling anonymous users to share videos despite their copyright protection. Since Bittorrent masks users' identities, Strike 3 can only identify an infringing Internet protocol (IP) address, using geolocation technology to trace that address to a jurisdiction. This method is famously flawed: virtual private networks and onion routing spoof IP addresses (for good and ill); routers and other devices are unsecured; malware cracks passwords and opens backdoors; multiple people (family, roommates, guests, neighbors, etc.) share the same IP address; a geolocation service might randomly assign addresses to some general location if it cannot more specifically identify another. *See, e.g., James Temple, Lawsuit Says Grandma Illegally Downloaded Porn*, S.F. Chron. (July 15, 2011, 4:00 AM), <https://www.sfgate.com/business/article/Lawsuit-says-grandma-illegally-downloaded-porn-2354720.php>. Simply put, inferring the person who pays the cable bill illegally downloaded a specific file is even less trustworthy than inferring they watched a specific TV show. But in many cases, the method is enough to force the Internet service provider (ISP) to unmask the IP address's subscriber. And once the ISP outs the subscriber, permitting them to be served as the defendant, any future Google search of their name will turn-up associations with the websites *Vixen*, *Blacked*, *Tushy*, and *Blacked Raw*. . . . Little wonder so many defendants settle. Indeed, the copyright troll's success rate comes not from the Copyright Act, but from the law of large numbers. According to PACER, over the past thirteen months, Strike 3 has filed 1849 cases just like this one in courts across the country—forty in this district alone—closely following the copyright trolls who together consumed 58% of the federal copyright docket in 2015. These serial litigants drop cases at the first sign of resistance, preying on low-hanging fruit and staying one step ahead of any coordinated defense. They don't seem to care about whether defendant actually did the infringing, or about developing the law. If a Billy Goat Gruff moves to confront a copyright troll in court, the troll cuts and runs back under its bridge. Perhaps the trolls fear a court disrupting their rinse-wash-and-repeat approach: file a deluge of complaints; ask the court to compel disclosure of the account holders; settle as many claims as possible; abandon the rest. *See* Matthew Sag & Jake Haskell, *Defense Against the Dark Arts of Copyright Trolling*, 103 Iowa L. Rev. 571, 575-80 (2018).⁴⁰

Applying both the D.C. Circuit's prior ruling in *AF Hold-*

2018), *rev'd*, 964 F.3d 1203 (D.C. Cir. 2020).

⁴⁰*Strike 3 Holdings, LLC v. Doe*, 351 F. Supp. 3d 160, 161-62 (D.D.C. 2018), *rev'd*, 964 F.3d 1203 (D.C. Cir. 2020).

*ings, LLC v. Does 1-1058*⁴¹ and the Second Circuit’s decision in *Arista Records, LLC v. Doe 3*,⁴² Judge Lamberth declined to permit discovery, even recognizing the low level of privacy protection afforded to those who download copyrighted works, because Strike 3 failed “to give the Court adequate confidence this defendant actually did the infringing. Given this uncertainty, Strike 3 cannot overcome defendant’s weighty privacy expectation. Imagine having your name and reputation publicly—and permanently—connected to websites like Tushy and Blacked Raw. (Google them at your own risk.) How would an improperly accused defendant’s spouse react? His (or her) boss? . . . The risks of a false accusation are real; the consequences are hard to overstate and even harder to undo. And Strike 3’s flawed identification method cannot bear such great weight.”⁴³

Judge Lamberth concluded his opinion by chastising the practice of copyright porn trolls:

Armed with hundreds of cut-and-pasted complaints and boilerplate discovery motions, Strike 3 floods this courthouse (and others around the country) with lawsuits smacking of extortion. It treats this Court not as a citadel of justice, but as an ATM. Its feigned desire for legal process masks what it really seeks: for the Court to oversee a high-tech shakedown. This Court declines.⁴⁴

On appeal, however, the D.C. Circuit reversed the lower court’s order denying Rule 26(d)(1) discovery, and hence also reversed the lower court’s order dismissing plaintiff’s Complaint, which had been premised on the denial of discovery, ruling that the trial court had been unduly influenced by the nature of the content and that Strike 3 had made a sufficient showing both to state a claim and obtain pre-service discovery where it asserted that it had “used a combination of forensic and geolocation technology to tie a single IP address, registered to a user in the District of Columbia, to twenty-two acts of infringement on specified dates over the

⁴¹*AF Holdings, LLC v. Does 1-1058*, 752 F.3d 990 (D.C. Cir. 2014) (vacating and remanding an order directing ISPs to comply with discovery of numerous defendants, where personal jurisdiction could not be established and joinder of the unknown individuals was improper).

⁴²*Arista Records, LLC v. Doe 3*, 604 F.3d 110, 118 (2d Cir. 2010).

⁴³*Strike 3 Holdings, LLC v. Doe*, 351 F. Supp. 3d 160, 165 (D.D.C. 2018), *rev’d*, 964 F.3d 1203 (D.C. Cir. 2020).

⁴⁴*Strike 3 Holdings, LLC v. Doe*, 351 F. Supp. 3d 160, 166 (D.D.C. 2018), *rev’d*, 964 F.3d 1203 (D.C. Cir. 2020).

course of a year.”⁴⁵

Other courts have continued to allow these subpoenas to issue,⁴⁶ typically subject to the types of protections outlined earlier in this subsection, at least when requested, or otherwise conditioned on allowing the subscriber the right to move to quash.⁴⁷ Some courts have even allowed a party to proceed anonymously (in actuality, pseudonymously).⁴⁸

Alternative means to compel the disclosure of the identity of anonymous and pseudonymous infringers are addressed in sections 37.02 and 50.06.

4.12[9][F] Suits Against Copyright Owners Over DMCA Notifications Based on Theories Other Than Section 512(f)

4.12[9][F][i] In General

In addition to remedies available under 17 U.S.C.A. § 512(f)—which are separately analyzed in section 4.12[9][D]—users and service providers have sued copyright owners over false, unwarranted, or allegedly fraudulent DMCA notices under theories such as interference with contract. While there have been instances where DMCA no-

⁴⁵*Strike 3 Holdings, LLC v. Doe*, 964 F.3d 1203, 1221 (D.C. Cir. 2020). The appellate panel further opined that: “Based on these allegations, a court could reasonably infer that someone with prolonged, continuous access to this IP address was responsible for the alleged infringement. Viewing the allegations in the light most favorable to Strike 3, we think it at least plausible that the registered IP address subscriber ‘actually did the infringing.’” *Id.*

⁴⁶*See, e.g., Strike 3 Holdings, LLC v. Doe*, No. 1:18-cv-2211 (PLF/GMH), 2019 WL 1778054 (D.D.C. Apr. 23, 2019) (disagreeing with Judge Lamberth’s Order; allowing pre-service discovery); *Strike 3 Holdings, LLC v. Doe*, No. 1:18-CV-01490 EAW, 2019 WL 1529339, at *3 (W.D.N.Y. Apr. 8, 2019) (declining to follow Judge Lamberth’s order, denying a motion to quash, and finding that a protective order would adequately protect the defendant’s privacy interests).

⁴⁷*See, e.g., Strike 3 Holdings, LLC v. Doe*, Civil Action No. 21-4021-KSM, 2021 WL 4477446, at *3 (E.D. Pa. Sept. 29, 2021); *Strike 3 Holdings, LLC v. Doe Subscriber Assigned IP address 173.63.148.25*, Civil Action No. 19-10252 (KM)(MAH), 2020 WL 5525549, at *5-6 (D.N.J. Sept. 14, 2020) (citing *Doe v. Meglass*, 654 F.3d 404, 408-09 (3d Cir. 2011), *cert. denied*, 565 U.S. 1197 (2012)); *Strike 3 Holdings, LLC v. Doe*, No. 18-cv-16593, 2019 WL 4745360, at *7 (D.N.J. Sept. 30, 2019).

⁴⁸*See, e.g., Strike 3 Holdings, LLC v. Doe*, No. 18-cv-16593, 2019 WL 4745360, at *7 (D.N.J. Sept. 30, 2019) (declining to issue a protective order but permitting the plaintiff to proceed anonymously).

tices have been used improperly—such as by competitors to have a businesses’ website taken down during a peak sales season or to have a rival’s YouTube channel suspended—other claims have been found to lack merit. These suits typically are brought by accused infringers (as addressed in section 4.12[9][F][ii]) or service providers (as addressed in section 4.12[9][F][iii]). As discussed in the following subsections, some state law claims may be preempted based on field preemption (and if so, could be sanctionable under anti-SLAPP statutes¹ if the claim is deemed to raise a matter of public interest).

4.12[9][F][ii] Suits By Users Who Are Accused Infringers

Suits based on various theories of liability have been brought against copyright owners by affected site owners or users for sending notifications alleging infringement. The DMCA expressly exempts service providers from liability for responding to notifications and counter notifications in accordance with the requirements of the statute,¹ and allows copyright owners, service providers, users and others to recover damages, costs and attorneys’ fees in connection with material misrepresentations knowingly made in notifications or counter notifications.² Although an argument may be advanced that section 512(f) was intended to define the exclusive rights of parties in the event of misrepresentations in a notification or counter notification, based on Congress’s intent to create a pervasive regulatory scheme,³ this argument has yet to be decided in any binding appellate decision. To date, courts have allowed several suits to proceed based on the contents of notifications, although some such suits have been dismissed for failure to state a claim⁴ or on summary judgment. In at least one case, a state court in Califor-

[Section 4.12[9][F][i]]

¹Anti-SLAPP statutes are analyzed more extensively in section 37.02[3].

[Section 4.12[9][F][ii]]

¹See 17 U.S.C.A. § 512(g); supra § 4.12[8].

²See 17 U.S.C.A. § 512(f); supra § 4.12[9][D].

³See, e.g., *Gade v. National Solid Wastes Management Ass’n*, 505 U.S. 88, 98 (1992).

⁴See, e.g., *Capitol Records, Inc. v. MP3tunes, LLC*, 611 F. Supp. 2d 342, 347–48 (S.D.N.Y. 2009) (dismissing claims under N.Y. Gen. Bus. Law

nia held that a service provider (YouTube) could not be held liable to a user for libel or defamation for posting a notice, on the page where a musician's video used to appear, that the video was removed for a Terms of Service violation.⁵

In *Rossi v. Motion Picture Association of America, Inc.*,⁶ the Ninth Circuit affirmed the entry of summary judgment for the defendant-copyright owner on state tort law claims for tortious interference with contractual relations, tortious interference with prospective economic advantage, libel and defamation, and intentional infliction of emotional distress. In that case, the court had held that the copyright owner had complied with the procedures of the DMCA based on a "good faith belief" that the plaintiff's website had included infringing copies of its protected motion pictures (based on plaintiff's own representations on the site). The Ninth Circuit did not address the issue of preemption, finding in a case where there was no knowing material misrepresentation in the notification that plaintiffs' state law claims failed based on the elements required to support them—not preemption.

In a case decided just prior to *Rossi* by a district court in the Ninth Circuit, a court ruled, in *Online Policy Group v. Diebold Election Systems, Inc.*,⁷ that section 512(f) represented the only remedy to the recipient of a notification that was found to have included knowing material misrepresentations, and thus plaintiffs' claim for tortious interference with contractual relations was preempted based on field preemption because of the irreconcilable conflict between the DMCA and the state law.⁸ As explained by the court:

Even if a copyright holder does not intend to cause anything

§ 349, Cal. Bus. & Prof. Code § 17200 and common law unfair competition).

⁵See *Bartholomew v. YouTube, LLC*, 17 Cal. App. 5th 1217, 225 Cal. Rptr. 3d 917 (2017) (affirming YouTube's demurrer).

⁶*Rossi v. Motion Picture Ass'n of America Inc.*, 391 F.3d 1000 (9th Cir. 2004), *cert. denied*, 544 U.S. 1018 (2005).

⁷*Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004); see also *Amaretto Ranch Breedables, LLC v. Ozimals, Inc.*, No. C 10-05696 CRB, 2011 WL 2690437 (N.D. Cal. July 8, 2011) (holding DMCA-related claims preempted by section 512(f)).

⁸*Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004), citing *Hillsborough County, Fla. v. Automated Medical Laboratories, Inc.*, 471 U.S. 707, 713 (1985) (holding that preemption occurs "when compliance with both state and federal [laws] is a physical impossibility or when state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."). In *Diebold*, the district court applied a stricter standard under § 512(f) than the one

other than the removal of allegedly infringing material, compliance with the DMCA's procedures nonetheless may result in disruption of a contractual relationship: by sending a letter, the copyright holder can effectuate the disruption of ISP service to clients. If adherence to the DMCA's provisions simultaneously subjects the copyright holder to state tort law liability, there is an irreconcilable conflict between state and federal law. To the extent that plaintiffs argue that there is no conflict because Diebold's use of the DMCA in this case was based on misrepresentation of Diebold's rights, their argument is undercut by the provisions of the statute itself. In section 512(f), Congress provides an express remedy for misuse of the DMCA's safe harbor provisions. It appears that Congress carefully balanced the competing interests of copyright holders, ISPs, and the public, by providing immunity subject to relief for any misuse of the statute.

Other courts have subsequently held that tortious interference or other state claims are barred by the DMCA based on field preemption.⁹ In *Complex Media, Inc. v. X17, Inc.*,¹⁰ for example, the plaintiff, a creator and publisher of video com-

subsequently adopted by the Ninth Circuit. *See supra* § 4.12[9][D].

⁹*See, e.g., Tine Bak LLC v. Selkatz, Inc.*, CV 20-5065 DSF (SK), 2020 WL 9074806, at *4-6 (C.D. Cal. Nov. 30, 2020) (dismissing plaintiff's claim for tortious interference, premised on a false takedown notice, as preempted by the DMCA); *Beyond Blond Productions, LLC v. Heldman*, CV 20-5581 DSF (GSJx), 2020 WL 4772796, at *2-3 (C.D. Cal. Aug. 17, 2020) (dismissing claims for tortious interference, unfair competition, and trade libel, as preempted by the DMCA, to the extent they depended on alleged misrepresentations in DMCA takedown notices); *Furnituredealer.net, Inc. v. Amazon.com, Inc.*, Civil No. 18-232 (JRT/HB), 2019 WL 3738622, at *3-5 (D. Minn. Aug. 8, 2019) (dismissing with prejudice, as preempted by the online service provider provisions of the DMCA, common law claims of tortious interference with existing business relationships and prospective economic advantage, after plaintiff brought actions for the alleged appearance of copyrighted marketing content on defendant's e-commerce website); *Stardock Systems, Inc. v. Reiche*, Case No: C 17-07025 SBA, 2019 WL 8333514, at *4-8 (N.D. Cal. May 14, 2019) (dismissing, as preempted by the DMCA, claims of tortious interference with prospective economic advantage and contractual relations, arising out of allegedly bad-faith takedown notices submitted to videogame platforms and distributors involving the "Star Control" franchise); *Complex Media, Inc. v. X17, Inc.*, Case No. CV 18-07588 SJO (AGRx), 2019 WL 2896117, at *4-6 (C.D. Cal. Mar. 4, 2019) (granting defendant's anti-SLAPP motion and dismissing with prejudice plaintiff's claim for interference with contract (and awarding attorneys' fees to the defendant under the anti-SLAPP statute) in a suit brought by a copyright owner under section 512(f) (and for related state claims) alleging that the defendant repeatedly sent unjustified DMCA takedown notices to YouTube, jeopardizing its entitlement to use that platform); *infra* § 37.02[3] (analyzing the case in connection with anti-SLAPP motions); *Amaretto Ranch Breedables, LLC v.*

mentary (on its website and via third party platforms such as Roku and Apple TV), sued the celebrity Paparazzi photography service X17, alleging that X17 sent repeated DMCA takedown notices to YouTube for Complex Media content without justification, causing YouTube to disable access to its videos and prevent Complex Media from posting new material to its video channel, and risking the termination of Complex Media's YouTube channel (with the resulting loss of 2.4 million subscribers). Complex Media sued for misrepresentation of copyright claims under section 512(f), a declaration of non-infringement, and intentional interference with contractual relations. X17 brought an anti-SLAPP motion under California law¹¹ to dismiss Complex Media's claim

Ozimals, Inc., No. C 10-05696, 2011 WL 2690437, at *4 (N.D. Cal. July 8, 2011) (holding preempted Amaretto's interference with contract claim, as well as "any other state law claim to the extent such claim is based on Ozimals's DMCA Takedown Notifications" in a suit alleging that DMCA takedown notices were wrongfully sent, even though the material addressed in the notices was not actually removed); *Lenz v. Universal Music Corp.*, No. C 07-03783, 2008 WL 962102, at *4 (N.D. Cal. Apr. 8, 2008) (dismissing plaintiff's claim for intentional interference with contractual relations based on field preemption, but allowing leave to amend "because it is possible that Lenz may be able to allege that the take down notice was based on YouTube's Terms of Use policy rather than the DMCA"); see also *Rock River Communications, Inc. v. Universal Music Group, Inc.*, No. CV08-635 CAS (AJWx), 2011 WL 1598916, at *13-16 (C.D. Cal. Apr. 27, 2011) (granting summary judgment for the defendants on plaintiff's section 512(f) claim because the cease and desist letter at issue was not a DMCA notice and accordingly holding that plaintiff's tortious interference claim arising out of the cease and desist letter was not preempted by the DMCA); see generally *infra* chapter 35 (analyzing field preemption).

An intermediate appellate court in Texas remanded a case for consideration of whether plaintiff's tortious interference claim was preempted by section 512(f), but the court cited the general copyright preemption provision, 17 U.S.C.A. § 301, rather than field preemption. See *Mometrix Media, LLC v. LCR Publishing, LLC*, — S.W.3d —, 2018 WL 6072357 (Tex. Ct. App. 2018). Section 301 should not preempt a tortious interference claim based on sending takedown notices authorized by the DMCA (since 301 preemption applies when a claim alleges copying without an extra element; see *infra* § 4.18[1]), but field preemption could potentially apply. See *infra* chapter 35 (field preemption).

¹⁰*Complex Media, Inc. v. X17, Inc.*, Case No. CV 18-07588 SJO (AGRx), 2019 WL 2896117 (C.D. Cal. Mar. 4, 2019).

¹¹Cal. Code Civ. Proc. § 425.16. Section 425.16 authorizes a fee award and dismissal with prejudice of claims that arise from "any act of [a] person in furtherance of the person's right of petition or free speech under the United States Constitution or the California Constitution in connec-

for interference with contractual relations, which the district court granted. The court reasoned that the size of Complex Media's YouTube channel evidenced that the issue of takedowns was a matter of public interest and that the misappropriation claim was preempted by the DMCA, based on field preemption.¹² As a matter of public policy under the anti-SLAPP statute, this is a terrible decision in that it punishes a publisher for taking action to deter allegedly frivolous takedown notices, potentially emboldening those who seek to censor speech—which runs contrary to the objectives of the anti-SLAPP statute.¹³ By the court's logic in *Complex Media*, content creators entitled to bring a claim under section 512(f), and potentially recover their fees under the Copyright Act,¹⁴ could nonetheless be subject to sanctions, including a mandatory attorneys' fee award, if they join in the action a state law claim deemed preempted. This obviously would have a chilling effect on asserting any state law claim subject to California law, even though there is no binding appellate court precedent on field preemption under the DMCA.

It is also questionable that a state law claim arising out of a DMCA takedown notice could be barred by field preemption, but a state remedy arising out of the claim would not be preempted. If a claim for interference with contract impedes the federal DMCA notice and takedown scheme, then subjecting users who submit DMCA notices to anti-SLAPP motions certainly would interfere to the same extent, if not more. While one could argue that various supplementary state law claims complement, rather than impede sec-

tion with a public issue." Cal. Code Civil Procedure § 425.16(b)(1); see generally *infra* § 37.02[3] (analyzing the statute).

¹²See *Complex Media, Inc. v. X17, Inc.*, Case No. CV 18-07588 SJO (AGRx), 2019 WL 2896117, at *4-6 (C.D. Cal. Mar. 4, 2019). But see *Lenz v. Universal Music Corp.*, No. C 07-03783, 2008 WL 962102, at *3-4 (N.D. Cal. Apr. 8, 2008) (denying Universal's anti-SLAPP motion because, although a DMCA notice constitutes speech, it is not speech protected by the statute; rejecting the argument that "because its notice to YouTube was plainly speech, and Lenz's actions following the filing of the instant suit including appearances on television news shows and commenting about the suit in her personal blog show that the suit has the potential to impact a broad segment of society and thus involves a matter of public concern.").

¹³See *infra* § 37.02[3] (analyzing the anti-SLAPP Statute).

¹⁴See *infra* § 4.15 (analyzing entitlement to fees under 17 U.S.C.A. § 505).

tion 512(f), applying anti-SLAPP sanctions for submitting a DMCA notice, pursuant to section 512 (and the sanctions embodied in section 512(f)) plainly alters the obligations and potential liabilities of the parties contemplated by the DMCA.¹⁵

Other courts have allowed claims or counterclaims to proceed based on the allegedly tortious consequences of allegedly improper DMCA notifications.¹⁶ For example, in *Curtis v. Shinsachi Pharmaceutical Inc.*,¹⁷ the court entered a default judgment against plaintiff's competitors under section 512(f) of the DMCA¹⁸ and for cybersquatting, trademark cancellation, trade libel, interference with contract and prospective economic advantage and a declaratory ruling of non-infringement where a seller alleged that between 2011 and 2013 defendants submitted 30 false Notices of Claimed Infringement to eBay, resulting in the removal of at least 140 listings and causing eBay to issue strikes against her selling account, as well as allegedly false notices to Google, PayPal and Serversea.

In certain circumstances, the contents of notifications or counter notifications may be protected against tort or other claims based on state law litigation privileges.¹⁹

Liability for misrepresentations in DMCA notifications or counter notifications is separately addressed in section

¹⁵See *infra* chapter 35 (analyzing the case and others in the context of field preemption).

¹⁶See, e.g., *Flava Works, Inc. v. Gunter*, No. 10 C 6517, 2013 WL 4734002 (N.D. Ill. Sept. 3, 2013) (denying plaintiff's motion to dismiss the defendant's counterclaim for tortious interference with contract and misrepresentation of intellectual property infringement (pursuant to 17 U.S.C.A. § 512(f)) based on alleged misrepresentations about the extent of allegedly infringing material available on the myVidster.com website made to defendant's service providers and in DMCA notifications).

¹⁷*Curtis v. Shinsachi Pharmaceutical Inc.*, 45 F. Supp. 3d 1190 (C.D. Cal. 2014).

¹⁸See *supra* § 4.12[9][D].

¹⁹See, e.g., Cal. Civil Code § 47(b) (statements made in judicial proceedings); *Maponics, LLC v. Wahl*, No. C07-5777 BZ, 2008 WL 2788282 (N.D. Cal. July 18, 2008) (discussing the potential applicability of California Civil Code section 47(b) to DMCA notices as "reasonably relevant" to "achieve the objects of the litigation," but concluding that the emails at issue in that case did not meet the requirements of section 512(c)(3)(A) and "seem more like an attempt . . . to gain business from a customer by charging a competitor with theft, than an attempt to mitigate a customer's damages.").

4.12[9][D].

Suits by users against service providers typically are limited by contract (such as a service provider's Terms of Service agreement) or by the DMCA itself (for a service provider that complies with the DMCA and its notification and counter notifications provisions).²⁰

As discussed in section 4.12[9][D], claims under section 512(f) for damages and, if applicable, attorneys' fees, may be brought—subject to a \$30,000 cap for damages and \$5,000 cap for attorneys' fees and costs—before the Copyright Claims Board, pursuant to the Copyright Alternative in Small-Claims Enforcement (CASE) Act of 2020,²¹ which is separately analyzed in section 4.08[8], in lieu of seeking relief in federal court. Claims addressed in this section 4.12[F], to the extent not preempted, could only be asserted in a court of law, not in a Copyright Claims Board proceeding.

4.12[9][F][iii] Suits by Service Providers

In contrast to suits by alleged infringers against copyright owners (which are addressed in section 4.12[9][F][ii]), *Fat-wallet, Inc. v. Best Buy Enterprise Services, Inc.*,¹ was a suit by an ISP against copyright owners seeking a declaratory judgment that the service provider liability limitations of the DMCA were unconstitutional. In that case, Judge Philip Reinhard of the Northern District of Illinois ruled that the plaintiff lacked standing to challenge the user storage provision of the DMCA because it cannot claim that it suffered any injury. As explained by the court:

Nothing in the DMCA . . . creates liability for the ISP beyond that which already exists under copyright law generally. An ISP suffers no adverse consequences under the DMCA for its failure to abide by the notice. It is free to thumb its nose at the notice and it will suffer no penalty nor increased risk of copyright liability. Thus, plaintiff was in no worse a position regarding potential copyright liability for the postings of its subscribers whether it responded to the notice or not or for that matter even if the DMCA did not exist at all. In other words, the DMCA only inures to the benefit of plaintiff and visits no negative consequences upon it. Because of the unique

²⁰See generally *supra* § 4.12[9][C]; *infra* § 22.05[2][F].

²¹See 17 U.S.C.A. §§ 1501 to 1511.

[Section 4.12[9][F][iii]]

¹Copy L. Rep. (CCH) ¶ 28,799, 2004 WL 793548 (N.D. Ill. Apr. 12, 2004).

nature of the DMCA notice provisions and how they apply to an ISP, plaintiff cannot claim it suffered any injury or harm from the invocation of the notice provisions by defendant. It was free to ignore the notice and no harm would befall it that did not already exist irrespective of the DMCA. That being said, if in fact an ISP chooses to respond to the notice by taking down the challenged material, it then triggers the safe harbor provision and is insulated from potential liability for copyright infringement. Put another way, the only implication of the notice provisions of the DMCA is a positive one. Plaintiff has failed to identify any harm it has suffered as a result of its choosing to respond to the takedown notice and has therefore not shown it has standing under Article III of the Declaratory Judgment Act.

The court also ruled that the plaintiff lacked standing to assert claims on behalf of third-party posters because of the lack of an actual injury by plaintiff.

In *Arista Records, Inc. v. MP3Board, Inc.*,² the defendant, MP3Board, asserted claims against the RIAA for (1) knowing material misrepresentations in violation of the DMCA (17 U.S.C.A. § 512(f)); and (2) tortious interference with contractual relations. The court granted summary judgment in favor of the RIAA on the DMCA claim, ruling that liability could not be imposed for sending a notification that merely was insufficient to comply with statutory requirements, in the absence of any evidence that a copyright owner or its agent “knowingly materially misrepresent[ed] . . . that material or activity [wa]s infringing.”³ The court also rejected the argument that the RIAA’s notification was actionable because of the alleged vagueness of its allegations.

The court further rejected the contention that the RIAA’s notification constituted a “knowing material misrepresentation” because it threatened the service provider with liability for money damages. Judge Stein ruled that section 512 only penalizes copyright holders for materially misrepresenting “that material or activity is infringing.”⁴

The court also entered summary judgment in favor of the

²*Arista Records, Inc. v. Mp3Board, Inc.*, No. 00 CIV. 4660(SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002).

³*Arista Records, Inc. v. Mp3Board, Inc.*, No. 00 CIV. 4660(SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002), quoting 17 U.S.C.A. § 512(f).

⁴*Arista Records, Inc. v. Mp3Board, Inc.*, No. 00 CIV. 4660(SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002). Although not discussed in the context of this claim, the court noted elsewhere in its opinion that there was no evidence presented that MP3Board’s service provider was in fact

RIAA on MP3Board's claim of tortious interference with contractual relations and prospective economic advantage. The court found that MP3Board failed to present evidence to contradict that the RIAA acted in good faith in notifying MP3Board's service provider about the acts of alleged infringement, which constituted a full defense under applicable state law.

Although Judge Stein did not reach the issue in the *MP3Board* case, a claim for tortious interference based on a notification ultimately arguably could fail as a privileged communication under the *Noerr-Pennington* doctrine.⁵

Since a service provider may obtain dismissal of a third-party suit if the copyright owner fails to tender a substantially complying notification,⁶ sending a notification effectively amounts to a statutorily-required precondition to initiating litigation against the provider (in cases where the service provider fails to take action) and is therefore arguably privileged.⁷

In addition to potential *Noerr-Pennington* immunity, California has a statutory litigation privilege, Civil Code § 47(b), which has been judicially construed to extend to pre-litigation statements made in connection with proposed litigation that is "contemplated in good faith and under serious

immune from liability or that the RIAA knew this fact. Indeed, the threat of money damages should not have amounted to a misrepresentation since service providers are not exempt from liability under the statute. Rather, as discussed earlier in this section, 17 U.S.C.A. § 512 establishes liability limitation defenses that may, but do not automatically apply.

⁵See, e.g., *Matsushita Electronics Corp. v. Loral Corp.*, 974 F. Supp. 345, 354–59 (S.D.N.Y. 1997) (ruling that threatening litigation in bad faith, or filing a suit with no belief in its merit, may be actionable if the other elements of a claim for tortious interference are satisfied under New York law, but holding that even so a litigant is immune from liability for initiating legal action under the *Noerr-Pennington* doctrine, unless the sham litigation exception were found to apply; extending immunity to infringement warning letters sent to defendant's customers); *Keystone Retaining Wall Systems, Inc. v. Rockwood Retaining Walls, Inc.*, No. CIV. 00–496RHK/SRN, 2001 WL 951582 (D. Minn. Apr. 22, 2001) (extending *Noerr-Pennington* immunity to notices of patent infringement that 35 U.S.C.A. § 287 requires be sent as a precondition to filing suit, provided the sham litigation exception is inapplicable).

⁶See *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001); see generally *supra* § 4.12[6][A].

⁷See *Keystone Retaining Wall Systems, Inc. v. Rockwood Retaining Walls, Inc.*, No. CIV. 00–496RHK/SRN, 2001 WL 951582 (D. Minn. Apr. 22, 2001).

consideration.”⁸ In certain circumstances, the contents of notifications or counter notifications may be protected based on state law litigation privileges.⁹

4.12[10] Liability Limitation for Nonprofit Education Institutions

The DMCA creates an additional liability limitation for service providers that are also nonprofit Education Institutions (NEIs) out of recognition that—according to the House Report—“the university environment is unique.” In addition to the four specific limitations created for all service providers, NEIs may benefit from special rules that may limit the liability of universities and other educational institutions for the infringing acts of faculty members or graduate students that otherwise might be imputed to an NEI, as employer, and prevent it from benefiting from the transitory digital network communications, system caching or user storage limitations. As explained in the House Report:

Ordinarily, a service provider may fail to qualify for the liability limitations in Title II simply because the knowledge or actions of one of its employees may be imputed to it under basic principles of respondeat superior and agency law. The special relationship which exists between universities and their faculty members (and their graduate student employees) when they are engaged in teaching or research is different from the ordinary employer-employee relationship. Since independence—freedom of thought, word and action—is at the core of academic freedom, the actions of university faculty and graduate student teachers and researchers warrant special consideration . . . embodied in new . . . special rules.

Under this special limitation, the acts or knowledge of a faculty member or graduate student will not be imputed to the “public or other nonprofit institution of higher education” that employs her if four specific criteria can be met. First, the “faculty member or graduate student” must be “an employee of such institution . . . performing a teaching or

⁸*Aronson v. Kinsella*, 58 Cal. App. 4th 254, 262, 68 Cal. Rptr. 2d 305, 310 (4th Dist. 1997) (quoting earlier cases), *review denied* (Dec. 23, 1997).

⁹*See, e.g., Maponics, LLC v. Wahl*, No. C07-5777 BZ, 2008 WL 2788282 (N.D. Cal. July 18, 2008) (discussing the potential applicability of California Civil Code section 47(b) to DMCA notices as “reasonably relevant” to “achieve the objects of the litigation,” but concluding that the emails at issue in that case did not meet the requirements of section 512(c)(3)(A) and “seem more like an attempt . . . to gain business from a customer by charging a competitor with theft, than an attempt to mitigate a customer’s damages.”).

research function.” Second, the faculty member’s or graduate student’s infringement must not involve the provision of online access to instructional materials that are or were required or recommended by that faculty member or graduate student within the proceeding three-year period for a course taught at the NEI. Third, the NEI must not have received more than two DMCA notifications (as defined in section 4.12[9][B]), which claim copyright infringement by such faculty member or graduate student, within the three-year period (provided such notifications do not contain material misrepresentations, as defined in section 512(f)).¹ Fourth, the NEI must provide all users of its system or network with informational materials that accurately describe and promote compliance with U.S. copyright laws.²

The legislative history emphasizes that the special limitation for NEIs does not apply “[w]hen the faculty member or the graduate student employee is performing a function other than teaching or research.” For example, “exercising institutional administrative responsibilities, or . . . carrying out operational responsibilities that relate to the institution’s function as a service provider” would not constitute exempt activities under the statute. Moreover, the House Report states that “the research must be a genuine academic exercise—i.e. a legitimate scholarly or scientific investigation or inquiry—rather than an activity which is claimed to be research but is undertaken as a pretext for engaging in infringing activity.”

The special provisions governing the acts of faculty members and graduate students do not otherwise affect an NEI’s obligations to meet the technical requirements of the four liability limitations and one broad exemption created by the Act if it seeks to benefit from the DMCA’s safe harbors. NEIs must still designate agents to respond to notifications and counter notifications and comply with the terms of the statute in order to fully limit their liability.

4.12[11] Injunctive Relief

The Act authorizes limited injunctive relief to deny access

[Section 4.12[10]]

¹17 U.S.C.A. § 512(e)(1)(B). The effect of misrepresentations in a notification are discussed earlier in this chapter in section 4.12[9][D].

²17 U.S.C.A. § 512(e)(1).

to infringers and block infringing content, both in the United States and overseas. A court may grant only three specific forms of equitable relief against a service provider (other than a service provider that is also an NEI) that is otherwise immune from liability under the system caching,¹ user storage² or information location tools³ limitations:

- (1) a court order restraining the service provider “from providing access to infringing material or activity residing at a particular site on the provider’s system or network”;
- (2) a court order requiring that a particular infringer’s account or subscription be terminated by the service provider in order to deny it access to the system or network; or
- (3) such other injunctive relief as the court may consider necessary to prevent or restrain infringement of specific material at a particular online location “if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.”⁴

By contrast, a court may only enjoin a service provider (that is not also an NEI) whose liability is otherwise limited under the transitory digital network communications limitation from providing access to a subscriber or account holder who is using the service provider’s services to engage in infringing activity by terminating its account or restraining it from providing access (through reasonable steps to be specified in the court order) to infringing material at a particular online location outside the United States.⁵ This provision is significant for copyright owners, in that it specifically authorizes a court to compel a service provider subject to jurisdiction in the United States to block access to content which would be infringing under U.S. law, even though it may be located overseas in a country where it may not be deemed infringing under that country’s laws or on a server owned by an entity that is not subject to U.S. jurisdiction.

[Section 4.12[11]]

¹See *supra* § 4.12[5].

²See *supra* § 4.12[6].

³See *supra* § 4.12[7].

⁴17 U.S.C.A. § 512(j)(1)(A).

⁵17 U.S.C.A. § 512(j)(1)(B).

As a practical matter, however, it may be difficult for a copyright owner to fully benefit from this provision because it is so easy for infringers to move content from one location to another in cyberspace.

In determining whether to grant injunctive relief against a service provider otherwise immune from liability, courts are directed to weigh several factors, including: (1) whether the order would significantly burden either the service provider or the operation of its system or network; (2) the magnitude of harm likely to be suffered by the copyright owner if steps are not taken to prevent or restrain the online infringement; (3) whether implementation of a proposed injunction would be technically feasible and effective and would not interfere with access to noninfringing material at other online locations; and (4) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available. These criteria generally are consistent with the standards for granting injunctive relief applied in the various federal circuits in copyright infringement lawsuits.⁶

The Act provides that injunctive relief generally may only be granted where a service provider is given notice and the opportunity to appear. Advance notice is not required, however, for orders “ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider’s communications network.”

The ability of third parties to obtain *ex parte* relief to preserve evidence is beneficial for copyright owners given how quickly information may be moved online and how difficult it has proven on occasion to convince a judge of the technological reasons why a TRO must be granted in an Internet-related infringement case. On the other hand, the provision for *ex parte* relief may encourage counsel for copyright owners to move swiftly to seek a TRO even in cases where time would allow for notice and a hearing (recognizing that the injunction sought would be against the service provider, rather than the direct infringer, who may not yet have notice of the suit at the time an injunction against the service provider is sought).

The considerations for granting injunctive relief and requirement for notice apply equally to service providers

⁶See *infra* § 4.13[1].

that are also NEIs, although the limitations on the specific forms of injunctive relief which may be granted (as set forth in section 512(j) and discussed in this section) do not apply to NEIs.⁷ Thus, broader injunctive relief may be obtained against NEIs, which is not unreasonable since they potentially are entitled to broader protections from liability for monetary damages than other service providers.

The standards for obtaining injunctive relief generally are addressed in section 4.13[1]. At least in the Ninth Circuit, an injunction compelling a service provider to remove user content is deemed to be a mandatory injunction, which is disfavored.⁸ It may also be viewed as an impermissible prior restraint.⁹

4.12[12] Extra-Judicial Remedies Available to Copyright Owners

The Digital Millennium Copyright Act provides potentially valuable extra-judicial remedies to copyright owners who are careful to strictly comply with the technical requirements and time limits imposed by the Act. Whereas before the DMCA became law a copyright owner might have had to spend tens of thousands of dollars or more to obtain an injunction compelling a service provider to disable access to or block allegedly infringing content, the same relief may be obtained at virtually no cost from a service provider that has chosen to comply with the statute by designating an agent to receive notifications.

Copyright owners potentially may obtain extra-judicial relief from service providers where alleged acts of infringement involve material stored at the direction of a user, information location tools or certain cached content that either was (or has been ordered to be) removed from its original

⁷See 17 U.S.C.A. § 512(e)(2).

⁸*Garcia v. Google, Inc.*, 786 F.3d 733, 740 & n.4 (9th Cir. 2015) (*en banc*); *infra* § 4.13[1].

⁹See *Garcia v. Google, Inc.*, 786 F.3d 733, 746-47 (9th Cir. 2015) (*en banc*) (dissolving a previously entered preliminary injunction compelling YouTube to take down copies of the film “Innocence of Muslims” and take all reasonable steps to prevent further uploads, which the *en banc* panel held had operated as a prior restraint), *citing Alexander v. United States*, 509 U.S. 544, 550 (1993) (“Temporary restraining orders and permanent injunctions—i.e., court orders that actually forbid speech activities—are classic examples of prior restraints.”); *infra* § 4.13[1].

location.¹ In all other cases, or where a service provider has chosen not to comply with the Act, copyright owners must resort to more traditional means of enforcing their copyrights in cyberspace. Copyright owners also would need to bring suit to obtain damages or injunctive relief directly from the primary infringer or to compel the disclosure (by subpoena) of the identity of a pseudonymous infringer.²

Extra-judicial remedies are available to copyright owners only from service providers that have sought to limit their liability under the DMCA. Service providers need not comply with the Act and their failure to do so may not be cited as evidence that their conduct constitutes infringement.³ Moreover, service providers may elect to comply with some, but not all of the statute's requirements, even though that may mean exposing themselves potentially to liability that otherwise could be limited or avoided under the DMCA.

Whether a service provider will afford a copyright owner extra-judicial relief pursuant to the DMCA usually can be determined from information on the service provider's website. Participating service providers will have filed the appropriate forms with the U.S. Copyright Office to designate an agent. The identity of a service provider's agent—to whom notifications must be directed—may be obtained from the U.S. Copyright Office (both in person and online) and should be posted on the service provider's website.

Simply by sending a notification that provides substantially all of the information required by the statute⁴ to the designated agent of a participating service provider, a copyright owner may obtain immediate relief. Upon receipt by its agent of a substantially complying notification, a service provider must expeditiously remove or disable access to any allegedly infringing content or links identified in the notification. Where a notification is based on information location tools or cached content, no further action will be taken by the service provider.

[Section 4.12[12]]

¹See *supra* § 4.12[9].

²See *generally infra* §§ 37.02 (standards for compelling the disclosure of the identity of anonymous and pseudonymous internet users), 50.06[4] (subpoenas directed to service providers).

³See 17 U.S.C.A. § 512(l).

⁴See *supra* § 4.12[9][B].

When a notification concerns content stored at the direction of a user, a service provider that seeks to limit its liability to subscribers for removing or disabling access to infringing material must promptly notify its subscriber when the content is removed (or access to it disabled), in order to afford the subscriber the opportunity to serve a counter notification.⁵ If the affected subscriber ignores the notification, the material will remain off the Internet (or access to it will continue to be blocked) and the copyright owner will have obtained the rough equivalent of injunctive relief for next to no cost.⁶ The same result would obtain if the service provider has chosen not to comply with the provisions governing counter notifications (if, for example, it concludes that it is unlikely to be exposed to significant liability in suits brought by subscribers).

Even where a subscriber serves a counter notification or files suit in response to a notification, a copyright owner may be in a much better position after having availed itself of the extra-judicial remedies under the DMCA than if, instead, it had simply filed suit against the alleged infringer. If the subscriber serves a counter notification, the copyright owner must file suit and provide notice of the suit to the service provider's agent in order to maintain the status quo. Otherwise, between ten and fourteen business days after receiving the counter notification, the service provider must replace or restore access to the disputed content. If the copyright owner files suit (or if the subscriber initiates litigation in lieu of serving a counter notification), the burden will be on the subscriber to obtain a court order compelling restoration of the removed material. Unless and until the subscriber obtains such an order, the material will remain inaccessible. By contrast, in an ordinary copyright infringement suit, the copyright owner has the burden of obtaining an order to

⁵See *supra* § 4.12[9][C].

⁶The subscriber responsible for the infringing content would not actually be enjoined and therefore could post the material elsewhere in cyberspace. Where an infringer appears likely to persist in its practices, injunctive relief should be obtained prohibiting the person responsible for the act of infringement from further activities. The extra-judicial remedies provided by the DMCA, however, are especially valuable because it is not always easy to identify a primary infringer. In addition, in many cases, infringing content is posted by people who will take no further action once advised that their use of a work is infringing. In those cases, a copyright owner may be able to obtain complete relief merely by preparing and transmitting a substantially complying notification.

have infringing material affirmatively removed (or access to it disabled).

A copyright owner also may obtain procedural advantages in the event of litigation by filing a notification. If a subscriber files a counter notification, the subscriber must consent to the jurisdiction of the federal district court for the address it provides (or if the subscriber is located outside of the United States, “for any judicial district in which the service provider may be found.”) and agree to accept service.⁷ While this provision may allow a subscriber to engage in limited forum shopping (by choosing which address to list for itself), it also allows a copyright owner to avoid costly procedural skirmishes by suing the subscriber in the jurisdiction where it has already consented to be sued. Where a subscriber is not located in the United States, the consent to jurisdiction may be especially valuable. Moreover, the statute does not compel a copyright owner to sue the subscriber in the location where the subscriber has consented to jurisdiction (or even to sue the subscriber at all). The statute merely provides the service provider with a potential procedural advantage. In point of fact, the requirement that a subscriber consent to jurisdiction and service of process in a counter notification itself may discourage many subscribers from even filing counter notifications.

The risk that an accused infringer will file a preemptive lawsuit in response to a notification is somewhat reduced by the fact that the statute also provides an incentive for subscribers to use the counter notification procedure to obtain inexpensive relief (at least in instances where a service provider has chosen to comply with the procedures for counter notifications). By filing a counter notification, a subscriber may compel a service provider to restore access to or replace content removed in response to a notification, if the original complainant fails to provide notice to the service provider within ten (10) business days that it has initiated litigation, in which case within fourteen (14) business days access to the content must be restored. While serving a counter notification therefore would likely trigger litigation in many instances, in some cases it could allow a subscriber to obtain relief if the copyright owner ultimately chose not to bring suit or missed the tight time deadlines established by

⁷17 U.S.C.A. § 512(g)(3)(D).

the Act.⁸

If a copyright owner misses the deadline for responding to a counter notification, the statute does not place any express prohibition on it simply serving a new notification. A copyright owner that did so repeatedly at some point presumably could expose itself to liability for engaging in unfair trade practices or other state law claims. Moreover, if a service provider refused to respond to a second notification (served after the copyright owner failed to timely respond to an initial counter notification), the copyright owner would likely have no recourse but to file suit. The copyright owner would then have to convince a judge to grant it injunctive relief, after locating and serving the primary infringer. In such circumstances, the copyright owner could well have difficulty seeking to hold a service provider liable when the service provider discharged its duties under the Act in response to the original notification.

Although the extra-judicial remedies available under the DMCA may not provide complete relief in all cases, they afford potentially significant, relatively inexpensive benefits. Copyright owners therefore should be careful not to squander the benefits afforded by the Act. Copyright owners must pay especially close attention to the deadlines for responding to counter notifications. Although subscribers potentially have flexibility in deciding when to file a counter notification, a copyright owner merely has ten business days from the time *the service provider* receives the counter notification—not the time the copyright owner receives it—to notify the service provider that it has initiated litigation.⁹

4.12[13] Compliance Burdens Imposed on ISPs

While the Act provides potentially valuable liability limitations for service providers, ISPs that seek to benefit from all of the provisions face potentially complicated, time consuming and expensive compliance obligations. For this reason, some ISPs initially determined that the costs of compliance exceeded the benefits. Today, it is more common for eligible entities to seek to comply with the DMCA. Even so, service providers potentially may comply with provisions governing notifications but avoid the additional burden of

⁸Unscrupulous subscribers may simply move the content to a different location on the Web, rather than even pursue a counter notification.

⁹*See supra* § 4.12[9][C].

honoring counter notifications.

The agent designation provisions applicable to the caching, user storage and information location tools limitations require service providers to incur limited administrative fees. Entities that choose to designate an agent, however, may face an increased volume of complaints, especially because the Act makes it easier and less costly for copyright owners to compel service providers to take action against alleged infringers. Indeed, within days of the statute being signed into law, the volume of demand letters received by some service providers increased significantly (even before the affected companies designated agents to receive notifications). For some companies, the cost of receiving and responding to notifications may be significant.

Service providers that have *subscribers* potentially face the most onerous burdens under the Act if they seek to benefit from the broad exemption created by subpart 512(g)(2) for removing content in response to a notification.¹ To benefit from both the user storage limitation² and the exemption for removing content, an agent must accept and separately calendar its obligations in response to notifications and counter notifications to ensure that the appropriate content is located and expeditiously removed (or access to it disabled) and then—within ten to fourteen business days after a counter notification is received (if no response to the counter notification has been received within ten business days)—restore access to or replace the content. Service providers also must be sure to take reasonable steps to promptly notify subscribers when content has been removed (or access to it disabled) and promptly notify copyright owners when counter notifications are received. While these procedures make sense in the abstract, in practice they impose significant time and cost burdens on ISPs and compel them to use calendaring software or rely on counsel to ensure that statutory time frames are met. For this reason, service providers that calculate the risk of liability to a subscriber for removing content as being fairly low may choose to ignore entirely the procedures for benefiting from the exemption created by subpart 512(g)(2).

[Section 4.12[13]]

¹See *supra* § 4.12[8].

²See *supra* § 4.12[6].

Service providers that comply with the user storage limitation, but not the exemption created by subpart 512(g)(2) (and corresponding procedures governing counter notifications), may still find that they face an increased volume of complaints. ISPs that resell service to other ISPs, for example, may find themselves technically required to disable access to an entire system in order to literally comply with the Act's mandate to disable access to or remove infringing content (because it may not be technologically possible to do anything other than cut off service to the ISPs own "subscriber").³

The information location tools limitation imposes less burdensome compliance demands on service providers. Search engine firms, portals, destinations and other entities sent notifications relating to links or other information location tools simply must disable the links (or information location tools) in order to comply with the requirements of the Act. The system caching limitation imposes even fewer burdens (except to the extent an agent must evaluate whether certain cached content has been removed, or ordered to be removed, from the site where it originally was stored).⁴

Service providers complying with the user storage, information location tools and caching limitations must be prepared periodically to respond to the special subpoenas created by the Act. This procedure, however, actually may be less burdensome than under pre-existing law where the scope of a service provider's obligations potentially had to be re-litigated every time a service provider was sued. As a practical matter, DMCA subpoenas most commonly will be sought in response to material stored at the direction of a user.

In general, the system caching limitation (except in cases involving cached content no longer found on the genuine site or subject to a court order) and transitory digital network communication limitations impose the fewest burdens on service providers. Aside from meeting the threshold requirements set forth in section 4.12[3], most service providers need not do anything further in order to benefit from these limitations.

Where a service provider fails to satisfy the requirements

³See *infra* § 4.12[14].

⁴See *supra* §§ 4.12[5], 4.12[9][A].

of any of the provisions established by the Act, its liability will be determined by existing law.⁵ The service provider's failure to meet the requirements for any one of the DMCA's safe harbors may not be cited as evidence of infringement or liability.⁶

4.12[14] Liability of NSPs and Downstream Service Providers Under the Digital Millennium Copyright Act

The Digital Millennium Copyright Act does not account for differences between individual or corporate subscribers and therefore does not adequately account for Network Service Providers (NSPs) whose own *subscribers* actually are ISPs, rather than individual account holders.¹ While the Act's provisions may not be unduly onerous for service providers that do not have *subscribers* (such as some portals or search engine firms that do not also offer free email or other services) or ISPs that merely have individual subscribers, the statute is less well suited to large service providers that resell access to other commercial service providers.

An NSP or other reseller of service is unlikely to have the technical capability to disable access to or remove the specific content placed online by an individual subscriber of a commercial purchaser of its service (or a "downstream service provider"). Yet, if a notification is directed to an NSP concerning infringing content posted on the personal homepage of a subscriber of a downstream service provider, the NSP, as a service provider, would be compelled by the Act to disable access to the downstream service provider—affecting

⁵See *supra* § 4.11. For a discussion of how to limit site owner and service provider liability, whether or not the site or service complies with the DMCA, see *infra* chapter 50.

⁶See 17 U.S.C.A. § 512(l).

[Section 4.12[14]]

¹The legislative history reveals that Congress intended to maximize the protections afforded service providers. The House Report provides that:

The liability limitations apply to networks "operated by or for the service provider," thereby protecting both service providers who offer a service and subcontractors who may operate parts of, or an entire, system or network for another service provider.

H. Rep. No. 105-796, 105th Cong. 2d Sess. 1, 73 (1998). Congress apparently did not appreciate the problems a broad definition could create when liability is sought to be imposed on a reseller for the conduct of a downstream provider.

potentially hundreds or thousands of customers of the downstream provider—in order to limit its liability. In such circumstances, the NSP may find it more economical to risk liability for infringement than to cut off service to a commercial subscriber.

Although the statute does not distinguish among service providers—and therefore could impose overlapping obligations where a service provider has downstream commercial customers that are both *subscribers* and *service providers* under the Act—NSPs may negotiate agreements (or impose conditions on) downstream service providers to minimize their potential liability. For example, downstream providers could be compelled to indemnify an NSP for acts of infringement by their users and suits brought by subscribers directly against the NSP for material removed (or access to it disabled) in response to a notification initially directed to the NSP. This type of indemnification provision should insulate an NSP from both liability for infringement and for removing (or disabling access to) content.

Downstream providers also could be contractually bound to comply with the provisions of the DMCA and *immediately* (or at least expeditiously) respond whenever a notification relating to the conduct of their users or account holders is forwarded to them by the NSP. An NSP thus could simply transmit notifications directly to the appropriate downstream service provider without having to either disable access to the downstream provider's service (which would be unreasonable) or expose itself to liability by ignoring the notification. So long as access to infringing material ultimately was disabled (or the content removed) expeditiously, the NSP could not be held liable under the DMCA.

If a downstream service provider is further contractually obliged to comply with the DMCA, an NSP may effectively shift most of the burden of complying with notifications directed to remote subscribers on the downstream provider which is the primary service provider to the subscriber. To avoid complications or misunderstandings, NSPs also would be well advised to notify the original complainant that the proper recipient of the notification would be the downstream service provider (whose agent and contact information should be provided). This may encourage the complainant to deal directly with the downstream provider. While an NSP need not worry about the procedures for counter notifications (assuming that it is properly indemnified by its downstream

service provider), it should not put itself in the position of having to direct traffic back and forth between a copyright owner, on the one hand, and its downstream service provider and a remote subscriber, on the other.

Where responsibility could not be imposed by contract or where a downstream provider fails to expeditiously remove or disable access to infringing content, the NSP would be unable to limit its own liability unless it disabled access to the content itself. Unless the NSP also hosts the downstream service provider's servers, it may not have the technological capability to do so. Disabling access to an entire downstream service would not be commercially feasible and would likely result in greater financial harm than simply risking liability for infringement.

Even where an NSP may be unable to benefit from the liability limitations created by the DMCA, it may not necessarily be held responsible for the conduct of remote infringers of downstream service providers. An NSP or commercial reseller of service ultimately may face more limited liability than other service providers.

An NSP's conduct—in merely providing service to a downstream provider that in turn sells access to customers (one of whom may have posted infringing content)—is even more attenuated than that of a typical ISP. It would therefore be correspondingly more difficult for a plaintiff to show “direct action” or “volitional conduct” by the NSP, which is required to justify the imposition of direct liability under *Religious Technology Center Services, v. Netcom On-Line Communication Services, Inc.*² and its progeny.

Similarly, it would be more difficult for a plaintiff to establish that an NSP could be held contributorily liable for failing to respond to a complaint about a remote subscriber when the NSP's only possible means of preventing the infringement would be to shut off all service to the downstream provider (and the copyright owner itself presumably could have contacted the downstream provider directly). An NSP also could well argue that liability should not be imposed because the service it sold had “substantial noninfringing

²*Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361 (N.D. Cal. 1995).

uses.”³

It would also be more difficult for a copyright plaintiff to make out a case for vicarious liability against an NSP based on the NSP reselling service to a downstream service provider whose subscriber is alleged to have posted infringing material. An NSP’s ability to control the conduct of the direct infringer is more attenuated in the case of a remote subscriber of a downstream service provider. Similarly, any financial benefit would be even more remotely connected to the act of infringement than in the case of a typical ISP.⁴ Thus, although the DMCA fails to adequately account for commercial resellers of service in its definition of *service providers*, in practice the risk of liability for NSPs as a result of third-party acts of infringement also may be lower in many cases than for many other categories of providers.

4.12[15] Checklist of Service Provider Compliance Issues

The following is a short-hand checklist of the things a service provider should do in order to comply with all potential liability limitations under the Digital Millennium Copyright Act.¹ This list is intended to supplement, rather than replace, any legal analysis of an individual company’s specific obligations in order to benefit from the Digital Millennium Copyright Act:

- Adopt and implement a policy of terminating the accounts of “repeat infringers.”
- Inform users and subscribers of the policy:

³See *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984); see generally *supra* § 4.10.

⁴See *supra* § 4.11[8][C].

[Section 4.12[15]]

¹This checklist assumes that a service provider intends to fully comply with all provisions of the statute. Service providers that seek to benefit from only some—but not all—of the provisions need not comply with all of the elements of the checklist. This checklist does not address the technical requirements for compliance with the transitory digital network (routing) or system caching limitations that describe the way information is transmitted over the Internet and within networks. These limitations generally apply so long as material is not altered while stored or transmitted and is not maintained for longer than necessary for the purpose of transmission. The caching limitation applies to system caching, rather than proxy caching. See generally *supra* §§ 4.12[4], 4.12[5].

- post the policy on your website or intranet (as part of “Terms of Use”);²
 - reference the policy in any subscriber or user agreements; and
 - notify existing subscribers by email.
- Implement the new policy:
 - notify first-time infringers that they may not post infringing content and may lose their access rights if they infringe again in the future (and remove or disable access to infringing content—see below);
 - document all instances in which the accounts of “repeat infringers” were terminated; and
 - maintain records of communications sent to infringers and “repeat infringers” to verify that the policy was properly implemented (if challenged in litigation).
 - Accommodate “standard technical measures” (not yet applicable).
- Designate an agent to respond to notifications and counter notifications:
 - file the appropriate form with the U.S. Copyright Office; and
 - post the agent’s contact information (name, address, email address, telephone and fax number) on your website and/or intranet.
 - Remove or disable access to material believed in good faith to be infringing.
 - The obligation to disable access to or remove material arises
 - when a service provider has actual knowledge that material is infringing;
 - when a service provider is aware of facts or circumstances from which infringement is apparent (i.e., it raises a “red flag”); or
 - upon receipt of a substantially complying notification

If the infringement is discovered because a notification has been sent to the designated agent, comply with the provisions described below.

- Where an agent receives a notification, assuming that

²See *infra* § 22.05[2][A].

the notification substantially complies with the requirements of the statute,³ the service provider must:

- expeditiously remove the allegedly infringing content or link or disable access to it; and
- if the offending content has been posted by a user who is also a *subscriber*, promptly notify the subscriber that its material has been removed (or access to it disabled). In response to this notice, the agent may be served with a counter notification by the subscriber. Where a counter notification is received, the service provider must:
 - provide a copy to the complainant who filed the original notification and inform it that the offending material will be replaced (or access to it restored) within ten business days from the date of the counter notification unless the complainant notifies the service provider that it has initiated a lawsuit seeking a court order to restrain the subscriber from infringing activity;⁴ and
 - replace (or restore access to) the offending content within fourteen business days of the date of the counter notification if, and only if, the original complainant fails to notify the service provider's agent within ten business days that it has initiated a lawsuit against the subscriber. Where timely notice of litigation is provided, the service provider must not replace or restore access to the infringing content unless ordered to do so by the appropriate federal court.

4.12[16] Copyright Owners' Compliance Checklist

The following checklist should be referenced by copyright owners seeking to benefit from the extra-judicial remedies created by the Digital Millennium Copyright Act. When an

³Where a notification does not meet the requirements of the statute, the service provider, in appropriate circumstances, should promptly notify the complainant of deficiencies and request additional information and/or remove or disable access to the content (if—independently of the information contained in the notification—the content appears to the service provider in good faith to be infringing). *See supra* § 4.12[9][B].

⁴Although no time period is specified in the statute, this should be done as soon as possible given that the ten-day period runs from the date of the service provider's receipt of the counter notification rather than the date the complainant is notified of it.

infringing copy of a protected work is found online, the copyright owner should:

- Identify the service provider's agent from the service provider's website or the database maintained by the U.S. Copyright Office.
- If the service provider on whose system infringing content has been posted has designated an agent, prepare a notification that substantially provides all of the information required by the statute.¹
- Once material has been removed (or access to it disabled), anticipate the arrival of a counter notification.² Where a counter notification is received, a copyright owner must initiate litigation and notify the service provider's agent *within ten business days of the service provider's receipt of the counter notification* (not the date when it was transmitted to or received by the copyright owner) in order to prevent the material from being placed back online (or access to it restored).
- To the extent possible, verify that all copies of infringing content accessible electronically (including older copies that may have been cached) have been removed in response to a notification. Where appropriate, submit additional notifications.

4.12[17] User Generated Content Principles

4.12[17][A] In General

In October 2007, a coalition of motion picture, television,

[Section 4.12[16]]

¹If the service provider has not designated an agent in accordance with the provisions of the Digital Millennium Copyright Act, the service provider may simply disregard the notification. Service providers are not required to comply with the Act and a service provider's refusal to do so may not be cited as evidence that its conduct constitutes infringement (which must be separately proven).

²Copyright owners may find it beneficial (1) to determine if the particular service provider to whom a notification is directed complies with provisions governing counter notifications, and (2) evaluate whether the infringing content was posted by a subscriber. Unless both of these conditions apply, a copyright owner need not worry about the prospect of a counter notification being served. A counter notification may only be served where material removed from the Internet was posted by a user who was also a subscriber and the service provider has opted to benefit from the broad exemption for potential liability to subscribers for removing or disabling access to content in response to a notification.

computer and Web 2.0 companies promulgated the Principles for User Generated Content Services, which are best practices that they advance for UGC sites. The companies promoting the initiative at the time of its launch were Disney, CBS, NBC Universal, Daily Motion, Veoh, Viacom, MySpace, FOX and Microsoft. A copy of the UGC Principles is reproduced below in section 4.12[17][B].

From a legal standpoint, UGC sites are no different than the interactive websites, chat rooms and bulletin boards in existence at the time Congress enacted the DMCA. The user storage safe harbor applies to claims “for infringement . . . by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for a service provider . . . ,”¹ which plainly applies to UGC sites. A UGC site is merely a location where users may post material for others to view (or in some cases copy). A legitimate UGC site is little more than a location, operated by a service provider, where material may be posted at the direction of a user. Indeed, it is the DMCA which has allowed these sites to emerge and flourish. Aside from terminology and sociology, technology is the only thing different about UGC, video file sharing and blogging sites and social networks, on the one hand, and websites of the late 1990s, on the other. Better bandwidth connections, memory, more socially-oriented interfaces and numerous inexpensive devices (including cameras and mobile phones) have made it much easier for users to quickly and easily create, post, store and transmit rich media. The legal framework, however, is mostly the same. While most of the major sites are filled with legitimate UGC, as with any Internet location, some users may post material that is unauthorized. Given the community-based nature of many UGC sites, if unauthorized material is posted, it potentially may be disseminated quite quickly. Indeed, a number of suits were filed against UGC sites starting in late 2006.²

To address these challenges, the UGC Principles were

[Section 4.12[17][A]]

¹17 U.S.C.A. § 512(c).

²See *Tur v. YouTube*, Civil No. 0443 6-FMC (C.D. Cal. complaint filed July 14, 2006); *UMG Recordings, Inc. v. Grouper Networks, Inc.*, Civil No. 06-CV-06561 (C.D. Cal. complaint filed Oct. 16, 2006); *UMG Recordings, Inc. v. MySpace, Inc.*, Civil No. 06-C V-07361 (C.D. Cal. complaint filed Nov. 17, 2006); *Io Group, Inc. v. Veoh Networks, Inc.*, Case No. 06-3926 HRL (N.D. Cal. 2006); *Viacom Int’l, Inc. v. YouTube, Inc.*, No. 07-C V-2103

proposed as “best practices.” These guidelines reflect practices that in fact have been implemented by leading sites and should be viewed as steps that UGC sites should take—beyond what may be required by the DMCA. Copyright owners who signed on to the UGC Principles agree not to sue service providers who comply with the principles for user submitted content.

The first principle calls for UGC sites to post information promoting respect for intellectual property and discourages users from uploading infringing material. This principle reflects the importance in education in leading to responsible user conduct.

The second principle provides that during the upload process, UGC services should prominently inform users that they may not post infringing material and ask them to affirm that their upload complies with the site’s Terms of use. One way to accomplish this is to require users to affirmatively check a box certifying to their compliance with TOU and applicable law, including copyright law, and click their assent in conjunction with the upload process.

The third principle calls for sites to implement effective content identification technology. In fact, many leading sites that host UGC including MySpace and others had already implemented Audible Magic Copysense fingerprinting technology as of the time the UGC Principles were adopted. Among other things, sites and services may employ audio and video filters to physically prevent users from being able to upload files that match the digital “fingerprint” of files registered with the site or third-party technology provider such as Audible Magic.

The fourth principle focuses on cooperation between UGC sites and copyright owners to shut down illegitimate sites (such as locations that create links to unauthorized material that they find on multiple different sites, creating in effect infringement locations).

LLS (S.D.N.Y. complaint filed Mar. 13, 2007); *The Football Ass’n Premier League Ltd. v. YouTube, Inc.*, No. 07-CV-3582 (S.D.N.Y. complaint filed May 4, 1007); *Cal IV Entertainment, LLC v. YouTube, Inc.*, No. 3:07-cv-00617 (M.D. Tenn. 2007); *Veoh Networks, Inc. v. UMG Recordings, Inc.*, 522 F. Supp. 2d 1265 (S.D. Cal. 2007) (dismissing declaratory relief action brought by Veoh shortly before Veoh was sued by UMG in the Central District of California); *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 2:07-cv-05744 (C.D. Cal. 2007); *Divx, Inc. v. UMG Recordings, Inc.*, 3:07cv1753 (S.D. Cal. 2007).

The fifth principle calls on sites to provide commercially reasonable enhanced searching capabilities to allow copyright owners to more quickly remove unauthorized material.

The eighth principle calls upon sites to comply with the DMCA, but also to provide copies of any counter notifications received to the copyright owner who complained in the first instance.

The UGC Principles also address measures to assist copyright owners in vindicating their rights, such as tracking uploads to better identify repeat infringers, and preserving records. The principles also call upon copyright owners to account for fair use in sending takedown notices.

The UGC Principles are intended to supplement the provisions of the DMCA, not supplant them. Companies signing on to the Principles also agree to implement them internationally.

A copy of the UGC Principles is reproduced below. Practical guidance on the DMCA and UGC Principles is set forth in section 50.03.

4.12[17][B] UGC Principles¹

Leading commercial copyright owners (“Copyright Owners”) and services providing user-uploaded and user generated audio and video content (“UGC Services”) have collaborated to establish these Principles to foster an online environment that promotes the promises and benefits of UGC Services and protects the rights of Copyright Owners. In this context, UGC Services are services such as Soapbox on MSN Video, MySpace, Dailymotion and *Veoh.com*, and not other technologies such as browsers, applets, email, or search services. While we may differ in our interpretation of relevant laws, we do not mean to resolve those differences in these Principles, which are not intended to be and should not be construed as a concession or waiver with respect to any legal or policy position or as creating any legally binding rights or obligations. We recognize that no system for deterring infringement is or will be perfect. But, given the development of new content identification and filtering technologies, we are united in the belief that the Principles set out below, taken as a whole, strike a balance that, on a

[Section 4.12[17][B]]

¹Available at <http://www.ugcprinciples.com>

going-forward basis, will result in a more robust, content-rich online experience for all.

In coming together around these Principles, Copyright Owners and UGC Services recognize that they share several important objectives: (1) the elimination of infringing content on UGC Services, (2) the encouragement of uploads of wholly original and authorized user generated audio and video content, (3) the accommodation of fair use of copyrighted content on UGC Services, and (4) the protection of legitimate interests of user privacy. We believe that adhering to these Principles will help UGC Services and Copyright Owners achieve those objectives.

1. UGC Services should include in relevant and conspicuous places on their services information that promotes respect for intellectual property rights and discourages users from uploading infringing content.
2. During the upload process, UGC Services should prominently inform users that they may not upload infringing content and that, by uploading content, they affirm that such uploading complies with the UGC Service's terms of use. The terms of use for UGC Services should prohibit infringing uploads.
3. UGC Services should use effective content identification technology ("Identification Technology") with the goal of eliminating from their services all infringing user-uploaded audio and video content for which Copyright Owners have provided Reference Material (as described below). To that end and to the extent they have not already done so, by the end of 2007, UGC Services should fully implement commercially reasonable Identification Technology that is highly effective, in relation to other technologies commercially available at the time of implementation, in achieving the goal of eliminating infringing content. UGC Services should enhance or update the Identification Technology as commercially reasonable technology that makes a meaningful difference in achieving the goal becomes available.
 - a. If a Copyright Owner has provided: (1) the reference data for content required to establish a match with user-uploaded content, (2) instructions regarding how matches should be treated, and (3) representations made in good faith that it possesses the appropriate rights regarding the content (collec-

tively, “Reference Material”), then the UGC Service should apply the Identification Technology to that content to implement the Filtering Process described below. UGC Services should ensure that reasonable specifications, as well as any tools and/or technical support, for the delivery of Reference Material are made available to Copyright Owners. If a Copyright Owner does not include in the Reference Material instructions regarding how matches should be treated, the UGC Service should block content that matches the reference data.

- b. The Identification Technology should use Reference Material to identify user-uploaded audio and video content that matches the reference data and should permit Copyright Owners to indicate how matches should be treated.
- c. If the Copyright Owner indicates in the applicable Reference Material that it wishes to block user-uploaded content that matches the reference data, the UGC Service should use the Identification Technology to block such matching content before that content would otherwise be made available on its service (“Filtering Process”). The Copyright Owner may indicate in the applicable Reference Material that it wishes to exercise an alternative to blocking (such as allowing the content to be uploaded, licensing use of the content or other options), in which case, the UGC Service may follow those instructions or block the content, in its discretion.
- d. Copyright Owners and UGC Services should cooperate to ensure that the Identification Technology is implemented in a manner that effectively balances legitimate interests in (1) blocking infringing user-uploaded content, (2) allowing wholly original and authorized uploads, and (3) accommodating fair use.
- e. UGC Services should use the Identification Technology to block user-uploaded content that matches Reference Material regardless of whether the UGC Service has any licensing or other business relationship with the Copyright Owners who have provided such Reference Material (except that UGC Services may require that Copyright Owners enter into agreements with respect to the specifications

for delivery of Reference Material that are commercially reasonable and that facilitate the provision of Reference Material by Copyright Owners and promote the goal of the elimination of infringing content). If a Copyright Owner authorizes specific users to upload content that would otherwise match Reference Material submitted by the Copyright Owner, the Copyright Owner should provide to the UGC Service a list of such users (a so-called white list).

- f. UGC Services may, at their option, utilize manual (human) review of all user-uploaded audio and video content in lieu of, or in addition to, use of Identification Technology, if feasible and if such review is as effective as Identification Technology in achieving the goal of eliminating infringing content. If a UGC Service utilizes such manual review, it should do so without regard to whether it has any licensing or other business relationship with the Copyright Owners. Copyright Owners and UGC Services should cooperate to ensure that such manual review is implemented in a manner that effectively balances legitimate interests in (1) blocking infringing user-uploaded content, (2) allowing wholly original and authorized uploads, and (3) accommodating fair use.
- g. Copyright Owners should provide Reference Material only with respect to content for which they believe in good faith that they have the appropriate rights to do so, and should update rights information as reasonable to keep it accurate. The inclusion of reference data for content by, or at the direction of, a Copyright Owner shall be deemed to be an implicit representation made in good faith that such Copyright Owner has the appropriate rights regarding such content. Copyright Owners should reasonably cooperate with UGC Services to avoid unduly stressing the Services' Identification Technology during limited periods when Copyright Owners, collectively, may be providing an overwhelmingly high volume of Reference Material. UGC Services should reasonably cooperate with Copyright Owners to ensure that such Reference Material is utilized by the Identification Technology as soon as possible during such overload periods.

- h. Promptly after implementation of Identification Technology, and at intervals that are reasonably timed throughout each year to achieve the goal of eliminating infringing content, UGC Services should use Identification Technology throughout their services to remove infringing content that was uploaded before Reference Material pertaining to such content was provided.
 - i. Copyright Owners and UGC Services should cooperate in developing reasonable procedures for promptly addressing conflicting claims with respect to Reference Material and user claims that content that was blocked by the Filtering Process was not infringing or was blocked in error.
- 4. UGC Services and Copyright Owners should work together to identify sites that are clearly dedicated to, and predominantly used for, the dissemination of infringing content or the facilitation of such dissemination. Upon determination by a UGC Service that a site is so dedicated and used, the UGC Service should remove or block the links to such sites. If the UGC Service is able to identify specific links that solely direct users to particular non-infringing content on such sites, the UGC Service may allow those links while blocking all other links.
- 5. UGC Services should provide commercially reasonable enhanced searching and identification means to Copyright Owners registered with a service in order:
 - (a) to facilitate the ability of such Copyright Owners to locate infringing content in all areas of the UGC Service where user-uploaded audio or video content is accessible, except those areas where content is made accessible to only a small number of users (not relative to the total number of users of the UGC Service), and
 - (b) to send notices of infringement regarding such content.
- 6. When sending notices and making claims of infringement, Copyright Owners should accommodate fair use.
- 7. Copyright Owners should provide to UGC Services URLs identifying online locations where content that is the subject of notices of infringement is found—but only to the extent the UGC Service exposes such URLs.

8. When UGC Services remove content pursuant to a notice of infringement, the UGC Service should (a) do so expeditiously, (b) take reasonable steps to notify the person who uploaded the content, and (c) promptly after receipt of an effective counter-notification provide a copy of the counter-notification to the person who provided the original notice, and, at its option, replace the content if authorized by applicable law or agreement with the Copyright Owner.
9. When infringing content is removed by UGC Services in response to a notice from a Copyright Owner, the UGC Service should use reasonable efforts to notify the Copyright Owner of the removal, and should permit the Copyright Owner to provide, or request the UGC Service to provide on its behalf, reference data for such content to be used by the Identification Technology.
10. Consistent with applicable laws, including those directed to user privacy, UGC Services should retain for at least sixty (60) days: (a) information related to user uploads of audio and video content to their services, including Internet Protocol addresses and time and date information for uploaded content; and (b) user-uploaded content that has been on their services but has been subsequently removed following a notice of infringement. UGC Services should provide that information and content to Copyright Owners as required by any valid process and consistent with applicable law.
11. UGC Services should use reasonable efforts to track infringing uploads of copyrighted content by the same user and should use such information in the reasonable implementation of a repeat infringer termination policy. UGC Services should use reasonable efforts to prevent a terminated user from uploading audio and/or video content following termination, such as blocking re-use of verified email addresses.
12. In engaging in the activities set forth in these Principles outside the United States, UGC Services and Copyright Owners should follow these Principles to the extent that doing so would not contravene the law of the applicable foreign jurisdiction.
13. Copyright Owners should not assert that adherence to these Principles, including efforts by UGC Services

to locate or remove infringing content as provided by these Principles, or to replace content following receipt of an effective counter notification as provided in the Copyright Act, support disqualification from any limitation on direct or indirect liability relating to material online under the Copyright Act or substantively similar statutes of any applicable jurisdiction outside the United States.

14. If a UGC Service adheres to all of these Principles in good faith, the Copyright Owner should not assert a claim of copyright infringement against such UGC Service with respect to infringing user-uploaded content that might remain on the UGC Service despite such adherence to these Principles.
15. Copyright Owners and UGC Services should continue to cooperate with each other's reasonable efforts to create content-rich, infringement-free services. To that end, Copyright Owners and UGC Services should cooperate in the testing of new content identification technologies and should update these Principles as commercially reasonable, informed by advances in technology, the incorporation of new features, variations in patterns of infringing conduct, changes in users' online activities and other appropriate circumstances.

4.12[18] Discovery Issues and Spoliation of Evidence in DMCA Litigation

There have not been a lot of reported decisions involving discovery issues in DMCA litigation.

Some amount of discovery generally will be permitted in a DMCA case on the elements of the defense as outlined in the statute, such as a service provider's policies for removing and potentially reviewing user material and traffic statistics¹ or other potential evidence of a service provider's financial interest. Greater leeway in considering legal standards generally is indulged by courts in allowing discovery, so long as relevant to a claim or defense, than when ruling on the merits. Discovery requests, however, must be reasonable

[Section 4.12[18]]

¹See *Io Group, Inc. v. Veoh Networks, Inc.*, No. C06-03926 HRL, 2007 WL 1113800 (N.D. Cal. Apr. 13, 2007) (granting in part a motion to compel on these issues).

and may be scaled back by a court when they are overly broad or unduly burdensome.

In *Perfect 10, Inc. v. CCBill, LLC*,² the Ninth Circuit held that, in evaluating a service provider's compliance with the threshold requirement that a service provider adopt, notify subscribers about and reasonably implement a policy of terminating "repeat infringers" in "appropriate circumstances," a court may also consider the service provider's responses in other instances where it received notifications or had knowledge or red flag awareness of infringement (not merely how it acted in responding to the plaintiff's own works) to evaluate whether it is properly identifying infringers and, by extension, reasonably implementing its repeat infringer policy. This substantially expands the potential scope of relevant discovery—at least for user storage cases³ in the Ninth Circuit. In the Ninth Circuit, and to the extent followed elsewhere, plaintiffs presumably will be entitled to some level of discovery on a service provider's response to *all* instances where it had notice, knowledge or red flag awareness in any case in which the DMCA is asserted as a defense, subject potentially to limitations imposed in response to a motion for a protective order based on scope and burdensomeness.

As discussed in section 4.12[3][B][iv], the court in *Arista Records LLC v. Usenet.com, Inc.*,⁴ following *Perfect 10*, imposed an evidentiary sanction on a service provider and other defendants precluding them from raising the DMCA as a defense to plaintiffs' suit for copyright infringement, based on bad faith spoliation of documents and other evasive tactics. The court wrote that "if defendants were aware of . . . red flags, or worse yet, if they encouraged or fostered

²*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

³The requirement that a service provider respond where it has knowledge or awareness also applies under the information location tools liability limitation, but would not necessarily impose similarly broad discovery obligations. Unless a service provider has subscribers or account holders, it is questionable whether it would have an obligation to terminate repeat infringers as a precondition to benefit from the information location tools safe harbor. *See supra* § 4.12[7].

⁴*Arista Records LLC v. Usenet.com, Inc.*, 633 F. Supp. 2d 124 (S.D.N.Y. 2009). Magistrate Judge Katz's earlier recommendation may be found at *Arista Records LLC v. Usenet.com, Inc.*, 608 F. Supp. 2d 409 (S.D.N.Y. 2009).

. . . infringement, they would be ineligible for the DMCA's safe harbor provisions."⁵ Because adequate records were not preserved, the court drew a negative inference against defendants.

Although not a DMCA case, it is worth noting that terminating sanctions also were imposed in *Columbia Pictures, Inc. v. Bunnell*,⁶ following the defendants' failure to comply with an earlier order entered in the case⁷ in which the court, ruling in response to recommendations by the magistrate judge,⁸ found that server log data that was temporarily stored in RAM was "extremely relevant" and ordered that it be preserved (in a manner that masked the IP addresses of the computers used by those accessing the site).⁹

Likewise, in *UMG Recording, Inc. v. Escape Media Group, Inc.*,¹⁰ which also was not a DMCA case because the plaintiffs focused on over 4,000 infringing sound recordings that had been uploaded by the defendant's own employees, Judge Thomas P. Griesa of the Southern District of New York entered evidentiary sanctions against the company that operated the Grooveshark online music service and its two co-founders, where defendants deleted records showing which sound recordings one of the co-founders had personally uploaded to the service and where other records of employee uploads and source code that would have corroborated employee uploads had been deleted during the pendency of

⁵633 F. Supp. 2d at 142. In that case, the defendants had wiped clean seven hard drives that belonged to employees without backing up the data to a central server, and failed to adequately preserve email communications. The defendants also sent potentially key witnesses to Europe during the height of discovery to "engineer their unavailability," encouraged witnesses to evade process, provided evasive or false sworn statements and violated two court orders requiring them to present information regarding the despoiled computer evidence, although Judge Baer concluded that while these abuses were not sufficient on their own to justify terminating sanctions they supported the finding that sanctions for discovery abuse were warranted.

⁶*Columbia Pictures, Inc. v. Bunnell*, 85 U.S.P.Q.2d 1448, 2007 WL 4877701 (C.D. Cal. Dec. 13, 2007).

⁷*Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443 (C.D. Cal. 2007).

⁸*Columbia Pictures Industries v. Bunnell*, NO. CV 06-1093FMCJXC, 2007 WL 2080419 (C.D. Cal. May 29, 2007).

⁹Spoliation is addressed more extensively in chapter 58.

¹⁰*UMG Recording, Inc. v. Escape Media Group, Inc.*, No. 11 Civ. 8407, 2014 WL 5089743, at *8–14 (S.D.N.Y. 2014).

parallel state court litigation brought for common law copyright infringement. As sanctions, the court found that plaintiffs were entitled to a finding that 1,944 files had been illegally uploaded based on defendants' spoliation of employee upload files and defendant Greenberg's upload files (in addition to affirmative evidence of over 4,000 other infringing files) and precluded defendants from relying on a defense that could have been disproven by the deleted source code.¹¹

In *Viacom Int'l, Inc. v. YouTube, Inc.*,¹² Judge Louis L. Stanton of the Southern District of New York ruled that the contents of user videos posted to YouTube and marked "private" by users could not be produced in discovery based on the prohibition against knowingly divulging the contents of any stored electronic communications on behalf of subscribers, subject to exceptions which do not include civil discovery requests.¹³ Among other things, the court found that YouTube's user agreement did not expressly authorize disclosure of this information.¹⁴ By contrast, the court held that non-content data, such as the number of times a video has been viewed on *YouTube.com* or made accessible on a third-party site through an embedded link to the video, was

¹¹*UMG Recording, Inc. v. Escape Media Group, Inc.*, No. 11 Civ. 8407, 2014 WL 5089743, at *8–14, 20 (S.D.N.Y. 2014). In a later ruling, Judge Griesa granted in part a motion *in limine* prohibiting the defendants from disputing at trial that they acted willfully and in bad faith, based on the court's earlier findings in connection with plaintiff's summary judgment motion that Groovespark overtly instructed its employees to upload as many files as possible, which the court held constituted purposeful conduct with a manifest intent to foster copyright infringement, and that Escape Media acted in bad faith in deleting relevant user data and source code, entitling the plaintiffs to potentially recover up to \$150,000 per work infringed. He also ruled, however, that the defendants were entitled to present evidence about the degree and extent of their willfulness and bad faith in connection with the jury's consideration of the amount of statutory damages to award. See *UMG Recordings, Inc. v. Escape Media Group, Inc.*, No. 11 Civ. 8407 (TPG), 2015 WL 1873098, at *3–4 (S.D.N.Y. Apr. 23, 2015); see generally *infra* § 4.14[2][A] (analyzing statutory damage awards).

¹²*Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256 (S.D.N.Y. 2008).

¹³*Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008), citing 18 U.S.C.A. § 2702(a)(2) and *In re Subpoena Duces Tecum to AOL, LLC*, 550 F. Supp. 2d 606, 611–12 (E.D. Va. 2008).

¹⁴253 F.R.D. at 264–65.

not barred from disclosure by the ECPA.¹⁵

In *Viacom*, the court also granted a protective order barring disclosure of the source code for the *YouTube.com* search function or VideoID program, which the court found to be trade secrets, but ordered production of all videos removed from the site and data on viewing statistics.

Discovery of electronically stored information and spoliation of electronic evidence are addressed more generally in chapter 58.¹⁶

4.12[19] The DMCA's Applicability to State Statutory and Common Law Copyright Claims

While the Copyright Act preempts most state common law and statutory copyright claims,¹ to the extent any state law claims remain today they would be subject to the DMCA safe harbors.

Prior to October 11, 2018, there was no federal protection for sound recordings fixed before February 15, 1972. With the enactment of the Classics Protection and Access Act (Title II of the Orrin G. Hatch–Bob Goodlatte Music Modernization Act of 2018),² Congress extended most aspects of federal copyright law protection to pre-1972 sound recordings and expressly provided that these rights were subject to the section 512 DMCA safe harbors.³

To the extent state common law and statutory claims are not preempted by the Copyright Act or the additional preemption rules of the Classics Protection and Access Act,⁴ those state law claims should be subject to the DMCA safe harbor if asserted against a service provider otherwise entitled to take advantage of section 512 protections. In

¹⁵*Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 265 (S.D.N.Y. 2008).

¹⁶See generally *infra* §§ 58.03[5] (spoliation), 58.03[6] (fee shifting), 58.04[4] (discovery sanctions).

[Section 4.12[19]]

¹See 17 U.S.C.A. § 301; see generally *infra* § 4.18.

²The Orrin G. Hatch–Bob Goodlatte Music Modernization Act, PL 115-264, 2018 H.R. 1551, 132 Stat. 3676 (Oct. 11, 2018).

³See 17 U.S.C.A. § 1401(f)(3).

⁴See 17 U.S.C.A. §§ 301(c), 1401(e); see generally *infra* § 4.18[2].

Capitol Records, LLC v. Vimeo, LLC,⁵ the Second Circuit ruled that the Digital Millennium Copyright Act safe harbors apply to state statutory and common law copyrights, and not just federal copyright claims. In so ruling, the Second Circuit rejected the view of the U.S. Copyright Office that the DMCA applied only to common law copyrights. Judge Leval, writing for himself and Judges Hall and Lynch, held that:

Whether we confine our examination to the plain meaning of the text, or consider in addition the purpose the text was intended to achieve, we find no reason to doubt that § 512(c) protects service providers from all liability for infringement of all copyrights established under the laws of the United States, regardless whether established by federal law or by local law under the sufferance of Congress, and not merely from liability under the federal statute.⁶

In a subsequent opinion withdrawn upon reconsideration, the Ninth Circuit, in *dicta*, agreed with this analysis, in comparing the DMCA safe harbor created by section 512 (which it characterized as applying to both federal and state copyrights) with the compulsory license for music broadcasters created by 17 U.S.C.A. § 114, which it held, by its turn, applied only to federal copyrights.⁷

The conclusion that the DMCA safe harbors apply to state statutory and common law copyrights was significant when the Second Circuit first reached this decision—and important for service providers given that it is potentially difficult for a service provider to distinguish sound recordings fixed prior to February 15, 1972 from those works fixed after that date. Among other things, some artists recorded different versions of the same song before and after February 15, 1972. Moreover, many pre-1972 sound recordings were remastered after 1972 and separately registered as new or derivative works. In addition, mixes and mashups posted online or in social media may include excerpts from either pre- or post-1972 sound recordings. These issues and others surrounding state statutory and common law copyrights are separately ad-

⁵*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 87-93 (2d Cir. 2016).

⁶*Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 90 (2d Cir. 2016); see also *EMI Christian Music Group, Inc. v. MP3tunes, LLC*, 844 F.3d 79, 91 n.7 (2d Cir. 2016) (reaffirming *Vimeo* on the DMCA's applicability to state law copyright claims).

⁷See *ABS Entertainment, Inc. v. CBS Corp.*, 900 F.3d 1113, 1137-38, withdrawn and replaced by, 908 F.3d 405 (9th Cir. 2018).

dressed in section 4.18[2].

4.13 Equitable Remedies and Defenses in Civil Litigation

4.13[1] Injunctive Relief and Equitable Defenses (including waiver, estoppel, laches and unclean hands)

Injunctive relief generally may be obtained at three different stages in a lawsuit:

- temporary restraining orders (TROs) at the outset of litigation;
- preliminary injunctions early in the proceedings; and
- permanent injunctions following trial or final judgment.

The purpose of a temporary restraining order is to preserve the *status quo* and prevent irreparable harm until a hearing may be held on a motion for preliminary injunction.¹

An injunction is an equitable remedy. Injunctive relief is an “extraordinary and drastic remedy” that “is never awarded as of right.”² While the standards for obtaining injunctions in copyright cases had been relaxed over time, with most courts presuming irreparable injury if a strong enough showing was made that a plaintiff was likely to prevail on the merits, the U.S. Supreme Court made clear in *eBay, Inc. v. MercExchange, LLC*³ and *Winter v. Natural Resources Defense Council*⁴ that this presumption was unwarranted and a plaintiff seeking a preliminary injunction must show that irreparable injury is likely in the absence of an injunction.⁵

Injunctive relief is not automatic merely because a copy-

[Section 4.13[1]]

¹*Granny Goose Foods, Inc. v. Brotherhood of Teamsters and Auto Truck Drivers Local No. 70 of Alameda County*, 415 U.S. 423, 439 (1974); Fed. R. Civ. Proc. 65.

²*Munaf v. Geren*, 553 U.S. 674, 689–90 (2008).

³*eBay Inc. v. MercExchange, LLC*, 547 U.S. 388 (2006).

⁴*Winter v. Natural Resources Defense Council, Inc.*, 555 U.S. 7 (2008).

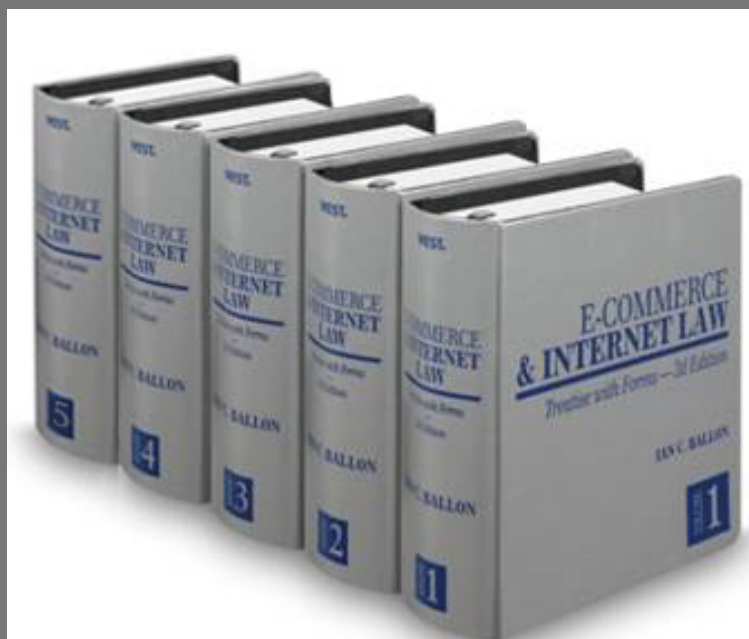
⁵*See, e.g., CoxCom, Inc. v. Chaffee*, 536 F.3d 101, 111–12 (1st Cir. 2008) (applying eBay); *Salinger v. Colting*, 607 F.3d 68, 77–78 (2d Cir. 2010) (holding that likelihood of success on the merits in a copyright infringement case no longer raises a presumption of irreparable harm; vacating the lower court’s entry of a preliminary injunction); *TD Bank N.A. v.*

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2022

Ian C. Ballon

2022
UPDATES -
INCLUDING
NEW AND
IMPORTANT
FEATURES

THE PREEMINENT
INTERNET AND
MOBILE LAW
TREATISE FROM A
LEADING INTERNET
LITIGATOR — A
5 VOLUME-SET &
ON WESTLAW!



To order call **1-888-728-7677**
or visit **lanBallon.net**

Key Features of E-Commerce & Internet Law

- ◆ AI, ML, screen scraping and data portability
- ◆ Antitrust in the era of techlash
- ◆ The CPRA, Virginia, Colorado and Nevada privacy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- ◆ Software copyrightability and fair use after *Google v. Oracle*
- ◆ Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- ◆ TCPA law and litigation after *Facebook v. Duguid* - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- ◆ The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- ◆ Platform moderation and liability, safe harbors, and defenses (including the CDA and DMCA)
- ◆ Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- ◆ The law of SEO and SEM – and its impact on e-commerce vendors
- ◆ Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- ◆ IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi*, patentable subject matter, negative trade secrets, rights of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- ◆ Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- ◆ Sponsored links, embedded links, #hashtags, and internet, mobile and social media advertising
- ◆ Enforcing judgments against foreign domain name registrants
- ◆ Valuing domain name registrations from sales data
- ◆ Applying the First Sale Doctrine to virtual goods
- ◆ Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- ◆ Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- ◆ Click fraud
- ◆ Copyright and Lanham Act fair use
- ◆ Practical tips, checklists and forms that go beyond the typical legal treatise
- ◆ Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ AI/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- ◆ Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- ◆ Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- ◆ Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- ◆ Addresses both law and best practices
- ◆ Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- ◆ Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

Volume 1

Part I. Sources of Internet Law and Practice: A Framework for Developing New Law

- Chapter* 1. Context for Developing the Law of the Internet
2. A Framework for Developing New Law
3. [Reserved]

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Data Scraping, Database Protection, and the Use of Bots and Artificial Intelligence to Gather Content and Information
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names

Volume 2

- Chapter* 8. Internet Patents
9. Unique Intellectual Property Issues in Search Engine Marketing, Optimization and Related Indexing, Information Location Tools and Internet and Social Media Advertising Practices
10. Misappropriation of Trade Secrets in Cyberspace
11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property
12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace
13. Idea Submission, Protection and Misappropriation
- ### **Part III. Licenses and Contracts**
14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: The Federal eSign Statute, Uniform Electronic Transactions Act, UICITA, and the EU Distance Selling Directive
16. Internet Licenses: Rights Subject to License and Limitations Imposed on Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content Licensing Pre-Existing Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements

Volume 3

- Chapter* 24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements
- ### **Part IV. Privacy, Security and Internet Advertising**
25. Introduction to Consumer Protection in Cyberspace
26. Data Privacy
27. Cybersecurity: Information, Network and Data Security
28. Advertising in Cyberspace

Volume 4

- Chapter* 29. Email and Text Marketing, Spam and the Law of Unsolicited Commercial Email and Text Messaging
30. Online Gambling

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. State and Local Sales and Use Taxes on Internet and Mobile Transactions
34. Antitrust Restrictions on Technology Companies and Electronic Commerce
35. Dormant Commerce Clause and Other Federal Law Restrictions on State and Local Regulation of the Internet
36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

Part VI. Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption

37. Defamation, Torts and the Good Samaritan Exemption (47 U.S.C.A. § 230)
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression in Cyberspace

Part VII. Obscenity, Pornography, Adult Entertainment and the Protection of Children

40. Child Pornography and Obscenity
41. Laws Regulating Non-Obscene Adult Content Directed at Children
42. U.S. Jurisdiction, Venue and Procedure in Obscenity and Other Internet Crime Cases

Part VIII. Theft of Digital Information and Related Internet Crimes

43. Detecting and Retrieving Stolen Corporate Data
44. Criminal and Related Civil Remedies for Software and Digital Information Theft
45. Crimes Directed at Computer Networks and Users: Viruses and Malicious Code, Service Disabling Attacks and Threats Transmitted by Email

Volume 5

- Chapter* 46. Identity Theft
47. Civil Remedies for Unlawful Seizures
- ### **Part IX. Liability of Internet Sites and Service (Including Social Networks and Blogs)**
48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Content Moderation and Platform Liability: Service Provider and Website, Mobile App, Network and Cloud Provider Exposure for User Generated Content and Misconduct
50. Cloud, Mobile and Internet Service Provider Compliance with Subpoenas and Court Orders
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites
- ### **Part X. Civil Jurisdiction and Litigation**
52. General Overview of Cyberspace Jurisdiction
53. Personal Jurisdiction in Cyberspace
54. Venue and the Doctrine of Forum Non Conveniens
55. Choice of Law in Cyberspace
56. Internet ADR
57. Internet Litigation Strategy and Practice
58. Electronic Business and Social Network Communications in the Workplace, in Litigation and in Corporate and Employer Policies
59. Use of Email in Attorney-Client Communications

“Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet.”

Jay Monahan

General Counsel, ResearchGate

ABOUT THE AUTHOR

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator in the firm's Silicon Valley Los Angeles and Washington, DC offices. He defends data privacy, cybersecurity breach, AdTech, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database, AI and other intellectual property cases, including disputes involving safe harbors and exemptions, platform liability and fair use.



Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top Intellectual Property litigators in every year the list has been published (2009-2021), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was selected as the Lawyer of the Year for information technology law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. He also serves as Executive Director of Stanford University Law School's Center for the Digital Economy.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

Mr. Ballon is also the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.IanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@IanBallon).

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2022

- > **Antitrust in the era of techlash** (chapter 34)
- > **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- > **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- > **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurity breach, data privacy, AdTech and TCPA class action suits.**
- > **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- > **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- > **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- > **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States*, 141 S. Ct. 1648 (2021)** (ch5)
- > **FOSTA-SESTA and ways to maximize CDA protection** (ch 37)
- > **IP aspects of the use of #hashtags in social media** (ch 6)
- > **The CLOUD Act** (chapter 50)
- > **Virginia, Colorado and Nevada privacy laws** (ch 26)
- > **Applying the single publication rule to websites, links and uses on social media** (chapter 37)
- > **Digital economy litigation strategies**
- > **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- > **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- > **Website and mobile accessibility under the ADA and state laws** (chapter 48)
- > **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- > **Updated *Defend Trade Secrets Act* and UTSA case law** (chapter 10)
- > **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- > **AdTech law** (chapter 28, Darren Abernethy)
- > **The risks of being bound by the CASE Act's ostensibly *voluntary* jurisdiction over small copyright cases**
- > **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- > **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- > **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- > **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 26)
- > **Patent law** (updated by Josh Raskin) (chapter 8)
- > **Idea protection & misappropriation** (ch 13)
- > **Revisiting links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- > **eSIGN case law** (chapter 15)

**SAVE 20% NOW!! To order call 1-888-728-7677
or visit IanBallon.net
enter promo code **WPD20** at checkout**

List Price: \$3,337.00
Discounted Price: \$2,669.60

LINKS (INCLUDING EMBEDDED LINKS) – IN GENERAL

Excerpted from the forthcoming 2022 updates to Chapter 9 (Unique Intellectual Property Issues in Search Engine Marketing, Optimization and Related Indexing, Information Location Tools and Internet and Social Media Advertising Practices)

E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition

A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

(These excerpts are unrevised page proofs for the current update and may contain errors. Please email the author at ballon@gtlaw.com for a complimentary copy of the final published version.)

IP LAW YEAR IN REVIEW

4TH ANNUAL HBCU TECH LAW SUMMIT AND 19TH ANNUAL IP AND SOCIAL JUSTICE CLE SEMINAR

INSTITUTE FOR INTELLECTUAL PROPERTY AND SOCIAL JUSTICE
HOWARD UNIVERSITY SCHOOL OF LAW
MARCH 3-4, 2022

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles: 1840 Century Park East, Ste. 1900 Los Angeles, CA 90067 Direct Dial: (310) 586-6575 Direct Fax: (310) 586-0575	Silicon Valley: 1900 University Avenue, 5th Fl. East Palo Alto, CA 914303 Direct Dial: (650) 289-7881 Direct Fax: (650) 462-7881	Washington, D.C.: 2101 L Street, N.W., Ste. 1000 Washington, D.C. 20037 Direct Dial: (202) 331-3138 Fax: (202) 331-3101
--	---	--

Ballon@gtlaw.com

<www.ianballon.net>

LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition* (Thomson West 2022 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (888) 728-7677
www.ianballon.net



Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal
Circuits

U.S. Supreme Court

JD, LLM, CIPP/US

Ballon@gtlaw.com

LinkedIn, Twitter, Facebook: IanBallon

Los Angeles

1840 Century Park East
Suite 1900

Los Angeles, CA 90067

T 310.586.6575

F 310.586.0575

Silicon Valley

1900 University Avenue
5th Floor

East Palo Alto, CA 94303

T 650.289.7881

F 650.462.7881

Washington, D.C.

2101 L Street, N.W.

Suite 1000

Washington, DC 20037

T 202.331.3138

F 202.331.3101

Ian C. Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and TCPA class action suits.

Ian is also the author of the leading treatise on internet and mobile law, [E-Commerce and Internet Law: Treatise with Forms 2d edition](#), the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of intellectual property law issues. In addition, he serves as [Executive Director of Stanford University Law School's Center for the Digital Economy](#). He also chairs [PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation](#) conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian was named the Lawyer of the Year for Information Technology Law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of Best Lawyers in America (including lawyer of the year for 2022). In 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder's* 2017 Litigation Departments of the Year Awards. He was also recognized as the 2012 [New Media Lawyer of the Year](#) by the Century City Bar Association. In 2010, he was the recipient of the California State Bar Intellectual Property Law section's [Vanguard Award for significant contributions to the development of intellectual property law](#). Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2021), and has been listed as a Northern California Super Lawyer every year from 2004 through 2021 and as one of the top 100 lawyers in California. He is also listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology.

Ian holds JD and LLM degrees and the [CIPP/US certification from the International Association of Privacy Professionals \(IAPP\)](#).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 2



THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

lows that he also knowingly received them.”¹¹

On the other hand, in *United States v. Navrestad*,¹² the Court of Appeals for the Armed Forces held that a defendant could not be convicted of possessing or distributing child pornography under the CPPA where, instead of using his own computer, the defendant accessed child pornography sites on a public computer at an Internet cafe, and thus cached copies were made on a hard drive owned by the Internet cafe, not the defendant. In addition, the government failed to present any evidence that the defendant even knew those temporary copies had been made. Although the defendant sent an email to a third party containing a link to the location online where the images could be accessed, the court held that emailing a link did not amount to distribution under the CPPA.

Child pornography laws are analyzed more extensively in section 40.01.

9.03 Hypertext Links

9.03[1] Links and Liability for Linking—In General

Links (also known as *hypertext links* or *hyperlinks*) allow visitors to a site to easily and quickly connect to another location on the World Wide Web or to view content located on another site. Site owners may use links, among other reasons, to show users material from third party locations on the Internet without actually copying it. A link is created by inserting the URL of the site to be linked into some HTML code, which then allows visitors to the website to point and click on a particular icon or portion of highlighted text and automatically access the linked location. A link is merely an instruction to a browser to go from one location to another. A link therefore does not create a “copy” within the meaning of *MAI Systems Corp. v. Peak Computer, Inc.*,¹ on the server of the party creating a link and therefore, subject to some exceptions discussed in this section, generally will not sup-

¹¹*U.S. v. Romm*, 455 F.3d 990, 1002 (9th Cir. 2006), citing *U.S. v. Mohrbacher*, 182 F.3d 1041, 1048 (9th Cir. 1999) (holding that downloading child pornography constitutes both the act of possession and receipt).

¹²*U.S. v. Navrestad*, 66 M.J. 262 (C.A.A.F. 2008).

[Section 9.03[1]]

¹*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 510 U.S. 1033 (1994); see generally *supra* § 9.01.

port a claim for direct infringement (although it may create a cached “copy” on a user’s screen memory² and therefore potentially facilitate a claim for secondary liability even where direct liability may not be imposed). Linking *per se* likewise generally is not actionable under the *Lanham Act*. In particular cases, however, in narrow circumstances, linking may support certain claims.

Linking is a central component of the World Wide Web. The very name *World Wide Web* conjures up an image of multiple locations linked together like a spider’s web. Nonetheless, at the dawn of the Internet era, linking led to consternation on the part of companies that were astonished to learn that strangers could link to their sites. Businesses that were accustomed to making deliberate decisions about how to promote their goods and services and corporate images felt seemingly powerless to control their brand image and messaging when they came to understand that people and entities with whom they had no desire to affiliate could encourage their customers or visitors to obtain free content (via links), disrupt the appearance of a page (with frames), alter the order in which content was presented (through *content links*, also known as *deep links*) or seemingly copy material from their sites via *in-line links*.³ This early sense that people were getting something for nothing or misappropriating a company’s content or image led to a number of lawsuits, which in turn have left the lasting perception that linking can lead to liability. While certain forms of links may be actionable, much of the linking that takes place online is not.

Liability for linking under the Copyright Act typically is limited to claims for secondary liability where the link encourages or induces infringement. Copyright liability also potentially could be imposed where a link displays a live performance or streamed transmission that constitutes a public performance. Liability alternatively potentially could be imposed where a link is created in violation of a copyright license or contract, such as website Terms of Use, where copyright liability was premised on exceeding the scope of the license. In general, however, it is difficult to impose liability under the Copyright Act for most types of links.

Copyright law also may not be helpful by analogy when a

²See *supra* § 9.02.

³See *infra* § 9.04 (frames and in-line and embedded links).

breach of contract dispute turns on links.⁴

In contrast to regular links, in-line or embedded links or frames, while generally viewed in the same way as other links in most jurisdictions, may be directly actionable in some venues.

Even where a *prima facie* case may be made for copyright infringement, a potential defendant may be able to avoid liability under the information location tools safe harbor of the Digital Millennium Copyright Act, the *Sony* safe harbor or the defenses of fair use, *de minimis* infringement, or implied license.⁵

Under the Lanham Act, a link could lead to liability to the extent that it falsely suggests sponsorship, affiliation or endorsement. The risk of consumer confusion may be greatest when content is framed or made accessible through in-line links, depending on how they are structured and what notices or disclaimers may be prominently posted. A confusing link potentially could be actionable based on traditional likelihood of confusion analysis and, even more so, initial interest confusion, where recognized.⁶

The significance of a simple link should not be overstated. A link facilitates navigation from one location to another, but usually does not lead people to places they could not otherwise go.

Links also generally are favored by most site owners. Among other things, the more links that are established to a site, the higher the site will be ranked in response to search engine queries.

A link often does little more than make it easy for a user to point and click to quickly go to a site that otherwise could be accessed by typing out a URL or finding the location using a search engine. Few people would dispute that a site

⁴See *Panda Paws Rescue v. Walters*, Case No. C20-5700JLR, 2021 WL 22591, at *6 (W.D. Wash. Jan. 4, 2021) (denying defendant's motion to dismiss plaintiff's breach of contract claim, alleging that by linking to a video the defendant breached his settlement agreement obligation to not "display" certain images, because even though a link does not display an image for purposes of copyright law under *Perfect 10*, what the parties intended by the term in their contract is a disputed issue that could not be resolved on a motion to dismiss).

⁵See *infra* §§ 9.03[3][B], 9.03[3][C].

⁶See *supra* § 7.08[2].

owner generally⁷ could display a URL prominently for users to copy (or cut and paste into their browsers).

Viewed in context, an ordinary site link typically is merely the interactive analogue to an address or telephone listing publicized by a third-party in a newspaper or magazine.⁸ The acts of embedding code (which instructs a browser to go to a specific URL) and displaying the typed address in a different color (or placing an icon on top of it), therefore, should not in and of themselves be deemed actionable (and typically do not absent additional facts such as active encouragement to access infringing material, a link used to create a public performance in a frame, in-line link or embedded link, or use in ways that under the Lanham Act would be viewed as likely to cause confusion or dilution).

Hypertext links may be established as either *site links* or *content links*. A site link connects a visitor to the first page of a website, where website owners typically include introductory information intended to promote the site and any goods or services they sell, and include links to the terms and conditions for visiting the location. While some site owners sought to establish legal precedent restricting content links in the early days of the commercialization of the Internet, they were largely unsuccessful in doing so.

Similarly, efforts to restrict content links (also known as *deep links*), as compared to site links, were also largely unsuccessful. A content or deep link connects a visitor directly to specific material posted beyond the homepage. A content link therefore allows a user to bypass whatever introductory promotional material (or legal notices) the owner of the site may have intended visitors to review before gaining access to the linked content. In some cases, a content link connects to more desirable material that may have been posted solely as an inducement for people to visit the site and review promotional information or advertisements on

⁷A list of addresses to otherwise unknown or difficult to locate sites, where infringing content or information on how to find infringing content or how to disable anti-piracy devices is posted, could potentially give rise to a claim for contributory copyright infringement if the list in fact was used by people to make infringing copies. *See supra* § 4.11.

⁸Creating an ordinary site link is not substantially different from including a company's telephone number in a magazine (except that on *terra firma* the magazine will not automatically dial the number in the same way that a browser will call up a website in response to a link and a user's click of a mouse).

the homepage. Content links, unlike site links, therefore were perceived as unfair by some site owners in the early days of the Internet (although not necessarily unlawful). Unless restricted by an enforceable contract or license or likely to cause confusion under the Lanham Act, an ordinary content link *per se* is not actionable, even if it may be viewed as more objectionable than a link to a site's homepage.

Today, there are other, more effective means available to grab someone's attention or make sure they assent to Terms and Conditions before using a site, than forcing users to click through other pages first. Indeed, as a practical matter, a site or service cannot easily restrict access to internal pages on a website without running the risk that users will lose patience and never click through to material made available only after a user takes multiple intermediary steps.

In the early days of the commercial Internet, when objections to deep links were first raised, some site owners sought to force visitors through a series of screens before allowing them to access particular content. Even then, however, an owner's homepage often could be easily by-passed if a user bookmarked an internal page (albeit usually after having visited the owner's homepage at least one time) or accessed the content via a search engine query.

In addition to potential exposure for the link itself, copyright or trademark liability could potentially arise if a site owner, in conjunction with establishing an otherwise permissible link to another site, uses a protected work as an icon (such as a copyrighted cartoon character or the company logo of the linked site), or a trademark or service mark as underlined text or an icon from which the link may be accessed. Uses of a company's name in a non-trademark sense or as a fair use, by contrast, generally would be permissible.⁹ Use of logos or protected images in particular are less likely to be deemed a fair use under the Lanham Act if the court determines that more of the mark was used than necessary in connection with any plausibly fair use. Where plain text would suffice, more substantial uses may not be found fair.

In contrast to ordinary links, companies may face somewhat greater risks in connection with embedded links, inline links or links that display linked content in frames,

⁹*See supra* § 6.14.

which are separately addressed in sections 9.03 and 9.04.

Sponsored links, which are links used in connection with advertising, are separately analyzed in section 9.11.

9.03[2] Linking Compared to Caching

To a user, there may be no practical difference between pointing and clicking on an icon that will connect to genuine content on an authorized website via a link, and pointing and clicking on an icon that will call up the same material that had been cached. The legal difference between caching and linking, however, may be more pronounced. Although it could constitute copyright infringement to copy the graphic representations found on a given website to a different location, a link merely is an instruction to a browser to go from one location to another and therefore generally does not create a “copy” within the meaning of *MAI Systems Corp. v. Peak Computer, Inc.*¹ As the Ninth Circuit observed, “[w]hile in-line linking and framing may cause some computer users to believe they are viewing a single . . . webpage, the Copyright Act, unlike the Trademark Act, does not protect a copyright holder against acts that cause consumer confusion.”²

Caching occurs for multiple reasons over the internet—both legitimate and (in the case of spoofers) nefarious. Caching relieves congestion over the Internet and allows for faster user access to specific content, but may deny a site owner valuable user data and advertising revenue. Hyperlinks, by contrast, increase traffic to a website and may benefit both the company that establishes the link, and the linked site, by increasing visits to both locations. On the other hand, if the linked site is already popular, the linking site may simply be trying to increase traffic to its own site by establishing links to popular third party locations. Links may also be troubling to companies to the extent that they could be construed as suggesting sponsorship, affiliation or endorsement.

Except where visitors or linking sites mask their identity,

[Section 9.03[2]]

¹*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994); *see generally supra* §§ 4.03, 9.01.

²*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1161 (9th Cir. 2007).

a website owner (or its host) generally knows the last page viewed before a user accessed its site³ and in those instances can determine the source of links to its site (at least those links that actually point to the correct address and are used to access it). By comparison, the owner of a website may be unaware that its site has been cached unless it stumbles upon the cached location or a customer complains directly to it.

Indeed, in one case, Judge Margaret Morrow of the Central District of California even cited linking as a permissible non-infringing alternative to copying content from another site, which effectively undermined the defendant's fair use and First Amendment defenses in a copyright infringement suit. In that case—*Los Angeles Times v. Free Republic*⁴—defendant's racist website included verbatim copies of newspaper articles that had originally appeared in *The L.A. Times* and *Washington Post*. The defendants had argued that linking was impractical because the plaintiffs' articles appeared online free of charge for only a brief period of time before they were archived and made available for a fee. Judge Morrow wrote: "That this is so does not make linking plaintiffs' websites to the Free Republic site 'impractical.' It merely requires that Free Republic visitors pay a fee for viewing plaintiffs' articles just as other members of the public do."⁵

The court also rejected the argument that linking was impractical because unsophisticated users would be confused by the link. In a statement that contradicts the view of more conservative lawyers who believe that content (or "deep") linking generally violates the Lanham Act, Judge Morrow wrote (in the context of copyright fair use) that "defendant's assertion that unsophisticated Internet users would be confused by links is unpersuasive. Linking is familiar to most Internet users, even those who are new to the web."⁶

Unlike a typical link, which remains accessible for a defined period of time, the *Free Republic* case involved

³See *infra* §§ 26.01 to 26.03, 37.02.

⁴*Los Angeles Times v. Free Republic*, 54 U.S.P.Q.2d 1453, 2000 WL 565200 (C.D. Cal. Mar. 31, 2000).

⁵*Los Angeles Times v. Free Republic*, 54 U.S.P.Q.2d 1453, 2000 WL 565200 (C.D. Cal. Mar. 31, 2000).

⁶*Los Angeles Times v. Free Republic*, 54 U.S.P.Q.2d 1453, 2000 WL 565200 (C.D. Cal. Mar. 31, 2000).

content links that were frequently rotated because the plaintiffs' news stories remained online only briefly.

9.03[3] Potential Copyright Liability for Creating Hyperlinks

9.03[3][A] Grounds for Liability

9.03[3][A][i] In general

A link is merely an instruction to a browser to go from one location to another. Accordingly, most courts that have considered the issue have held that a link, by itself, does not implicate "copying." The leading case is *Perfect 10, Inc. v. Amazon.com, Inc.*,¹ in which the Ninth Circuit adopted the "server test" in evaluating a claim asserting that links to photographs on other internet locations constituted unauthorized reproduction, distribution and public display under the Copyright Act. Under this test, merely creating a link to content on another server would not lead to direct liability, although it potentially could result in secondary liability for inducing copyright infringement or contributory or vicarious liability (based on direct infringement by a user, if any).² The only other circuit to consider the issue as of this writing is the Seventh Circuit, which held in *Flava Works, Inc. v. Gunter*,³ that a claim for contributory copyright infringement could not be based on creating bookmark links to infringing videos. The Seventh Circuit further suggested in *dicta* that direct liability similarly could not be imposed. Because of these two precedential circuit court opinions and the recognition that the entire structure of the World Wide Web is premised on establishing links between sites (and from search engines), ordinary links have rarely resulted in liability for copyright infringement except where links are obviously used to promote infringement (such as when a site creates numerous links to pirated content, or links to unauthorized material previously displayed on the defendant's

[Section 9.03[3][A][i]]

¹*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007).

²The grounds for establishing liability for direct, contributory, and vicarious liability, and for inducement, are analyzed extensively in section 4.11.

³*Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012).

own site, in lieu of hosting the material directly)⁴ or when linking occurs in conjunction with other acts of infringement⁵ (although linking has been included in boilerplate lists of activities to be enjoined in cases where other acts of infringement have been established, especially where the orders are entered as default judgments or as part of a stipulated settlement). There also should be no difference in most cases whether a link is established to the homepage of another site or is a content link (or “deep link”), which leads directly to information on an interior page of a website, despite several highly publicized efforts in the 1990s and thereafter to prevent this form of linking.⁶ While merely establishing a link to otherwise noninfringing content rarely has led to direct liability, some district courts—in decisions that disagree with or seek to distinguish *Perfect 10*—have held that a *prima facie* case for direct liability potentially may be made (subject to potential defenses) where in-line or embedded links or frames create public displays⁷ of photographs.⁸ From

⁴See, e.g., *Batesville Services, Inc. v. Funeral Depot, Inc.*, No. 1:02–CV–01011–DFH–TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004) (holding that a triable issue of fact existed on the issue of defendant’s potential direct liability for creating links to unauthorized photographs of plaintiff’s products, after having been warned to stop displaying the pictures itself on its own website); *Arista Records, Inc. v. Mp3Board, Inc.*, No. 00 CIV. 4660 (SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002) (denying cross-motions for summary judgment in a suit brought against a service that aggregated links to infringing music files, finding that a reasonable trier of fact could determine that MP3Board “engaged in an overall course of conduct which materially contributed” to copyright infringement by offering a search engine that collected and organized links to third-party sites that included audio files, solicited third-party links to such sites, offered a tutorial for new users that provided instructions on how to locate and download audio files and used one of plaintiffs’ protected works as an example in the tutorial).

⁵See, e.g., *Batesville Services, Inc. v. Funeral Depot, Inc.*, No. 1:02–CV–01011–DFH–TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004) (holding that a triable issue of fact existed on the issue of defendant’s potential direct or contributory liability for creating links to unauthorized photographs of plaintiff’s products, and for designing, creating and paying for the pages that it linked to, after having been warned to stop displaying the pictures itself on its own website); *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp. 2d 1290 (D. Utah 1999) (enjoining defendants from creating links to third-party sites that contained infringing material and encouraging users to visit those locations).

⁶See *infra* §§ 9.03[3][A][ii], 9.03[6], 9.03[7].

⁷The exclusive rights of a copyright owner—distribution, reproduction, public performance, public display, digital transmission and adapta-

a copyright perspective, embedded, in-line or framed links to static content should not be actionable because—like all links—they are set up merely as instructions to a browser to view material posted on a third party location and do not create a separate “fixed” copy on the website or the social media post that frames or establishes the in-line or embedded link to the third-party material, as discussed in section 9.03[3]. Nevertheless, some district courts, which consider an embedded link to a photograph to create a public display, would distinguish embedded or in-line links and frames from regular links in cases involving the display of a photograph from a third party website because the photo could be seen automatically via the embedded or inline link or frame (rather than after clicking on the link and being transferred to a third party website).

A *prima facie* case also was found for in-line linking live performances of streamed content,⁹ which may be accounted for because, unlike the other exclusive rights of a copyright

tion—are analyzed extensively in section 4.04[1].

⁸See, e.g., *Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *3-5 (S.D.N.Y. 2021) (denying defendant’s motion to dismiss plaintiff’s copyright infringement claim, holding that plaintiff stated a claim that Sinclair’s placement of an embedded link to plaintiff’s video of a starving polar bear (which plaintiff had uploaded to Instagram and Facebook), in an article describing how the video “went ‘viral,’” constituted an unauthorized public display, and that Sinclair’s fair use defense could not be resolved on a motion to dismiss); *Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585 (S.D.N.Y. 2018) (holding that an image displayed via embedded links in various publications, from the Twitter feed where it had been posted, constituted a public display under the Copyright Act; granting partial summary judgment to the plaintiff); *The Leader’s Institute, LLC v. Jackson*, Civil Action No. 3:14-CV-3572-B, 2017 WL 5629514, at *10 (N.D. Tex. Nov. 22, 2017) (denying plaintiff’s motion for summary judgment on defendant’s counterclaim for copyright infringement, holding that plaintiff publicly displayed copyrighted content from defendant’s website by framing it on its own website; distinguishing framing from ordinary linking). *But see Flava Works, Inc. v. Gunter*, 689 F.3d 754, 761 (7th Cir. 2012) (holding that creating an in-line link to videos via frames from the defendant’s website did not amount to a public performance); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1160-61 (9th Cir. 2007) (holding that Google did not violate plaintiff’s public display right in its photographs by creating in-line links to them in frames).

⁹See *Live Nation Motor Sports, Inc. v. Davis*, 81 U.S.P.Q.2d 1826, 2007 WL 79311 (N.D. Tex. Jan. 9, 2007) (holding that a link to a stream of a live webcast of motor races that were shown in real time constituted a public performance or display because those terms encompass “each step in the process by which a protected work wends its way to the audience”). *But see Flava Works, Inc. v. Gunter*, 689 F.3d 754, 761 (7th Cir. 2012)

owner, a public performance is “fixed” simultaneously with its transmission.¹⁰

Frames and in-line and embedded links are links that modify a user’s screen, displaying content from one location via a different site. These types of links are also addressed in section 9.04.

Aside from links to streamed content that may constitute public performances, ordinary links that lead to static material should not form the basis for a claim for direct infringement. Needless to say, even where a *prima facie* case may be established, substantial defenses, including the Digital Millennium Copyright Act safe harbor for “information location tools,” fair use,¹¹ and implied license¹² may

(holding that creating an in-line link to videos via frames from the defendant’s website did not amount to a public performance).

¹⁰A work that is reproduced, distributed, adapted or publicly displayed is fixed in a tangible medium of expression “when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.” 17 U.S.C.A. § 101. By contrast, a work “consisting of sounds, images, or both, that are being transmitted, is ‘fixed’ for purposes of this title if a fixation of the work is being made simultaneously with its transmission.” *Id.*

¹¹*See, e.g., Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 6393010 (E.D.N.Y. Nov. 2, 2020) (dismissing, as fair use, the copyright infringement claim of a photographer against a sports news publisher, which had included an embedded link to an Instagram post by professional tennis player Caroline Wozniacki, announcing her retirements (which included a low-resolution, cropped version of a photograph taken by the plaintiff), in an article it published about Wozniacki’s career, which also quoted the text of the Instagram post); *Walsh v. Townsquare Media, Inc.*, 464 F. Supp. 3d 570 (S.D.N.Y. 2020) (entering judgment on the pleadings, based on fair use, in a Paparazzi photographer’s copyright infringement claim, brought against the publisher of *XXL* magazine, which had embedded a link to an Instagram post by hip hop artist Cardi B, which included a photograph taken by plaintiff of Cardi B at a Tom Ford fashion show, in an article entitled *Cardi B Partners with Tom Ford for New Lipstick Shade*, which was focused on the event and referenced the Cardi B Instagram post which featured the photograph); *see also Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 7625222 (E.D.N.Y. Dec. 22, 2020) (denying reconsideration). *Cf. Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *5-7 (S.D.N.Y. 2021) (denying defendant’s motion to dismiss plaintiff’s copyright infringement claim, premised on Sinclair’s placement of an embedded link to plaintiff’s video of a starving polar bear in an article describing how the video “went ‘viral,’” because Sinclair’s fair use defense could not be resolved on a mo-

tion to dismiss based solely on the allegations of the complaint, despite finding that the use was transformative); *McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 604-09 (S.D.N.Y. 2020) (holding, in an opinion decided before *Boesen* and *Walsh*, that, on the facts of that case, fair use could not be established as a matter of law at the pleadings stage, in a case where plaintiff posted a photograph of an ephemeral lake on March 13, 2019, and the very next day Newsweek allegedly published an article about the ephemeral lake, embedding plaintiff's Instagram post about the lake, as part of the article); see generally *supra* § 4.10[1] (analyzing fair use).

¹²An implied license generally may not be inferred where there is an express license agreement between the parties for the same subject matter. See, e.g., *Baer v. Chase*, 392 F.3d 609, 616-17 (3d Cir. 2004) ("There cannot be an implied-in-fact contract if there is an express contract that covers the same subject matter.").

District court judges in New York have held that Instagram receives an express license from users who upload images to its platform, to allow other users to embed those images, but whether Instagram in turn grants its users a license to imbed images posted by other users, when they use Instagram's API (application programming interface) to embed a link to an image posted on Instagram's servers, is a question that could not be resolved through a motion to dismiss because additional evidence was required. See *McGucken v. Newsweek LLC*, 19 Civ. 9617 (KPF), 2020 WL 6135733, at *1-3 (S.D.N.Y. Oct. 19, 2020) (affirming, in denying reconsideration, that "while Instagram's Terms of Use clearly granted Instagram a license to sublicense Plaintiff's publicly posted content, there was insufficiently clear language to support, in the context of a Rule 12(b)(6) motion, the existence of a sublicense between Instagram and Defendant."); *Sinclair v. Ziff Davis, LLC*, 18-CV-790 (KMW), 2020 WL 3450136, at *1-2 (S.D.N.Y. June 24, 2020) (adhering to its previous holding that, "by agreeing to Instagram's Terms of Use, Plaintiff authorized Instagram to grant API users, such as Mashable, a sublicense to embed her public Instagram content, as set forth in Instagram's Platform Policy" but granting reconsideration, and revising its previous decision, by holding "that the pleadings contain insufficient evidence to find that Instagram granted Mashable a sublicense to embed Plaintiff's Photograph on its website."); *McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 603-04 (S.D.N.Y. 2020) (denying Newsweek's motion to dismiss, holding that while Instagram's Terms of Use "unequivocally grant Instagram a license to sublicense Plaintiff's publicly posted content . . . , and the Privacy Policy clearly states that 'other Users may search for, see, use, or share any of your User Content that you make publicly available through' Instagram . . . , " the court could not dismiss plaintiff's claims; "Although Instagram's various terms and policies clearly foresee the possibility of entities such as Defendant using web embeds to share other users' content . . . , none of them expressly grants a sublicense to those who embed publicly posted content. Nor can the Court find, on the pleadings, evidence of a possible implied sublicense. . . . While the Court acknowledges that it may be possible to read Instagram's various terms and policies to grant a sublicense to embedders, the Court's role on a Rule 12(b)(6) motion is to 'draw all reasonable inferences in Plaintiff's favor.' ").

insulate a party from liability.¹³

9.03[3][A][ii] Case Law Analysis

The leading copyright case on links is *Perfect 10, Inc. v. Amazon.com, Inc.*,¹ in which the Ninth Circuit adopted the “server test” to evaluate whether a given online use violated plaintiff’s public display or distribution rights. Under this test, “a computer owner that stores an image as electronic information and serves that electronic information directly to the user . . . is displaying the electronic information in violation of a copyright holder’s exclusive display right. Conversely, the owner of a computer that does not store and

In *Ziff Davis*, Judge Wood previously had granted Ziff Davis’s motion, dismissing Sinclair’s copyright infringement claim, based on the finding that Mashable had used plaintiff’s photograph pursuant to a valid sublicense from Instagram. *See Sinclair v. Ziff Davis, LLC*, 454 F. Supp. 3d 342, 344-47 (S.D.N.Y. 2020). She explained:

The Terms of Use state that, by posting content to Instagram, the user “grant[s] to Instagram a non-exclusive, fully paid and royalty-free, transferable, sublicensable, worldwide license to the Content that you post on or through [Instagram], subject to [Instagram’s] Privacy Policy.” (Terms of Use, Rights § 1.) Pursuant to Instagram’s Privacy Policy (“Privacy Policy”), Instagram users designate their accounts as “private” or “public,” and can change these privacy settings whenever they wish. (Privacy Policy, Parties With Whom You May Choose to Share Your User Content § 1.). All content that users upload and designate as “public” is searchable by the public and subject to use by others via Instagram’s API. (*Id.* § 2.) The API enables its users to embed publicly-posted content in their websites. (Platform Policy, Preamble.). Thus, because Plaintiff uploaded the Photograph to Instagram and designated it as “public,” she agreed to allow Mashable, as Instagram’s sublicensee, to embed the Photograph in its website.

Id. at 345. On reconsideration, however, the court concluded that Instagram’s Platform Policy could be construed as granting Instagram API users the right to use the API to embed the public content of other Instagram users, but that was not the only interpretation to which it was susceptible (and accordingly construction of the license was not an issue that could be resolved on a motion to dismiss, which assumes as true the well pleaded facts in a plaintiff’s Complaint). *See Sinclair v. Ziff Davis, LLC*, 2020 WL 3450136, at *1.

¹³*See Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 596 (S.D.N.Y. 2018) (suggesting in *dicta* the potential availability of these defenses). Licenses and implied licenses are addressed in section 4.05[7]. The DMCA safe harbor for information location tools is addressed in section 4.12[7]. Fair use is analyzed in section 4.10[1]. *De minimis* infringement is addressed in section 4.08[1]. The *Sony* safe harbor is analyzed in sections 4.10[5] and 4.11[3]. Defenses to claims based on linking are addressed in summary form in sections 9.03[3][B] and 9.03[3][C].

[Section 9.03[3][A][ii]]

¹*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007).

serve the electronic information to a user is not displaying that information, even if such owner in-line links to or frames the electronic information.”² Applying this test, a link to content housed on a third party site would not result in a finding of direct liability, at least in the Ninth Circuit.

In *Perfect 10 v. Amazon.com*, the Ninth Circuit ruled that Google potentially could be held directly liable for photos stored on its own servers,³ but could not be held directly liable for links created to photos stored on third party websites. In the words of the court, “Google transmits or communicates only an address which directs a user’s browser to the location where a copy of the full-size image is displayed. Google does not communicate a display of the work itself.”⁴ Stated differently, “it is the website publisher’s computer, rather than Google’s computer, that stores and displays the infringing image.”⁵ Multiple other courts have likewise agreed that a link, *per se*, does not create a copy.⁶

²*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1159 (9th Cir. 2007).

³As discussed later in section 9.03[3][B], the court ultimately found the practice to be a fair use.

⁴*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1161 n.7 (9th Cir. 2007).

⁵*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1162 (9th Cir. 2007) (ultimately finding Google’s use to be a fair use).

⁶*See, e.g., Microsoft Corp. v. Softicle.com*, Civil Action No. 16–2762, 2017 WL 5517379, at *2 (D.N.J. Sept. 29, 2017) (dismissing a claim for direct copyright infringement based on a link to infringing material; “Providing a link to a website containing infringing material does not, as a matter of law, constitute direct copyright infringement.”); *Pearson Education, Inc. v. Ishayev*, 963 F. Supp. 2d 239, 251 (S.D.N.Y. 2013) (holding that the defendant was not liable for distributing infringing content by merely linking to it on a different site; “A hyperlink does not itself contain any substantive content; in that important sense, a hyperlink differs from a zip file. Because hyperlinks do not themselves contain the copyrighted or protected derivative works, forwarding them does not infringe on any of a copyright owner’s five exclusive rights under § 106.”); *MyPlayCity, Inc. v. Conduit Ltd.*, No. 10 Civ. 1615(CM), 2012 WL 1107648, at *12–14 (S.D.N.Y. Mar. 30, 2012) (granting summary judgment for the defendant on plaintiff’s claim for direct copyright infringement for distribution of plaintiff’s videogames by including a link on a toolbar it distributed following the termination of a license; “Because the actual transfer of a file between computers must occur, merely providing a ‘link’ to a site containing copyrighted material does not constitute direct infringement of a holder’s distribution right.”); *see also Flava Works, Inc. v. Gunter*, 689 F.3d 754, 760 (7th Cir. 2012) (holding that a video bookmarking site could not

The Seventh Circuit considered links, in the context of in-line links, in *Flava Works, Inc. v. Gunter*,⁷ in which the appellate panel in that case held that a claim for contributory copyright infringement could not be based on creating bookmark links to infringing videos. The Seventh Circuit further suggested in *dicta* in *Flava Works* that direct liability similarly could not be imposed.

While most forms of linking may not be actionable at all under the Ninth Circuit's server test, some district courts in other parts of the country have allowed claims for direct liability to proceed. Two of those cases pre-date *Perfect 10: Live Nation Motor Sports, Inc. v. Davis*,⁸ which involved a live transmission, and *Batesville Services, Inc. v. Funeral Depot, Inc.*,⁹ in which the court denied defendant's motion to dismiss a case where plaintiff had not simply linked to third party content, but linked to pages that he had allegedly helped create, to host content which previously had been on his own website until the copyright owner forced him to remove it.

In *Live Nation Motor Sports, Inc. v. Davis*,¹⁰ which pre-dates *Perfect 10*, Judge Sam Lindsay of the Northern District of Texas held that a link to a stream of a live webcast of motor races that was shown in real time constituted a public performance or display because those terms encompass "each step in the process by which a protected work wends its way

be held liable for contributory copyright infringement; "The direct infringers in this case are the uploaders; myVidster is neither a direct nor a contributory infringer—at least of Flava's exclusive right to copy and distribute copies of its copyrighted videos."); *Batesville Services, Inc. v. Funeral Depot, Inc.*, No. 1:02-CV-01011-DFH-TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004) (explaining that hyperlinking "does not itself involve a violation of the Copyright Act (whatever it may do for other claims) since no copying is involved."); *Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1202 n.12 (N.D. Cal. 2004) (stating in *dicta* that "[a]lthough hyperlinking *per se* does not constitute direct copyright infringement because there is no copying . . . in some instances there may be a tenable claim of contributory infringement or vicarious liability.").

⁷*Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012).

⁸*Live Nation Motor Sports, Inc. v. Davis*, Civil Action No. 3:06-CV-276-L, 81 U.S.P.Q.2d 1826 (N.D. Tex. Jan. 9, 2007).

⁹*Batesville Services, Inc. v. Funeral Depot, Inc.*, No. 1:02-CV-01011-DFH-TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004).

¹⁰*Live Nation Motor Sports, Inc. v. Davis*, Civil Action No. 3:06-CV-276-L, 81 U.S.P.Q.2d 1826 (N.D. Tex. Jan. 9, 2007).

to the audience.”¹¹ This outcome potentially may be justified because the definition of *fixation* for public performances is broader than for other uses. The Copyright Act provides that a “work consisting of sounds, images, or both, that are being transmitted, is ‘fixed’ for purposes of this title if a fixation of the work is being made simultaneously with its transmission.”¹² A work otherwise is only deemed fixed if it is “sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.” Under *MAI Systems Corp. v. Peak Computer, Inc.*,¹³ this means that a work is fixed when perceived on a user’s computer (and under *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*,¹⁴ depending on the nature of the work, it may or may not be fixed for a sufficient duration to be deemed a *copy* under the Copyright Act). For a live performance or other streamed transmission,¹⁵ however, the work is deemed *fixed* at the moment of transmission, arguably meaning that the link itself could be deemed to create the copy.¹⁶

¹¹*Live Nation Motor Sports, Inc. v. Davis*, Civil Action No. 3:06-CV-276-L, 81 U.S.P.Q.2d 1826 (N.D. Tex. Jan. 9, 2007), citing *National Football League v. PrimeTime 24 Joint Venture*, 211 F.3d 10, 12 (2d Cir.2000), cert. denied, 532 U.S. 941 (2001); see also *United States v. American Society of Composers, Authors & Publishers*, 627 F.3d 64, 74-75 (2d Cir. 2010), cert. denied, 565 U.S. 929 (2011) (explaining *NFL v. PrimeTime*; “In holding the transmission in *Cartoon Network* not to be a public performance, we distinguished *NFL* on the basis that in that case the final act in the sequence of transmissions was a public performance.”).

¹²17 U.S.C.A. § 101.

¹³*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), cert. dismissed, 510 U.S. 1033 (1994); *supra* § 9.01.

¹⁴*Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008), cert. denied, 557 U.S. 946 (2009); *supra* § 9.01.

¹⁵For example, in *Warner Bros. Entertainment Inc. v. WTV Systems, Inc.*, 824 F. Supp. 2d 1003 (C.D. Cal. 2011), the court preliminarily enjoined operation of a DVD rental service that allowed users to stream videos over the Internet. While not a linking case, *WTV Systems* illustrates that when a website streams material to users it may be found to involve a public performance. See *id.*; see also *Aereo Broadcasting Cos. v. Aereo, Inc.*, 573 U.S. 431 (2014) (holding that Aereo’s Internet-based streaming service involved public performances); see generally *supra* § 4.04[3] (analyzing *Aereo* and the right of public performance).

¹⁶The Second Circuit, in *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 134-39 (2d Cir. 2008), cert. denied, 557 U.S. 946 (2009), also analyzed whether Cablevision could be held liable for a public performance, in a different portion of the opinion. The appellate panel held that

In the other case pre-dating *Perfect 10, Batesville Services, Inc. v. Funeral Depot, Inc.*,¹⁷ a court in Indiana denied defendant's motion to dismiss, allowing plaintiff to proceed with claims for both direct and contributory copyright infringement arising out of links. In that case, the defendant not only created links to unauthorized photographs of plaintiff's products, but it had designed, created and paid for the pages that it linked to, after having been warned to stop displaying the pictures itself on its own website. The court acknowledged that hyperlinking "does not itself involve a violation of the Copyright Act (whatever it may do for other claims) since no copying is involved." It nonetheless found the facts "unusual enough to take th[e] case out of the general principle that linking does not amount to copying." *Batesville* therefore may be understood as a case where the defendant not only created a link but also created at least some of the infringing linked content. Alternatively, it perhaps should be seen as a case where a court was reluctant

because the RS-DVR system, as designed, only made transmissions to a single subscriber using a single copy made by that subscriber, the universe of people capable of receiving an RS-DVR transmission was the single subscriber whose self-made copy was used to create that transmission, and therefore the transmission did not constitute a public performance. Hence, in contrast to *Live Nation Motor Sports, Inc. v. Davis*, Civil Action No. 3:06-CV-276-L, 81 U.S.P.Q.2d 1826 (N.D. Tex. Jan. 9, 2007), if a link merely allowed a single individual to access a single copy of an audiovisual work stored by that user in the cloud or copied by that user to a remote DVR, under *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 134-39 (2d Cir. 2008), *cert. denied*, 557 U.S. 946 (2009), the subsequent performance might not be deemed actionable as a *public performance* in the Second Circuit (although a link that allowed multiple users to simultaneously or even separately access the same copy likely would be found a public performance), to the extent this aspect of *Cartoon Network* remains valid after *American Broadcasting Cos. v. Aereo, Inc.*, 573 U.S. 431 (2014). In *Aereo*, the Supreme Court held that a streaming service that allowed individuals to separately access individual transmissions of over-the-air television broadcasts using remote antennas constituted a public performance because of the service's similarity to a CATV cable service, which Congress sought to protect by the 1976 Copyright Act. The Court also rejected the notion that a public performance must be seen or heard by all recipients at the same time to be deemed a public performance. The majority did not expressly overrule *Cartoon Network*, however, and made clear that its limited holding was not necessarily intended to apply generally to cloud storage or in situations where the material accessed was licensed. *Aereo* and its longer term implications are analyzed in section 4.04[3] in chapter 4.

¹⁷*Batesville Services, Inc. v. Funeral Depot, Inc.*, No. 1:02-CV-01011-DFH-TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004).

to dismiss plaintiff's claim at the outset of the case.

More recently, some district court opinions have held that plaintiffs could state a claim for direct infringement based on embedded links to photos posted on Twitter¹⁸ or Instagram and Facebook,¹⁹ and a photo displayed using frames.²⁰

In *The Leader's Institute, LLC v. Jackson*,²¹ the court, in denying plaintiff's motion for summary judgment on defendant's counterclaim for copyright infringement, held that the plaintiff publicly displayed content from the defendant's website by framing it on its own website. The parties in that case were competitors in the team building industry. In accepting the argument that TLI committed copyright infringement by framing Magnovo's copyrighted content, Judge Jane Boyle of the Northern District of Texas, held, in an unreported opinion, that *Perfect 10* was factually distinguishable because, in that case, Google did not actually display infringing images but instead provided links for users to access sites that displayed infringing images.²² The court explained:

Although the infringing content appeared under a Google banner, the user was essentially navigating to an infringing website to view Perfect 10's photos. The same is not true of users who visited the accused TLI websites. Upon visiting one of the TLI sites, a user would necessarily see Magnovo's content. Unlike Google, TLI did not merely provide a link by which users could access Magnovo content but instead displayed Magnovo's content as if it were its own.²³

In other words, she distinguished ordinary links from framed links that (like in-line and embedded links) display the image in another location, rather than merely providing

¹⁸See *Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585 (S.D.N.Y. 2018).

¹⁹See *Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510 (S.D.N.Y. 2021).

²⁰See *The Leader's Institute, LLC v. Jackson*, Civil Action No. 3:14-CV-3572-B, 2017 WL 5629514, at *10 (N.D. Tex. Nov. 22, 2017) (denying plaintiff's motion for summary judgment on defendant's counterclaim for copyright infringement, holding that plaintiff publicly displayed copyrighted content from defendant's website by framing it on its own website; distinguishing framing from ordinary linking).

²¹*The Leader's Institute, LLC v. Jackson*, Civil Action No. 3:14-CV-3572-B, 2017 WL 5629514 (N.D. Tex. Nov. 22, 2017).

²²*The Leader's Institute, LLC v. Jackson*, Civil Action No. 3:14-CV-3572-B, 2017 WL 5629514, at *11 (N.D. Tex. Nov. 22, 2017).

²³*The Leader's Institute, LLC v. Jackson*, Civil Action No. 3:14-CV-3572-B, 2017 WL 5629514, at *11 (N.D. Tex. Nov. 22, 2017).

a connection to the source location.

Judge Boyle also rejected plaintiffs' argument that they could not have committed copyright infringement because they had not made any copies of Magnovo's work. She opined that, "to the extent *Perfect 10* makes actual possession of a copy a necessary condition to violating a copyright owner's exclusive right to display her copyrighted works, the Court respectfully disagrees with the Ninth Circuit."²⁴

In *Goldman v. Breitbart News Network, LLC*,²⁵ the court granted partial summary judgment to the owner of the copyright to a photograph of NFL quarterback Tom Brady, which had been embedded in articles published by the defendants from Twitter, where the photo had been posted. Southern District of New York Judge Katherine Forrest conceded that "none of the defendant websites copied and saved the Photo onto their own servers. Rather, they made the photo visible in their articles . . ." through embedded links.²⁶ She nevertheless held that the embedded links violated plaintiff's public display right in the photo based on the broad meaning given to *display* in the legislative history of the Copyright Act.²⁷ Among other things, the court concluded that "possession of an image" was not necessary, under the Copyright Act, to display it.²⁸

In so ruling, Judge Forrest expressly rejected the Ninth Circuit's server test,²⁹ explaining that "[t]he plain language of the Copyright Act, the legislative history undergirding its enactment, and subsequent Supreme Court jurisprudence [*Aereo*] provide no basis for a rule that allows the physical location or possession of an image to determine who may or may not have 'displayed' a work within the meaning of the

²⁴*The Leader's Institute, LLC v. Jackson*, Civil Action No. 3:14-CV-3572-B, 2017 WL 5629514, at *11 (N.D. Tex. Nov. 22, 2017).

²⁵*Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585 (S.D.N.Y. 2018).

²⁶*Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 587 (S.D.N.Y. 2018).

²⁷*Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 588-89 (S.D.N.Y. 2018).

²⁸*See Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 593 (S.D.N.Y. 2018).

²⁹*Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 590-93 (S.D.N.Y. 2018). Judge Forrest argued that the Ninth Circuit had conflated the display right in section 106(5) with the reproduction right in section 106(1). *See id.* at 595.

Copyright Act.”³⁰

In the alternative, the court held that if the Second Circuit were to adopt the server test, it would be inapplicable in this case because *Perfect 10* involved a search engine where users clicked on a link before an image was displayed. By contrast, Judge Forrest considered it significant that in *Breitbart* the defendants created the link that was made visible to users who accessed the articles in which the photo was visible without requesting it.³¹ This distinction—between whether an image is directly viewable or not—doesn’t get at the underlying legal issue of whether a link creates a *copy*.

Despite her holding on the issue of public display, Judge Forrest conceded that several defenses could apply. She explained that “there are genuine questions about whether plaintiff effectively released his image into the public domain when he posted it to his Snapchat account. Indeed, in many cases there are likely to be factual questions as to licensing and authorization. There is also a very serious and strong fair use defense, a defense under the Digital Millennium Copyright Act, and limitations on damages from innocent infringement.”³² Indeed, subsequent cases in the Southern and Eastern Districts of New York have dismissed claims or

³⁰*Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 593 (S.D.N.Y. 2018).

³¹*See Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 595-96 (S.D.N.Y. 2018). In *Free Speech Systems, LLC v. Menzel*, 390 F. Supp. 3d 1162, 1172 (N.D. Cal. 2019), the court, in denying the motion of the owner and operator of InfoWars to dismiss counterclaims brought against it, cited *Goldman v. Breitbart* and *The Leader’s Institute v. Jackson* for the proposition that the server test might be inapplicable to a case where in-line links to defendant’s copyrighted photographs were created by InfoWars, where the defendant could not cite to a Ninth Circuit case applying the server test “outside the search engine context.” This opinion, which involved only a cursory analysis of the issue, should be best understood in the context of a ruling on a motion to dismiss where InfoWars had sought unsuccessfully to have the court take judicial notice of an array of facts. Whether a work is displayed by creating a link to a third party website is not a function of whether the party creating the link is a search engine or a controversial political conspiracy news site. What constitutes a *display* is a matter of copyright law, not a function of a given business model.

³²*See Goldman v. Breitbart News Network, LLC*, 302 F. Supp. 3d 585, 596 (S.D.N.Y. 2018). Licenses and implied licenses are addressed in section 4.05[7]. The DMCA safe harbor for information location tools is addressed in section 4.12[7]. Fair use is analyzed in section 4.10[1]. Other potential defenses to a claim for copyright infringement based on linking

granted judgment on the pleadings in cases involving embedded links to Instagram posts, finding the practice a fair use.³³ Likewise, licensing questions have been analyzed in district court opinions that have held that Instagram receives an express license from users for images they upload to its platform to allow other users to embed those images (although whether Instagram, in turn, granted its users a license to embed those images when they use Instagram's API (application programming interface) could not be determined at the outset of a case on a motion to dismiss because additional evidence was required).³⁴

include *de minimis* infringement and the *Sony* safe harbor. See *infra* §§ 9.03[3][B], 9.03[3][C].

³³See *Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 6393010 (E.D.N.Y. Nov. 2, 2020) (dismissing, as fair use, the copyright infringement claim of a photographer against a sports news publisher, which had included an embedded link to an Instagram post by professional tennis player Caroline Wozniacki, announcing her retirements (which included a low-resolution, cropped version of a photograph taken by the plaintiff), in an article it published about Wozniacki's career, which also quoted the text of the Instagram post); *Walsh v. Townsquare Media, Inc.*, 464 F. Supp. 3d 570 (S.D.N.Y. 2020) (entering judgment on the pleadings, based on fair use, in a Paparazzi photographer's copyright infringement claim, brought against the publisher of *XXL* magazine, which had embedded a link to an Instagram post by hip hop artist Cardi B, which included a photograph taken by plaintiff of Cardi B at a Tom Ford fashion show, in an article entitled *Cardi B Partners with Tom Ford for New Lipstick Shade*, which was focused on the event and referenced the Cardi B Instagram post which featured the photograph); see also *Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 7625222 (E.D.N.Y. Dec. 22, 2020) (denying reconsideration). Cf. *Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *5-7 (S.D.N.Y. 2021) (denying defendant's motion to dismiss plaintiff's copyright infringement claim, premised on Sinclair's placement of an embedded link to plaintiff's video of a starving polar bear in an article describing how the video "went 'viral,'" because Sinclair's fair use defense could not be resolved on a motion to dismiss based solely on the allegations of the complaint, despite finding that the use was transformative); *McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 604-09 (S.D.N.Y. 2020) (holding, in an opinion decided before *Boesen* and *Walsh*, that, on the facts of that case, fair use could not be established as a matter of law at the pleadings stage, in a case where plaintiff posted a photograph of an ephemeral lake on March 13, 2019, and the very next day Newsweek allegedly published an article about the ephemeral lake, embedding plaintiff's Instagram post about the lake, as part of the article).

³⁴See *McGucken v. Newsweek LLC*, 19 Civ. 9617 (KPF), 2020 WL 6135733, at *1-3 (S.D.N.Y. Oct. 19, 2020) (affirming, in denying reconsideration, that "while Instagram's Terms of Use clearly granted Instagram a

In *Nicklen v. Sinclair Broadcast Group, Inc.*,³⁵ which like *Breitbart* was brought in the Southern District of New York, Judge Jed Rakoff denied Sinclair’s motion to dismiss plaintiff’s copyright infringement claim, holding that plaintiff stated a claim that Sinclair’s placement of an embedded link to plaintiff’s video of a starving polar bear, in an article describing how the video “went ‘viral,’” constituted an unauthorized public display, and that Sinclair’s fair use defense could not be resolved on a motion to dismiss. Judge Rakoff acknowledged that Sinclair’s use may well be a fair use, noting that the original purpose and meaning of the video was likely to highlight the cruel effects of climate change, whereas Sinclair’s article focused on the video’s popularity, which thus was transformative and weighed in favor of a finding of fair use.³⁶ He concluded, however, that fair use could not be resolved with finality in that case on a motion to dismiss, noting, for example, that a news article about a viral video was unlikely to threaten the market for the genu-

license to sublicense Plaintiff’s publicly posted content, there was insufficiently clear language to support, in the context of a Rule 12(b)(6) motion, the existence of a sublicense between Instagram and Defendant.”); *Sinclair v. Ziff Davis, LLC*, 18-CV-790 (KMW), 2020 WL 3450136, at *1-2 (S.D.N.Y. June 24, 2020) (adhering to its previous holding that, “by agreeing to Instagram’s Terms of Use, Plaintiff authorized Instagram to grant API users, such as Mashable, a sublicense to embed her public Instagram content, as set forth in Instagram’s Platform Policy” but granting reconsideration, and revising its previous decision, by holding “that the pleadings contain insufficient evidence to find that Instagram granted Mashable a sublicense to embed Plaintiff’s Photograph on its website.”); *McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 603-04 (S.D.N.Y. 2020) (denying Newsweek’s motion to dismiss, holding that while Instagram’s Terms of Use “unequivocally grant Instagram a license to sublicense Plaintiff’s publicly posted content . . . , and the Privacy Policy clearly states that ‘other Users may search for, see, use, or share any of your User Content that you make publicly available through’ Instagram . . . ,” the court could not dismiss plaintiff’s claims; “Although Instagram’s various terms and policies clearly foresee the possibility of entities such as Defendant using web embeds to share other users’ content . . . , none of them expressly grants a sublicense to those who embed publicly posted content. Nor can the Court find, on the pleadings, evidence of a possible implied sublicense. . . . While the Court acknowledges that it may be possible to read Instagram’s various terms and policies to grant a sublicense to embedders, the Court’s role on a Rule 12(b)(6) motion is to ‘draw all reasonable inferences in Plaintiff’s favor.’”).

³⁵*Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510 (S.D.N.Y. 2021).

³⁶*See Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *5 (S.D.N.Y. 2021).

ine work, but could do so if Sinclair’s use was widespread.³⁷

In ruling on whether embedding a link to an image in social media constitutes a public display, Judge Rakoff, like Judge Forrest, criticized the Ninth Circuit’s server test, writing that “[t]he Ninth Circuit’s approach, under which no display is possible unless the alleged infringer has also stored a copy of the work on the infringer’s computer, makes the display right merely a subset of the reproduction right.”³⁸

Judge Rakoff also argued that the server test distinguishes between “showing a copy possessed by the infringer and showing a copy possessed by someone else[.]”³⁹ which the Copyright Act does not. But this analogy is inapt because the Copyright Act in fact makes numerous distinctions between infringement and permitted use in considering identical copies, depending on whether the copyrighted work is licensed or subject to the First Sale doctrine, for example.⁴⁰ In addition, in digital media, a single copy may amount to a reproduction, distribution and/or public display—or none of the above—depending on how it has been placed online, and by whom, and the distribution system used.⁴¹ Judge Rakoff’s underlying assumption about the nature of copyrighted works in digital media, in holding that embedding a link constitutes a public display, is thus flawed.

Judge Rakoff relied on a dictionary definition of *display*,

³⁷See *Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *6-7 (S.D.N.Y. 2021) (noting that while “the pleadings alone could establish fair use in an appropriate case . . . this is not the rare case in which the Court can make a fair use determination simply by comparing the two works, such that ‘discovery would not provide additional relevant information.’”) (quoting *Arrow Productions, Ltd. v. Weinstein Co.*, 44 F. Supp. 3d. 359, 368 (S.D.N.Y. 2014)).

³⁸*Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *4 (S.D.N.Y. 2021), citing Jane C. Ginsburg & Luke Ali Budiardjo, *Embedding Content or Interring Copyright: Does the Internet Need the “Server Rule”?*, 32 Colum. J. L. & Arts 417, 430 (2019) (arguing that the server test “convert[s] the display right into an atrophied appendage of the reproduction right” and thereby “ignores Congress’s endeavor to ensure that the full ‘bundle’ of exclusive rights will address evolving modes of exploitation of works”).

³⁹*Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *4 (S.D.N.Y. 2021).

⁴⁰See generally *infra* § 16.02[1] (distinguishing a true license from a transaction subject to the First Sale doctrine).

⁴¹See generally *supra* § 4.04[3] (analyzing overlapping rights when copyrighted works are uploaded, downloaded or placed online).

rather than exclusively on Copyright Act definitions and case law, to conclude that “under the plain meaning of the Copyright Act, a defendant violates an author’s exclusive right to display an audiovisual work publicly when the defendant without authorization causes a copy of the work, or individual images of the work, to be seen — whether directly or by means of any device or process known in 1976 or developed thereafter.”⁴²

The focus in *Breitbart* and *Sinclair* on whether a photograph is displayed because it is seen blurs the distinction over whether the image is linked from another location or actually copied by the party that creates an embedded link—in other words whether there is causation. A public display occurs on the server where it is *displayed*, not everywhere it is *seen*. Indeed, were the rule otherwise, a single act of display on a website server could result in almost limitless liability.

One of the problems with judge-made tests like the “server test” is that the simplicity it affords may obscure the underlying legal issue, which in the case of links (including embedded links, in-line links and frames) is the question of *where* has a copy been made (*i.e.*, fixed in a tangible medium of expression) and, if that copy is actionable, who is legally responsible. Except in cases involving a public performance where the copy is made simultaneous with its transmission, this is the proper question to ask: has a *copy* been made, within the meaning of the Copyright Act’s fixation requirement (consistent with cases such as *MAI v. Peak*) and, if so, is there a legal basis to impose either direct or secondary liability for the creation of that copy. *Copies* are defined under the Copyright Act as “material objects, other than phonorecords, [1] in which a work is fixed by any method now known or later developed, *and* [2] from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.”⁴³ *Leaders Institute v. Jackson*, *Goldman v. Breitbart* and *Nicklen v. Sinclair* effectively focus on the second prong of this definition—perception (or display)—but overlook the requirement for fixation. When an in-line or embedded link is created by inserting a simple line of code to instruct a browser to view

⁴²*Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *3 (S.D.N.Y. 2021).

⁴³17 U.S.C.A. § 101 (emphasis added).

an image located elsewhere, that image is not *fixed* by the act of linking. The fixed copies exist on the host server where the link directs a browser to go, and then on a user's screen RAM.

Likewise, the public display of the photo is by the party that posted it, not a party who links to it. To *display* a work means "to show a copy of it, either directly or by means of a film, slide, television image, or any other device or process or, in the case of a motion picture or other audiovisual work, to show individual images nonsequentially."⁴⁴ The party that shows the image is the one that hosts it. A link may point a user to a location where the image is displayed, but it does not separately display the image. The displayed image exists only on the server to which the link directs a browser. Indeed, if the owner of the location where the image is displayed removes it or changes the address, the image would no longer be accessible by the embedded or in-line link (or in a frame). It is the place where the image is stored, where the image is displayed.

Because a link merely is an instruction to a browser to go from one location to another, aside from recent district court cases involving the public display of photographs accessed via an in-line or embedded link, copyright liability for creating a link typically would have to arise, if at all, based on claims for secondary liability, such as contributory infringement or potentially vicarious liability or inducement, where the underlying act of direct infringement⁴⁵ is the unauthorized cached copy made on a user's computer⁴⁶ when he or she accesses the link. As explained in *dicta* by one court, "[a]lthough hyperlinking *per se* does not constitute direct copyright infringement because there is no copying . . . in some instances there may be a tenable claim of contributory infringement or vicarious liability."⁴⁷

In *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*⁴⁸—the first U.S. case in which a court enjoined a defendant from establishing links to another website under

⁴⁴17 U.S.C.A. § 101.

⁴⁵To state a claim for secondary liability, there must be an underlying act of direct infringement by a third party. See *supra* § 4.11.

⁴⁶See *supra* § 9.02.

⁴⁷*Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1202 n.12 (N.D. Cal. 2004) (*dicta*; citations omitted).

⁴⁸*Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F.

copyright law—Judge Tena Campbell of the District of Utah entered an injunction prohibiting linking where defendants encouraged visitors to their website—via links—to access infringing content located on other sites. The case involved more than mere linking, however. Defendants—after being ordered to remove unauthorized copies of plaintiff’s protected “Church Handbook of Instructions” from their website—created links to three other locations where infringing copies of the book could be accessed. They also posted messages on their site encouraging visitors to browse the linked locations, print copies of the handbook, and email them to third-parties. Although the court concluded that plaintiffs had not shown that defendants contributed to the third-party acts of infringement by the owners of the linked sites, it ruled that defendants actively encouraged individual users to infringe plaintiff’s copyright by browsing the infringing sites (causing unauthorized temporary copies to be cached in users’ screen RAM) and printing or re-posting unauthorized copies on other websites.

Ultimately, it was the acts of encouragement by defendants, who already had been ordered to cease their acts of direct infringement—not the mere fact of linking—that was determinative in the *Utah Lighthouse Ministry* case. Indeed, the court likely would have entered the same order if the defendants had merely provided the URLs to visitors (rather than established links).

Similarly, in *Arista Records, Inc. v. MP3Board, Inc.*,⁴⁹ the court denied the defendant’s motion for summary judgment, finding that a reasonable trier of fact could determine that MP3Board “engaged in an overall course of conduct which materially contributed” to copyright infringement by offering a search engine that aggregated and organized links to third party sites that included audio files, solicited third party links to such sites, offered a tutorial for new users that provided instructions on how to locate and download audio files and used one of plaintiffs’ protected works as an example in the tutorial. The site also included a message board where users could post and answer questions. In response to user questions, MP3Board personnel personally searched for links to requested copyrighted songs, solicited

Supp. 2d 1290 (D. Utah 1999).

⁴⁹*Arista Records, Inc. v. Mp3Board, Inc.*, No. 00 CIV. 4660 (SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002).

users to provide the work directly when links could not be found, and obtained and posted passwords to enable users to access certain music files free of charge. According to the court, “[n]ot only could a jury find that MP3Board provided the facilities to promote infringing activity, but also that it directly assisted users in locating and downloading infringing files.” Thus, as in *Utah Lighthouse*, it was active encouragement, rather than links *per se*, that justified the court’s order.

Indeed, in *Perfect 10, Inc. v. Amazon.com, Inc.*⁵⁰ itself, although the Ninth Circuit had ruled that Google could not be held directly liable for creating links to photographs on third party sites, the panel remanded for further consideration the issue of whether Google and Amazon.com could be held contributorily liable for providing links to infringing websites as part of the operation of their search engines. The court held that “a computer system operator can be held contributorily liable if it ‘has *actual* knowledge that *specific* infringing material is available using its system,’ . . . and can ‘take simple measures to prevent further damage’ to copyrighted works, . . . yet continues to provide access to infringing works.”⁵¹ While the Ninth Circuit panel in *Perfect 10 v. Amazon.com* cautioned that liability could not automatically be established (and indeed, based on the test articulated, it seemed unlikely that it would be, on remand, in *Perfect 10 v. Amazon.com*), the court made clear that contributory liability potentially could be imposed for creating links to third party content, at least where that content was infringing.⁵²

This theory of imposing secondary liability for links was perhaps first articulated twelve years earlier in *Adobe Systems, Inc. v. Community Connexion, Inc.*,⁵³ *Adobe Systems, Inc. v. Geocities, Inc.*,⁵⁴ and *Adobe Systems, Inc. v. Tripod*,

⁵⁰*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007).

⁵¹*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1172 (9th Cir. 2007) (emphasis in original; citations omitted).

⁵²Although ultimately never decided on the merits, four years later, the Ninth Circuit affirmed the district court’s denial of Perfect 10’s motion for a preliminary injunction where Perfect 10 could not establish that Google’s search engine operations would cause it irreparable harm. See *Perfect 10, Inc. v. Google, Inc.*, 653 F.3d 976 (9th Cir. 2011).

⁵³*Adobe Systems, Inc. v. Community Connexion, Inc.*, Case No. C-96 20833 SW EAI (N.D. Cal. filed Oct. 7, 1996).

⁵⁴*Adobe Systems, Inc. v. Geocities, Inc.*, Case No. 96-7035 TJH (ANx)

*Inc.*⁵⁵ In those cases, plaintiffs, software publishers Adobe Systems, Inc., Claris Corp. and Travelling Software, Inc., brought suit against ISPs that allegedly established links to websites where visitors could obtain infringing copies of plaintiffs' software or cracker tools. Plaintiffs alleged that the ISPs were notified of their customers' alleged acts, but continued to maintain the links, facilitating third-party acts of infringement. In addition to alleging contributory copyright infringement by the ISPs for maintaining the links even after having received notice, plaintiffs sued the ISPs' individual owners for vicarious copyright infringement⁵⁶ on the theory that (1) they had the right and ability to control the conduct of the direct infringer by establishing (or disabling) the links and (2) they benefited financially from the third-party acts of copyright infringement.⁵⁷

These suits, which ultimately settled, were premised on the theory that liability could be imposed for facilitating infringement by creating links to sites that provided cracker tools. Whether contributory liability could be found (and, in turn, vicarious liability on the part of the owners of the sites) for establishing links to cracker tools or infringing content would have depended in part on the factual question of whether the link *materially* contributed to the underlying infringing conduct (such as—for example—if the infringing sites were not indexed and therefore were otherwise difficult to locate), or induced it (by, for example, providing detailed information in addition to the links), or merely facilitated access to locations that could just as easily have been found by the direct infringer with a search engine and a few extra clicks of a mouse.

Although a *prima facie* case for imposing third-party liability may be made (under appropriate circumstances) for knowingly⁵⁸ creating direct links to infringing content or tools that facilitate infringement, not all links should be

(C.D. Cal. filed Oct. 7, 1996).

⁵⁵*Adobe Systems, Inc. v. Tripod, Inc.*, Case No. 96-30189-MAP (D. Mass. filed Oct. 8, 1996).

⁵⁶*See, e.g., Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996); *see generally, supra* § 4.11.

⁵⁷A copy of one of the Adobe Systems, Inc. complaints is included in Appendix 1 at the end of this chapter. These lawsuits are discussed in greater detail in section 4.11[10].

⁵⁸The standard for imposing contributory liability presupposes knowledge, although specific knowledge about particular acts of infringement

viewed the same way. Links generated by a neutral search engine are different from links on a page dedicated to finding hacker tools or infringing media.

While it had generally been assumed among Internet lawyers prior to 2008 that claims for secondary liability for linking theoretically could be stated based on contributory or vicarious liability (or possibly inducement), the question of whether there is an underlying act of direct infringement is more complicated after *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*⁵⁹

To state a claim for secondary liability, there must be an underlying act of infringement by a third party. Absent an act of direct infringement, there is no basis for holding third-parties contributorily or vicariously liable or liable for inducement.⁶⁰ Unless a cached copy is retained for more than merely a transitory duration, however, the copy created in a

need not be proven. *See, e.g., A & M Records, Inc. v. Abdallah*, 948 F. Supp. 1449 (C.D. Cal. 1996) (holding defendant liable for contributory infringement for selling time-loaded blank cassette tapes for making counterfeit tape recordings, even though the defendant may not have had specific knowledge about any particular infringing recording made); *see generally supra* § 4.11. Imputed, not actual knowledge, may be sufficient in appropriate cases where the surrounding circumstances would justify it (such as where all of the links on a given page direct visitors to sites dedicated to cracking anti-piracy devices).

A greater showing of knowledge, however, may be required in cases where contributory liability is sought to be imposed based solely on creating a link where, for example, the contributory act (establishing a link) is several steps removed from the act of direct infringement or the connection between the contributory and underlying acts otherwise is more attenuated. Absent knowledge or intent, the mere act of establishing a link generally would be viewed as a permissible and legitimate, noninfringing use of Internet resources.

⁵⁹*Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008), *cert. denied*, 557 U.S. 946 (2009); *see generally supra* § 9.01 (discussing the opinion and its significance in caching, linking and framing cases).

⁶⁰*See, e.g., Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 (2005) (inducement); *Subafilms, Ltd. v. MGM-Pathe Communications Co.*, 24 F.3d 1088, 1092 (9th Cir.) (*en banc*), *cert. denied*, U.S. 1001 (1994); *Arista Records, Inc. v. MP3Board, Inc.*, No. 00 CIV. 4660 (SHS), 2002 WL 1997918 (S.D.N.Y. Aug. 29, 2002); *see generally supra* § 4.11[1].

In *Arista Records, Inc. v. MP3Board, Inc.*, the court acknowledged that although the plaintiffs had presented sufficient evidence to give rise to a “strong statistical inference” that MP3Board users downloaded copyrighted music, plaintiffs had failed to eliminate all genuine issues of fact, as required to obtain summary judgment.

user's screen RAM in fact would not be deemed actionable under *Cartoon Network*, at least in the Second Circuit.⁶¹ Thus, while claims such as the ones asserted in *Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*⁶² could still be raised in circuits that follow *MAI Systems Corp. v. Peak Computer, Inc.*⁶³ but not *Cartoon Network*, in a court applying *Cartoon Network*, a plaintiff would need to show that the copy created in screen RAM was fixed for more than merely a transitory duration or that, as in *MP3Board*, copies were actually downloaded (or otherwise copied in a more traditional sense), rather than merely viewed on a user's screen. Presumably, streaming material to the public also would qualify as creating an underlying infringing copy. As a result of *Cartoon Network*, however, the infringement analysis has become more complex (and jurisdiction-specific), at least in cases involving reproduction or distribution.

The premise that a user's act of accessing material via a link constitutes direct infringement also potentially may be challenged in some cases based on the absence of volitional conduct by the user. Even assuming that merely accessing a website is deemed to cause a "copy" of the site to be created in the user's temporary screen memory under *MAI*, the user may not have undertaken volitional conduct sufficient to rise to a level that would justify the imposition of direct copy-right liability.⁶⁴ While some users may volitionally access a link to obtain infringing material, others may not realize

⁶¹See *supra* § 9.02.

⁶²*Intellectual Reserve, Inc. v. Utah Lighthouse Ministry, Inc.*, 75 F. Supp. 2d 1290 (D. Utah 1999).

⁶³*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994); see generally *supra* § 9.01 (explaining the significance of MAI and its impact on caching, linking and framing).

⁶⁴See *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1370 (N.D. Cal. 1995) (Usenet postings; in order to find direct liability, "there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party."); see also, e.g., *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 131 (2d Cir. 2008) (holding that a cable service provider could not be held directly liable for its provision of a DVR service because "the operator . . . , the person who actually presses the button to make the recording, supplies the necessary element of volition, not the person who manufactures, maintains, or, if distinct from the operator, owns the machine."), *cert. denied*, 557 U.S. 946 (2009); *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544 (4th Cir. 2004) (holding an ISP not liable for direct infringement where it was "simply the owner and

manager of a system used by others who [we]re violating [plaintiff's] copyrights and [wa]s not an actual duplicator itself"); *BWP Media USA, Inc. v. T&S Software Associates, Inc.*, 852 F.3d 436, 438-44 (5th Cir.) (affirming summary judgment for T&S Software Associates, an internet service provider, holding that it was not directly liable for hosting an internet forum on which third-party users posted images that allegedly infringed copyrights owned by plaintiffs), *cert. denied*, 138 S. Ct. 236 (2017); *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 666-67 (9th Cir. 2017) (affirming dismissal and summary judgment for defendants on plaintiff's direct infringement claims brought against ISPs that provided access to the USENET and a software program to be able to view USENET content, which, among many other things, plaintiffs claimed included infringing copies of its photos); *Fox Broadcasting Co. v. Dish Network LLC*, 747 F.3d 1060, 1066-68 (9th Cir. 2014) (following *Cartoon Network* in holding that a cable company that provided technology to its subscribers that they could use to make copies was not likely to be held directly liable because Dish itself did not make the copies; direct liability requires a showing of "copying by the defendant"); *Parker v. Google, Inc.*, 422 F. Supp. 2d 492, 497 (E.D. Pa. 2006) ("Google's automatic archiving of USENET postings and excerpting of websites in its results to users' search queries do not include the necessary volitional element to constitute direct copyright infringement."), *aff'd*, 242 F. App'x 833 (3d Cir. 2007), *cert. denied*, 552 U.S. 1156 (2008); *Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1115 (D. Nev. 2006) (holding Google not liable for caching plaintiff's website articles as part of its automatic caching of the Internet, where the plaintiff had indicated in the metatags of his website that he wanted to be crawled by Google; "Google is passive in this process Without the user's request the copy would not be created and sent to the user, and the alleged infringement at issue in this case would not occur. The automated, non-volitional conduct by Google in response to a user's request does not constitute direct infringement"); *Ellison v. Robertson*, 189 F. Supp. 2d 1051, 1057 (C.D. Cal. 2002) (following *Netcom* in holding that "AOL's role in the infringement as a passive provider of USENET access to AOL users cannot support direct copyright infringement liability" in a case involving an eBook posted to a newsgroup), *aff'd in part and rev'd in part*, 357 F.3d 1072 (9th Cir. 2004); *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1168 (C.D. Cal. 2002) (following *Netcom* for the proposition that "defendants must actively engage in one of the activities recognized in the Copyright Act" before direct liability could be imposed on a site or service); *Marobie-FL, Inc. v. National Ass'n of Fire Equipment Distributors*, 983 F. Supp. 1167, 1172 (N.D. Ill. 1997) (holding a company which hosted a website on which infringing material was posted not liable for direct infringement because, even though it "provide[d] a service somewhat broader than the . . . Internet access provider in Religious Technology Center . . . [it] only provided the means to copy, distribute or display plaintiff's works, much like the owner of a public copy machine used by a third-party to copy protected material."); *Playboy Enterprises, Inc. v. Russ Hardenburgh, Inc.*, 982 F. Supp. 503, 512 (N.D. Ohio 1997) ("some element of direct action or participation" is required); *Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923, 932 (N.D. Cal. 1996) (finding no evidence that BBS operator caused infringing copies to be made merely by operating a

that the act of linking is purportedly unauthorized (for example, where the violation arises from allegedly exceeding the scope of a license rather than because the accessed material is pirated).

Without analyzing any of these questions, the Seventh Circuit, in *Flava Works, Inc. v. Gunter*,⁶⁵ vacated a preliminary injunction entered against myVidster, a social bookmarking site, finding that the plaintiff, the owner of copyrights to gay porn videos, was not likely to prevail on its claim of contributory copyright infringement based on myVidster's use of in-line links to display infringing copies of videos that had been "bookmarked" by users (in a case where the DMCA safe harbors were inapplicable).

myVidster allowed users to "bookmark" videos stored elsewhere on the Internet for other users to access via frames from its site.⁶⁶ Judge Posner, writing for himself and Judges Flaum and Wood, held that the plaintiff had not shown "personal conduct that encourages or assists the infringement" sufficient to establish contributory infringement, where myVidster allowed users to post bookmarks related to any topic (not just plaintiff's works or infringing material),

BBS where third-parties posted infringing software). *But see Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993) (holding a BBS operator liable for infringing photographs potentially posted by a third-party because the Copyright Act is a strict liability statute); *see generally supra* § 4.11[2].

⁶⁵*Flava Works, Inc. v. Gunter*, 689 F.3d 754 (7th Cir. 2012).

⁶⁶When a user bookmarked a video, myVidster would automatically request the video's embed code from the host server, which included the URL for the video with instructions on how to display it. myVidster would then create a page on its site where the video could be viewed in a frame containing ads placed by myVidster. *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 756 (7th Cir. 2012); *see generally infra* § 9.04[1] (analyzing framing). An image of the opening shot of the video would then be displayed as a thumbnail image on the myVidster site. Users who clicked on an image would be shown the video in a frame on the myVidster page for the video, via an in-line link to the host server. As explained by Judge Posner, a user "may think, therefore, that he's seeing the video on myVidster's website. But actually the video is being transmitted directly from the server on which the video is stored to the user's computer." *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 756 (7th Cir. 2012).

Flava operated a service that made its videos available to subscribers behind a paywall. Flava's Terms of Use allowed its subscribers to download videos for personal use but not upload them to other Internet sites. Flava had alleged that 300 bookmarks on myVidster linked to infringing copies of its works.

the infringing videos represented merely 300 out of over 1.2 million bookmarks available on its site, the allegedly infringing videos were available elsewhere on the Internet, myVidster was not providing a market for pirated works, and the losses identified by the plaintiff could not be ascribed entirely to myVidster. In so ruling, the court emphasized that myVidster could have been enjoined for backing up copies of bookmarked videos on its servers (which it had done, prior to being sued by Flava Works, for users who purchased premium memberships)⁶⁷ and suggested in *dicta* that Flava Works could be held liable for inducing copyright infringement if myVidster had *invited* people to post copyrighted videos on the Internet without authorization or bookmark them on its site.⁶⁸

The outcome in *Flava Works* was influenced (perhaps unduly so) by the fact that users viewed, rather than downloaded, copies of videos from myVidster (although the court did not analyze whether streaming, under either the Second Circuit's decision in *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*⁶⁹ or the Ninth Circuit's opinion in *MAI Systems Corp. v. Peak Computer, Inc.*,⁷⁰ amounted to unauthorized reproduction) and by Judge Posner's conclusion that creating an in-line link did not amount to a public performance.⁷¹

In focusing on materiality and largely dismissing plaintiff's knowledge as immaterial, Judge Posner also took a different approach to evaluating links in *Flava Works* than the Ninth Circuit had in *Perfect 10, Inc. v. Amazon.com, Inc.*⁷²

Whether and to what extent a claim may be stated for sec-

⁶⁷*Flava Works, Inc. v. Gunter*, 689 F.3d 754, 762–63 (7th Cir. 2012).

⁶⁸*Flava Works, Inc. v. Gunter*, 689 F.3d 754, 758–59 (7th Cir. 2012); see generally *supra* § 4.11[6] (analyzing inducement).

⁶⁹*Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008), *cert. denied*, 557 U.S. 946 (2009); *supra* § 9.01; see generally *supra* § 4.03 (analyzing the fixation requirement under the Copyright Act in greater detail).

⁷⁰*MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), *cert. dismissed*, 510 U.S. 1033 (1994); *supra* § 9.01; see generally *supra* § 4.03.

⁷¹*Flava Works, Inc. v. Gunter*, 689 F.3d 754, 760–61 (7th Cir. 2012); see generally *supra* § 4.04[3] (analyzing what constitutes a reproduction and public performance in digital media).

⁷²*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1172 (9th Cir. 2007) (reversing the entry of summary judgment on the issue of contributory infringement for providing links to allegedly infringing copies of

ondary copyright infringement based on links thus depends in part on which circuit's law is to be applied.

Even where a *prima facie* case of infringement may be shown, defendants may be able to avoid liability for copyright infringement for establishing links to unauthorized material by virtue of the fair use defense, implied license,

plaintiffs' photographs because liability could be imposed where a defendant had knowledge of specific infringing images coupled with the failure to take "simple measures to prevent further damage."). In *Flava Works*, the plaintiff had sent myVidster takedown notices for specific videos, which the plaintiff allegedly had ignored, which arguably could have created a factual question about whether the defendant could be held liable for continuing to make the videos accessible via in-line links. See *supra* § 4.11[3] (analyzing liability for contributory copyright infringement based on notice and a failure to take corrective action). Focusing on the DMCA, rather than notice for purposes of contributory infringement, Judge Posner explained that failing to respond to notices was irrelevant unless myVidster was contributing to infringement. He wrote that "[t]he infringers are the uploaders of copyrighted work. There is no evidence that myVidster is encouraging them, which would make it a contributory infringement." *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 758 (7th Cir. 2012). While it is true that the DMCA creates a safe harbor, and that failing to comply with the requirements for safe harbor protection may not provide grounds for imposing liability for infringement (17 U.S.C.A. § 512; *supra* § 4.12), Judge Posner did not address *Perfect 10 v. Amazon.com* or other contributory infringement cases, including his own prior opinion in *In re Aimster Copyright Litig.*, 334 F.3d 643 (7th Cir. 2003), that have held that liability for contributory infringement potentially could be imposed based on notice and a subsequent failure to take remedial action. Given that Judge Posner cited the *Perfect 10 v. Amazon.com* case in three different places in the *Flava Works* opinion but did not discuss its contributory infringement analysis or any similarity between that case and *Flava Works*, it seems likely that Judge Posner disagreed with the Ninth Circuit's conclusion that contributory liability for linking could be imposed merely based on notice and a subsequent failure to take simple measures to prevent further damage. See *supra* § 4.11[3] (analyzing the case in greater detail).

In focusing on materiality, Judge Posner's analysis was consistent with another Ninth Circuit case brought by Perfect 10 that also reached a different conclusion about contributory liability than the court in *Perfect 10 v. Amazon.com*. See *Perfect 10, Inc. v. Visa Int'l Service Ass'n*, 494 F.3d 788, 799–800 (9th Cir. 2007) (holding that defendants did not materially contribute to the underlying acts of infringement by providing payment processing services to websites that sold access to infringing images because they did "not operate the servers" on which the infringing images resided), *cert. denied*, 553 U.S. 1079 (2008); see also *Perfect 10, Inc. v. Visa Int'l Service Ass'n*, 494 F.3d at 810–18 (9th Cir. 2007) (Kozinski, C.J. dissenting) (arguing that the majority's finding in *Visa* was inconsistent with *Perfect 10 v. Amazon.com*); see generally *supra* §§ 4.11[3] (contributory infringement), 4.11[5][C] (analyzing *Perfect 10 v. Visa Int'l*).

the *Sony* safe harbor or the information location tools safe harbor created by the Digital Millennium Copyright Act,⁷³ which are addressed later in sections 9.03[3][B] and 9.03[3][C]. As discussed at greater length in those sections, implied license may provide a strong basis for establishing links to most publicly accessible, noninfringing locations, but may be easily negated in most instances where there was not detrimental reliance by the linking party if the owner of the linked material objects to the practice, such as in a letter, notice or email message.⁷⁴ Where available, fair use provides an absolute defense, but it must be proven by a multi-part balancing test, and therefore may be more difficult to establish except through litigation and a ruling on the merits⁷⁵ (although it been relied upon as the basis to grant preliminary relief, based solely on the pleadings, in at least two embedded link cases involving links to Instagram posts).⁷⁶ Where links have been generated by legitimate service providers, the Digital Millennium Copyright Act

⁷³17 U.S.C.A. § 512(d); see generally *supra* § 4.12[7].

⁷⁴See *infra* § 9.03[3][B].

⁷⁵See *infra* § 9.03[3][B].

⁷⁶See *Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 6393010 (E.D.N.Y. Nov. 2, 2020) (dismissing, as fair use, the copyright infringement claim of a photographer against a sports news publisher, which had included an embedded link to an Instagram post by professional tennis player Caroline Wozniacki, announcing her retirements (which included a low-resolution, cropped version of a photograph taken by the plaintiff), in an article it published about Wozniacki's career, which also quoted the text of the Instagram post); *Walsh v. Townsquare Media, Inc.*, 464 F. Supp. 3d 570 (S.D.N.Y. 2020) (entering judgment on the pleadings, based on fair use, in a Paparazzi photographer's copyright infringement claim, brought against the publisher of *XXL* magazine, which had embedded a link to an Instagram post by hip hop artist Cardi B, which included a photograph taken by plaintiff of Cardi B at a Tom Ford fashion show, in an article entitled *Cardi B Partners with Tom Ford for New Lipstick Shade*, which was focused on the event and referenced the Cardi B Instagram post which featured the photograph); see also *Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 7625222 (E.D.N.Y. Dec. 22, 2020) (denying reconsideration). Cf. *Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *5-7 (S.D.N.Y. 2021) (denying defendant's motion to dismiss plaintiff's copyright infringement claim, premised on Sinclair's placement of an embedded link to plaintiff's video of a starving polar bear in an article describing how the video "went 'viral,'" because Sinclair's fair use defense could not be resolved on a motion to dismiss based solely on the allegations of the complaint, despite finding that the use was transformative); *McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 604-09 (S.D.N.Y. 2020) (holding, in an opinion decided before *Boesen* and *Walsh*, that, on the facts

(DMCA) safe harbor for information location tools may insulate a service provider from liability for damages and attorneys' fees if it disables access to or removes a link upon receipt of a substantially compliant DMCA notification.⁷⁷ Likewise, where the links lead to both infringing and noninfringing locations, the *Sony* safe harbor may provide a defense based on substantial noninfringing use. In appropriate circumstances, linking also potentially may be justified as *de minimis* infringement.⁷⁸

Just as the DMCA provides a strong defense for legitimate service providers, it provides an easy mechanism for copyright owners to have links disabled, regardless of whether linking *in fact* constitutes infringement, so long as the link established leads to infringing material.⁷⁹

9.03[3][A][iii] Liability for unwanted links to genuine material on a copyright owner's own site

While linking to infringing material is actionable in appropriate circumstances, parties have had less success using copyright law to restrict links to genuine material on a copyright owner's own site where the claim of infringement is based on a link arguably created in violation of a license term (such as a deep link to otherwise noninfringing material).

Linking potentially may be restricted by contract or license, such as website Terms of Use. Where an enforceable copyright license has been agreed upon, a defendant's use of a site in ways that violate the license (such as linking) potentially could be deemed copyright infringement.¹ In practice, courts may be uncomfortable enforcing contractual

of that case, fair use could not be established as a matter of law at the pleadings stage, in a case where plaintiff posted a photograph of an ephemeral lake on March 13, 2019, and the very next day Newsweek allegedly published an article about the ephemeral lake, embedding plaintiff's Instagram post about the lake, as part of the article).

⁷⁷See *infra* § 9.03[3][C].

⁷⁸See *infra* § 9.03[3][B].

⁷⁹See *infra* § 9.03[3][D].

[Section 9.03[3][A][iii]]

¹*E.g., Ticketmaster LLC v. RMG Technologies, Inc.*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007) (holding that the defendant was bound by posted Terms that formed a non-exclusive license to access Ticketmaster's website where the defendant acknowledged that it was on notice that its access to

restrictions that limit otherwise permissible conduct.² Where asserted, claims over unwanted links to otherwise noninfringing material may turn on the enforceability of the alleged license. To date, few cases have been brought involving ostensibly unauthorized links to otherwise noninfringing content.

In *Ticketmaster Corp. v. Tickets.com, Inc.*,³ Judge Harry L. Hupp of the Central District of California granted the defendant's motion to dismiss Ticketmaster's claim for contributory copyright infringement, ruling in part that Ticketmaster's purported license restrictions prohibiting deep linking were unenforceable because they were contained in Terms and Conditions which users were not actually required to review in order to access the Ticketmaster site and therefore were not part of a binding contract.⁴

In a subsequent decision,⁵ the court denied the defendant's motion for summary judgment on Ticketmaster's breach of contract claim, finding that a contract could have been formed when Tickets.com proceeded into the interior of the Ticketmaster site after knowing of the conditions imposed by Ticketmaster for doing so. The *Ticketmaster* case, which also raised Lanham Act issues, is considered in greater detail in section 9.03[7].

In both theory and practice, it may be difficult to state a claim over unwanted links (other than in limited circumstances in a few district court opinions involving embedded links to photographs, as discussed in section 9.03[3][A][ii]). A plaintiff would have to establish that visiting its website was a licensed activity, that the license prohibited linking and that a site that established an unwanted link facilitated a third-party's act of infringement (i.e., a user's unauthorized visit, via a link, which created a copy of the website to be cached—or created—in the temporary memory of the visi-

the site was subject to Terms); see generally *supra* § 5.03[2]; *infra* § 21.02[7].

²See *supra* § 5.02 (restrictions in database contacts); *infra* § 16.04 (misuse).

³*Ticketmaster Corp. v. Tickets.com, Inc.*, 54 U.S.P.Q.2d 1344, 2000 WL 525390 (C.D. Cal. Mar. 27, 2000).

⁴See *infra* § 21.03 (discussing Tickets.com and enforceable unilateral contracts).

⁵*Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 Copr. L. Dec. P 28607, 2003 WL 21406289 (C.D. Cal. Mar. 7, 2003).

tor's computer). Otherwise, a plaintiff would have difficulty explaining how creating a temporary copy via a link constituted infringement while creating the same temporary copy through direct access would not. To establish a copyright violation merely for the act of creating an unauthorized link, a plaintiff therefore would have to prove the existence of a valid license (express or implied) restricting the rights of visitors to link to the site⁶ (which, in turn, may depend on how its website Terms and Conditions are structured,⁷ unless the site is otherwise accessible only to subscribers) and establish that the party creating the link knew or should have known that it was creating an unauthorized link (to show contributory infringement), which could be difficult to do.

To make out such a claim in the case of a publicly accessible website, a plaintiff would have to ensure that there was a notice on its website purporting to prohibit unauthorized links or that visitors had to click their assent to a formal agreement before gaining access to the site. However, to the extent an infringement claim may be dependent on proving that the defendant exceeded the scope of a unilateral website license, the claim could be difficult to establish because the purported license restrictions would not necessarily run to a user who accessed the linked site without prior knowledge of the terms and conditions or the linking site's failure to obtain a formal license. The limitation, if enforceable, potentially could be construed as binding only on the party that created the link. Absent a direct copyright violation by users accessing a site via an unauthorized link, there would be no basis for holding a defendant contributorily liable (or the owner such party if it had a direct financial interest in the site).

A claim over unwanted site links to otherwise noninfringing content generally suffers from the same potential obstacles as one involving links to infringing materials—*Cartoon Network*, the DMCA, fair use, implied license, the

⁶*See, e.g., S.O.S., Inc. v. Payday, Inc.*, 886 F.2d 1081, 1087–89 (9th Cir. 1989) (exceeding the scope of a license constitutes copyright infringement); *Apple Computer, Inc. v. Microsoft Corp.*, 35 F.3d 1435, 1442 (9th Cir. 1994), *cert. denied*, 513 U.S. 1184 (1995) (same).

⁷For an analysis of the enforceability of website licenses and terms and conditions, *see infra* §§ 21.03, 21.04 & chapter 22.

Sony safe harbor⁸ and even whether the basic elements to establish secondary liability may be established—with the added burden of requiring a showing of infringement based on exceeding the scope of a license (since the material is not inherently infringing) and the practical problem of convincing a court to take action in a case that does not involve piracy (and where both damages and irreparable injury may be difficult to show). Ultimately, a theory of liability that depends upon a court finding users of the World Wide Web directly liable for copyright infringement—in order to provide the necessary underlying act of infringement to impose secondary liability on the business entity that created the link—may be too difficult to successfully advance in court in many cases. Suits over unwanted links to genuine (as opposed to pirated) material may be better framed as interference with contract claims, assuming damages can be shown, or on other grounds besides copyright infringement.

9.03[3][A][iv] Multiple links

To the extent that liability may be premised on facilitating or encouraging an act of infringement through the creation of a link, the connection between the linking site and location of infringing content would have to be direct, rather than more attenuated. For example, in *Bernstein v. J.C. Penney, Inc.*,¹ celebrity photographer Gary Bernstein filed suit against the J.C. Penney department store and cosmetics company Elizabeth Arden alleging copyright infringement based on a link from a J.C. Penney site created in November 1997 to advertise Passion, an Elizabeth Arden perfume promoted by actress Elizabeth Taylor. A link from a portion of the site that featured online chat with Ms. Taylor led to a site hosted by Internet Movie Database that contained biographical information about her. That site, in turn, contained links to several other locations—including a site run by Swedish University Network (SUNET) where unauthorized reproductions of two photographs that Mr. Bernstein had taken of Ms. Taylor were posted.

In dismissing plaintiff's suit in September 1998, Judge Manuel Real of the Central District of California implicitly

⁸See *infra* §§ 9.03[3][B], 9.03[3][C].

[Section 9.03[3][A][iv]]

¹*Bernstein v. JC Penney, Inc.*, 26 Media L. Rep. (BNA) 2471, 50 U.S.P. Q.2d 1063, 1998 WL 906644 (C.D. Cal. 1998).

ruled that the connection between defendant's site and the infringing photographs were too far removed to be actionable under the Copyright Act.² Even where a link is one click away from infringing content, a plaintiff likely would need to show more than merely the establishment of a link in order to state a claim for contributory infringement.³

9.03[3][B] General Defenses to Liability for Linking: Implied License, Fair Use, *De Minimis* Infringement and the *Sony* Safe Harbors

9.03[3][B][i] Linking Defenses—In General

Even where copyright liability potentially may be shown, a number of defenses may apply to permit linking in different contexts on the World Wide Web, including implied license, fair use and *de minimis* infringement and the Digital Millennium Copyright Act (DMCA) and *Sony* safe harbors. The DMCA liability limitation for information location tools is separately considered in sections 9.03[3][D] (as a defense) and 9.03[3][E] (as a potential remedy for copyright owners).

²*Bernstein v. JC Penney, Inc.*, 26 Media L. Rep. (BNA) 2471, 50 U.S.P. Q.2d 1063, 1998 WL 906644 (C.D. Cal. 1998); *see also* John Borland, "Court Dismisses Web Copyright Case," TechWeb, CMPnet, Sept. 22, 1998. Judge Real did not specifically state the basis for his ruling, although his characterization of plaintiff's claim as being "for copyright infringement based on multiple linking . . ." suggests in part his view of the principal issue in the case. He also re-stated defendants' arguments in his brief ruling:

Arden contends that plaintiff's theory of infringement by multiple linking would have a devastating impact on the Internet and argues the claim should be dismissed for three reasons: (1) a company whose product is merely displayed on another entity's website cannot be held liable for any infringement by the author of that website; (2) linking cannot constitute direct infringement because the computer server of the linking website does not copy or otherwise process the content of the linked-to site; and (3) multiple linking cannot constitute contributory infringement because (a) Internet users viewing of the material at issue is not infringing and thus there was no direct infringement in the United States to which Arden could contribute, . . . (b) linking "is capable of substantial noninfringing uses" and thus cannot support a claim for contributory infringement, . . . and (c) the Court cannot infer from the facts alleged that Arden knew the photos had been posted to SUNET and multiple linking does not constitute substantial participation in any infringement where the linking website does not mention the fact that Internet users could, by following the links, find infringing material on another website

1998 WL 906644, at *1 (citations omitted).

³*See infra* §§ 9.03[3][A][ii], 9.03[3][B].

9.03[3][B][ii] Implied License

Linking on the Internet is pervasive. As its name implies, the World Wide Web is little more than a series of links, interconnected like a spider's web. For this reason, a strong argument may be advanced in most instances that, by placing a publicly accessible site or publicly accessible material on the World Wide Web, a party impliedly licenses others to link to it.¹ If a site owner did not want third-parties to link to its site, it arguably would have required users to register and prevented unauthorized access. A publicly accessible website, by inference (and based on both netiquette and the technology underlying the World Wide Web), is one that may be linked to by third-parties, at least to the extent that the link is not deceptive or confusing and provided the site owner has not taken steps to negate any inference of implied license.

The implied license defense, however, usually does not assure a potential defendant of the right to continue linking to a site in the future, even if it was permissible to do so in the past. Except where consideration has been paid, an implied license generally may be revoked.² If a website owner learns of an unwanted link and sends the linking party a cease and desist letter demanding that the link be disabled, the defense of implied license should cease to provide ongoing protection.³ The linking party, however, may still assert other defenses.

Rather than wait until a party establishes a link to send notice negating any inference of implied license, some website owners incorporate provisions in their terms and conditions (or the legal notices section of a website) purporting to prohibit or condition a third-party's right to establish links to the site.⁴ Whether website terms and conditions constitute binding contractual restrictions on visitors to a site will depend on the way they are presented to users, whether

[Section 9.03[3][B][ii]]

¹*See, e.g., Effects Associates, Inc. v. Cohen*, 908 F.2d 555, 558–59 (9th Cir. 1990), *cert. denied*, 498 U.S. 1103 (1991); *see generally supra* §§ 4.05[7], 9.02[2].

²*See supra* § 4.05[7].

³A linking party theoretically could potentially assert ongoing rights in derivative works when an implied license is terminated, but this copyright law principle may not apply to links, which may be easily disabled. *See supra* § 4.05[7].

⁴For sample provisions, *see infra* chapter 20.

users may avoid them and still gain access to the site and ultimately whether assent was obtained either expressly or by implication.⁵ Where there is an express license, an implied license generally may not be inferred between the same parties for the same subject matter.⁶

Even where purported restrictions on linking contained in website terms and conditions are found not to be binding under contract law (and therefore may not support a claim for breach of contract or copyright infringement based on exceeding the scope of a license), they may be sufficient to negate an inference of an implied license. It therefore may be advisable to check the terms and conditions before linking to a site that may be likely to object to links.

Although the issue of implied license has not been litigated extensively in connection with links, district court judges in New York have held that Instagram receives an express license from users who upload images to its platform, to allow other users to embed those images, but whether Instagram in turn grants its users a license to imbed images posted by other users, when they use Instagram's API (application programming interface) to embed a link to an image posted on Instagram's servers, is a question that could not be resolved through a motion to dismiss because additional evidence was required.⁷

Implied licenses are analyzed further in section 4.05[7] in

⁵See *infra* chapters 21, 22 (especially sections 21.03 and 21.04).

⁶See, e.g., *Baer v. Chase*, 392 F.3d 609, 616-17 (3d Cir. 2004) ("There cannot be an implied-in-fact contract if there is an express contract that covers the same subject matter.").

⁷See *McGucken v. Newsweek LLC*, 19 Civ. 9617 (KPF), 2020 WL 6135733, at *1-3 (S.D.N.Y. Oct. 19, 2020) (affirming, in denying reconsideration, that "while Instagram's Terms of Use clearly granted Instagram a license to sublicense Plaintiff's publicly posted content, there was insufficiently clear language to support, in the context of a Rule 12(b)(6) motion, the existence of a sublicense between Instagram and Defendant."); *Sinclair v. Ziff Davis, LLC*, 18-CV-790 (KMW), 2020 WL 3450136, at *1-2 (S.D.N.Y. June 24, 2020) (adhering to its previous holding that, "by agreeing to Instagram's Terms of Use, Plaintiff authorized Instagram to grant API users, such as Mashable, a sublicense to embed her public Instagram content, as set forth in Instagram's Platform Policy" but granting reconsideration, and revising its previous decision, by holding "that the pleadings contain insufficient evidence to find that Instagram granted Mashable a sublicense to embed Plaintiff's Photograph on its website."); *McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 603-04 (S.D.N.Y. 2020) (denying Newsweek's motion to dismiss, holding that while Instagram's Terms of Use "unequivocally grant Instagram a license to sublicense

chapter 4 on digital copyright law.

9.03[3][B][iii] Linking as a Fair Use

Fair use, unlike implied license, does not depend on a copyright owner's tacit consent and therefore cannot be easily negated by a copyright owner. The fair use defense presupposes that any copying done is not authorized by the copyright owner.¹ Thus, even where website terms and conditions purport to prohibit links to a site, a party may avoid li-

Plaintiff's publicly posted content . . . , and the Privacy Policy clearly states that 'other Users may search for, see, use, or share any of your User Content that you make publicly available through' Instagram . . . ,” the court could not dismiss plaintiff's claims; “Although Instagram's various terms and policies clearly foresee the possibility of entities such as Defendant using web embeds to share other users' content . . . , none of them expressly grants a sublicense to those who embed publicly posted content. Nor can the Court find, on the pleadings, evidence of a possible implied sublicense. . . . While the Court acknowledges that it may be possible to read Instagram's various terms and policies to grant a sublicense to embedders, the Court's role on a Rule 12(b)(6) motion is to ‘draw all reasonable inferences in Plaintiff's favor.’ ”).

In *Ziff Davis*, Judge Wood previously had granted Ziff Davis's motion, dismissing Sinclair's copyright infringement claim, based on the finding that Mashable had used plaintiff's photograph pursuant to a valid sublicense from Instagram. *See Sinclair v. Ziff Davis, LLC*, 454 F. Supp. 3d 342, 344-47 (S.D.N.Y. 2020). She explained:

The Terms of Use state that, by posting content to Instagram, the user “grant[s] to Instagram a non-exclusive, fully paid and royalty-free, transferable, sublicensable, worldwide license to the Content that you post on or through [Instagram], subject to [Instagram's] Privacy Policy.” (Terms of Use, Rights § 1.) Pursuant to Instagram's Privacy Policy (“Privacy Policy”), Instagram users designate their accounts as “private” or “public,” and can change these privacy settings whenever they wish. (Privacy Policy, Parties With Whom You May Choose to Share Your User Content § 1.). All content that users upload and designate as “public” is searchable by the public and subject to use by others via Instagram's API. (*Id.* § 2.) The API enables its users to embed publicly-posted content in their websites. (Platform Policy, Preamble.). Thus, because Plaintiff uploaded the Photograph to Instagram and designated it as “public,” she agreed to allow Mashable, as Instagram's sublicensee, to embed the Photograph in its website.

Id. at 345. On reconsideration, however, the court concluded that Instagram's Platform Policy could be construed as granting Instagram API users the right to use the API to embed the public content of other Instagram users, but that was not the only interpretation to which it was susceptible (and accordingly construction of the license was not an issue that could be resolved on a motion to dismiss, which assumes as true the well pleaded facts in a plaintiff's Complaint). *See Sinclair v. Ziff Davis, LLC*, 2020 WL 3450136, at *1.

[Section 9.03[3][B][iii]]

¹*See supra* § 4.10.

ability for linking to it if any acts of unauthorized copying occurring in connection with the link are deemed a fair use.

In *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,² Judge Whyte suggested that a user's act of browsing both created a protectable copy and (if the copy were infringing) would inevitably be viewed as fair use. While many people believe that linking should be deemed a fair use as a matter of policy, fair use is determined by a multi-part balancing test, and therefore the outcome may vary in a given case depending on its unique facts.³ At a minimum, if the underlying act of viewing a website were viewed as a fair use, there would be no grounds for imposing secondary liability for copyright infringement on the party that created the link (since secondary liability must be premised on an underlying act of direct infringement by a third party).⁴ The fair use defense in connection is considered more extensively in section 9.02[4] in connection with caching and more generally in section 4.10[1] in chapter 4 (on copyright law).

In *Online Policy Group v. Diebold Election Systems, Inc.*,⁵ the court found that links to a database company's internal emails explaining technical flaws in its electronic voting machines were a fair use (for purposes of evaluating an award of fees for knowingly and materially misrepresenting information in a DMCA Notification pursuant to 17 U.S.C.A. § 512(f)),⁶ where at least some of the emails were not entitled to copyright protection, even though the links directed users to the defendant's entire proprietary database.

The Ninth Circuit analyzed fair use in connection with links generated by search engines in two separate cases. In *Kelly v. Arriba Software Corp.*,⁷ Ditto.com (previously Arriba Software Corp.) operated a visual search engine that allowed

²*Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1378 n.25 (N.D. Cal. 1995).

³The fair use defense of a user would likely be stronger than the fair use defense of a commercial entity seeking to establish an unauthorized link to another site, especially if there were a commercial market for links to the site.

⁴See *supra* § 4.11.

⁵*Online Policy Group v. Diebold, Inc.*, 337 F. Supp. 2d 1195 (N.D. Cal. 2004).

⁶See *supra* § 4.12[9][D].

⁷*Kelly v. Arriba Soft Corp.*, 336 F.3d 811 (9th Cir. 2003).

users to locate images on the Web. In response to a query, small, low resolution “thumbnail” images were displayed next to a link and brief description of the corresponding site where the photograph could be found. Images were obtained automatically by a crawler program that downloaded full size copies to Arriba’s server, where they were converted to thumbnails. Thumbnail images could be copied by users, but their resolution could not be improved. Users, in turn, could access the site from where a thumbnail originated via a link or, for brief periods in 1999 and 2000, view full size copies of the photographs via in-line links or frames, separate and apart from the rest of the content on the linked site.

The Ninth Circuit ruled that the reproduction of thumbnail images constituted a fair use because defendants’ copying was transformative (to index images on the Web) and did not adversely affect the potential market for the genuine works because the thumbnails were not a substitute for full-size, high resolution images. The court found that the nature of the work (creative photographs) weighed slightly in favor of the plaintiff and the amount and substantiality of the portion used was a neutral factor because if Arriba had copied anything less than the complete works it would have been more difficult to identify each image, which would have reduced the usefulness of the search engine.

In an earlier ruling that was subsequently vacated because the issue had not been properly preserved for appeal, the Ninth Circuit had ruled that the defendant’s initial practice of also making available via in-line links and frames full size copies of the photographs that appeared on indexed sites (with the surrounding text and other Web content removed) was not a fair use. Displaying the exact image from a site in isolation from the surrounding material via a frame or in-line link was held to serve no transformative purpose and harm the market for genuine works because people receiving photographs in this format would have had no reason to visit the website from which it had been copied.⁸

In *Perfect 10, Inc. v. Amazon.com, Inc.*,⁹ the Ninth Circuit reaffirmed its 2003 opinion in *Kelly v. Arriba Software Corp.* in a case involving very similar facts. In that case, Perfect

⁸See *Kelly v. Arriba Soft Corp.*, 280 F.3d 934, 947–48 (9th Cir. 2002), vacated, 336 F.3d 811 (9th Cir. 2003).

⁹*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1163–67 (9th Cir. 2007).

10, an adult magazine whose images were widely available without authorization on the Internet, sued Google and Amazon.com arguing that their visual search engines made unauthorized thumbnail reproductions of infringing copies of their works that were displayed with search results. To distinguish *Kelly v. Arriba Software Corp.*, Perfect 10 had argued that these thumbnail images undermined a market for thumbnail images sold for display on cell phones. Unlike in *Kelly*, Perfect 10 had argued (and the district court had agreed), the thumbnails displayed by Google had an adverse impact on the market for genuine products and therefore were not a fair use. The Ninth Circuit reversed, however, concluding that “the significantly transformative nature of Google’s search engine, particularly in light of its public benefit, outweighs Google’s superseding and commercial uses of the thumbnails in this case.”¹⁰ The court noted that any downloads for mobile phones in fact had taken place, making the superseding use “not significant.” Likewise, although thumbnails directed users to Google AdSense partners, including partners that hosted infringing images, which the court conceded added “a commercial dimension that did not exist in *Kelly*,” the Ninth Circuit emphasized that the district court had not determined that this commercial element was significant.¹¹ Judge Ikuto, writing for the court, concluded that “the transformative nature of Google’s use is more significant than any incidental superseding use or the minor commercial aspects of Google’s search engine and website.”¹² With respect to the nature of the copyrighted work, the court found the photos to be creative but because the images appeared on the Internet before they were used in search engine results, this factor weighted only slightly against a finding of fair use.

In *Perfect 10, Inc. v. Yandex, N.V.*,¹³ a subsequent case brought by Perfect 10 against a Russian search engine that, unlike Google, displayed full size versions of Perfect 10 images via in-line links (and not merely thumbnails) and also

¹⁰*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1166 (9th Cir. 2007).

¹¹*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1167 (9th Cir. 2007).

¹²*Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1163–67 (9th Cir. 2007).

¹³*Perfect 10, Inc. v. Yandex, N.V.*, 962 F. Supp. 2d 1146 (N.D. Cal. 2013).

displayed them separate and apart from the websites on which they appeared, the district court, in granting in part the defendant's motion for summary judgment, ruled, among other things, that the defendant's use of the images in connection with a search engine nonetheless constituted a fair use because it was highly transformative.¹⁴ The court wrote that "whether a browser window shows only a thumbnail and the full-size image—instead of the full-size image along with part of the surrounding web page—does not affect whether the use of the *thumbnail* has been transformed."¹⁵ Further, the court held that "even if yandex.com's use of the thumbnail were broadly described as an 'in-line link connected to a full-size image,' that use remains highly transformative."¹⁶

The court also rejected the argument that the defendant's use adversely harmed the market for the genuine works because, among other things, Perfect 10 had presented evidence that Yandex made accessible "billions of unauthorized views" from third party websites because Perfect 10's evidence was not substantiated by competent evidence. Perfect 10 had introduced screen shots from third-party websites showing that links on those sites led to Perfect 10 images that had been viewed 3.8 million times as of December 2012. Perfect 10 did not, however, provide evidence that any of those views were the result of yandex.com users clicking on thumbnails stored on yandex.com servers in the United States, however. The court wrote that "[t]he simple fact that the thumbnail links were stored in yandex.com's index and accessible on the internet does not compel a finding that those links were actually viewed or used."¹⁷

On balance, the court, in weighing the various factors,

¹⁴See *Perfect 10, Inc. v. Yandex, N.V.*, 962 F. Supp. 2d 1146, 1154–55 (N.D. Cal. 2013).

¹⁵*Perfect 10, Inc. v. Yandex, N.V.*, 962 F. Supp. 2d 1146, 1155 (N.D. Cal. 2013) (emphasis in original).

¹⁶*Perfect 10, Inc. v. Yandex, N.V.*, 962 F. Supp. 2d 1146, 1155 (N.D. Cal. 2013).

¹⁷*Perfect 10, Inc. v. Yandex, N.V.*, 962 F. Supp. 2d 1146, 1156 (N.D. Cal. 2013). Other arguments advanced by Perfect 10 were characterized as based on "speculation, not proof" or insufficient to show that the alleged drop in demand for Perfect 10 images was caused by Yandex, as opposed to other factors, because a "simple correlation, without more, does not constitute sufficient evidence that Yandex's use of 40,000 thumbnail images between June 2012 and March 2013 affected Perfect 10's market." *Id.* at 1156-57.

concluded that “Yandex’s significant transformative use” weighed more heavily in favor of fair use than the nature of the work, which weighed “slightly in favor of Perfect 10, and the neutral third and fourth factors. Upon due consideration, . . . Yandex.com’s thumbnails stored on its servers in the United States for a nine month period were a fair use.”¹⁸

By contrast, in *VHT, Inc. v. Zillow Group, Inc.*,¹⁹ the Ninth Circuit held that the unauthorized use of copyrighted photos in connection with a visual search engine used on a commercial real estate service’s website was not a fair use, explaining that “the label ‘search engine’ is not a talismanic term that serves as an on-off switch as to fair use.”²⁰ Unlike the search engines at issue in *Kelly v. Arriba* and *Perfect 10 v. Amazon* (as well as *Perfect 10 v. Yandex*, although the Ninth Circuit didn’t address that district court opinion), Digs, the search engine employed on the Zillow.com website for home improvement and remodeling, was “a closed-universe search engine” that did not crawl the web. Users could search a “searchable set” of images within a “walled garden. . . .”²¹ The search results did not direct users to the original sources of the photos, such as the plaintiff’s website, but rather linked to other pages within Zillow’s website. The Ninth Circuit found that making these images searchable did not fundamentally change their original purpose when produced by the plaintiff. Additionally, Digs displayed entire copies of plaintiff’s images, not merely thumbnails. Zillow’s use, the court found, merely superseded plaintiff’s purpose in creating the images in the first place. As in *Kelly v. Arriba* and *Perfect 10 v. Amazon*, the images at issue were found to be creative. But unlike in those cases, the Ninth Circuit found Zillow’s use to have few, if any, transformative qualities. In addition, “[i]n contrast to *Amazon* and *Kelly*, nothing justifie[d] Zillow’s full copy display of VHT’s photos on Digs.”²² Finally, unlike in those cases, the court found that Zillow’s use undermined plaintiff’s market for licensing

¹⁸*Perfect 10, Inc. v. Yandex, N.V.*, 962 F. Supp. 2d 1146, 1157 (N.D. Cal. 2013).

¹⁹*VHT, Inc. v. Zillow Group, Inc.*, 918 F.3d 723, 742-44 (9th Cir. 2019).

²⁰*VHT, Inc. v. Zillow Group, Inc.*, 918 F.3d 723, 742 (9th Cir. 2019).

²¹*VHT, Inc. v. Zillow Group, Inc.*, 918 F.3d 723, 742 (9th Cir. 2019).

²²*VHT, Inc. v. Zillow Group, Inc.*, 918 F.3d 723, 744 (9th Cir. 2019).

the photographs.²³ Although the plaintiff had only licensed a handful of photos for secondary uses (and none on a searchable database), the court characterized the market as more significant than the merely hypothetical market at issue in *Perfect 10 v. Amazon*. The appellate panel also found it significant that the plaintiff was “actively exploring” the market for licensing its photos to home design websites like Digs—including with Zillow itself.²⁴

Following *VHT*, the Eleventh Circuit in *MidlevelU, Inc. v. ACI Information Group*,²⁵ affirmed a jury finding that Newstex (operator of ACI Information Group, a wholesale news content aggregator)’s use of MidlevelU (operator of the ThriveAP blog)’s copyrighted articles in the Scholarly Blog Index, a curated index of abstracts and full-text articles of academic blogs, was not a fair use, even though its database was searchable, because, among other things, the jury “could have reasonably found that the Index was not a transformative use based on the Index’s inclusion of iFrames showing the full-text content of MidlevelU’s articles. A reasonable juror could have found that the iFrames obviated any need for an Index subscriber to visit MidlevelU’s website directly, so the Index superseded the use of the originals.”²⁶

Likewise, reproducing thumbnail images of advertisements for the purpose of advertising sales of the genuine product was held not to constitute a fair use in *Batesville Services, Inc. v. Funeral Depot, Inc.*²⁷ Similarly, creating links to a stream of a live webcast of motor races that were shown in real time was held not to be a fair use in *Live Nation Motor Sports, Inc. v. Davis*.²⁸

District courts in New York have also relied on the fair use defense in dismissing copyright infringement claims (or entering judgment on the pleadings) premised on publishers’

²³*VHT, Inc. v. Zillow Group, Inc.*, 918 F.3d 723, 744 (9th Cir. 2019).

²⁴*VHT, Inc. v. Zillow Group, Inc.*, 918 F.3d 723, 744 (9th Cir. 2019).

²⁵*MidlevelU, Inc. v. ACI Information Group*, 989 F.3d 1205 (11th Cir. 2021), *cert. denied*, — S. Ct. —, 2021 WL 2637905 (2021).

²⁶*MidlevelU, Inc. v. ACI Information Group*, 989 F.3d 1205, 1222 (11th Cir. 2021), *cert. denied*, — S. Ct. —, 2021 WL 2637905 (2021).

²⁷*Batesville Services, Inc. v. Funeral Depot, Inc.*, No. 1:02-CV-01011–DFH–TA, 2004 WL 2750253 (S.D. Ind. Nov. 10, 2004).

²⁸*Live Nation Motor Sports, Inc. v. Davis*, Civil Action No. 3:06-CV-276-L, 81 U.S.P.Q.2d 1826 (N.D. Tex. Jan. 9, 2007); *see generally supra* § 9.03[3][A][i] (discussing the case).

use of embedded links to Instagram posts that included plaintiff's photographs.²⁹

9.03[3][B][iv] *De Minimis* Infringement

Linking alternatively potentially could be found permissible as *de minimis* infringement. An act of unauthorized copying will not be deemed actionable where it is merely *de minimis*, as judged by both the quality and the quantity of the portion copied.¹ Although a link allows a visitor to create a complete copy of the linked page on a visitor's temporary screen RAM (when the site is called up), the copy is merely temporary and will not be permanently stored. Merely the

²⁹See *Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 6393010 (E.D.N.Y. Nov. 2, 2020) (dismissing, as fair use, the copyright infringement claim of a photographer against a sports news publisher, which had included an embedded link to an Instagram post by professional tennis player Caroline Wozniacki, announcing her retirements (which included a low-resolution, cropped version of a photograph taken by the plaintiff), in an article it published about Wozniacki's career, which also quoted the text of the Instagram post); *Walsh v. Townsquare Media, Inc.*, 464 F. Supp. 3d 570 (S.D.N.Y. 2020) (entering judgment on the pleadings, based on fair use, in a Paparazzi photographer's copyright infringement claim, brought against the publisher of *XXL* magazine, which had embedded a link to an Instagram post by hip hop artist Cardi B, which included a photograph taken by plaintiff of Cardi B at a Tom Ford fashion show, in an article entitled *Cardi B Partners with Tom Ford for New Lipstick Shade*, which was focused on the event and referenced the Cardi B Instagram post which featured the photograph); see also *Boesen v. United Sports Publications, Ltd.*, 20-CV-1552 (ARR) (SIL), 2020 WL 7625222 (E.D.N.Y. Dec. 22, 2020) (denying reconsideration). Cf. *Nicklen v. Sinclair Broadcast Group, Inc.*, — F. Supp. 3d —, 2021 WL 3239510, at *5-7 (S.D.N.Y. 2021) (denying defendant's motion to dismiss plaintiff's copyright infringement claim, premised on Sinclair's placement of an embedded link to plaintiff's video of a starving polar bear in an article describing how the video "went 'viral,'" because Sinclair's fair use defense could not be resolved on a motion to dismiss based solely on the allegations of the complaint, despite finding that the use was transformative); *McGucken v. Newsweek LLC*, 464 F. Supp. 3d 594, 604-09 (S.D.N.Y. 2020) (holding, in an opinion decided before *Boesen* and *Walsh*, that, on the facts of that case, fair use could not be established as a matter of law at the pleadings stage, in a case where plaintiff posted a photograph of an ephemeral lake on March 13, 2019, and the very next day Newsweek allegedly published an article about the ephemeral lake, embedding plaintiff's Instagram post about the lake, as part of the article).

[Section 9.03[3][B][iv]]

¹See *supra* § 4.08[1].

linked page²—not the full site—will be copied into temporary memory. Moreover, temporary RAM copies generally will be destroyed when the user turns off his or her computer (and in some cases even sooner). Although *de minimis* infringement typically is judged by physical world standards, which focus on the amount and quality of the portion copied, it could be argued that, as applied to cyberspace—where the extent of copying under certain circumstances should be judged at least in part by the length of time that the content may be made available online, rather than merely the percentage of the work that was copied³ (especially given the ethereal quality of cached copies)—a complete, but temporary, copy of a single linked Web page should be deemed *de minimis* in at least some cases.⁴ As a practical matter, however, it is difficult to prevail on a defense of *de minimis* infringement.

9.03[3][B][v] *Sony* Safe Harbor

In a suit based on linking, it is also possible that a defendant could assert the *Sony* safe harbor, arguing that liability should not be imposed because linking has substantial and commercially significant non-infringing uses.¹ In evaluating the applicability of the *Sony* safe harbor, the nature of the content made accessible by the links—not the act of linking, in the abstract—is what should be the focus of any inquiry into whether the links have substantial noninfringing uses.

9.03[3][C] DMCA Safe Harbor Liability Limitation Defense for Information Location Tools

Even if linking is found to constitute copyright infringement, entities that qualify as “Service Providers” under the

²Depending on the software run, a browser may automatically load pages in addition to the one directly linked to facilitate faster access to locations that a user may later select. In most cases, a user is not even aware of precisely which pages have been loaded into her computer’s temporary memory—many of which she in fact may not decide to access. Except where a website is comprised of a very small number of linked pages, the entire site generally is unlikely to be loaded into RAM.

³See generally *supra* §§ 1.06[6] to 1.06[9], 4.10.

⁴The transitory nature of a copy created in screen RAM also could be relevant to fair use analysis.

[Section 9.03[3][B][v]]

¹See *supra* §§ 4.10[5], 4.11[3].

Digital Millennium Copyright Act (DMCA) may be able to limit their liability for damages and attorneys' fees for links established to infringing sites.¹ Entities, but not necessarily individuals, may qualify if, among other things, they provide "online services or network access." or operate facilities therefor.² The limitation would not apply to linking *per se*, but only to the act of linking or referring users to an online location "containing infringing material or infringing activity"³ In other words, the limitation would not apply to all cases of unwanted links; only links alleged to lead to sites containing infringing content or promoting infringement (such as by the provision of cracker tools).

A Service Provider that otherwise meets certain general threshold prerequisites (described in section 4.12[3]) may limit its liability for infringement for linking or referring users to infringing material or activity by using "information location tools, including a directory, index, reference, pointer, or hypertext link" (1) if the Service Provider does not have actual knowledge or awareness of the infringement or, if it has either, it promptly removes or disables access to the infringing material; (2) where a Service Provider has the right and ability to control the infringing activity, it does not receive a financial benefit "directly attributable to the infringing activity" and (3) upon receipt of a Notification (as defined under the statute), the Service Provider removes or disables access to any allegedly infringing links.⁴

The DMCA liability limitations are analyzed extensively in section 4.12. The safe harbor applicable to links, as information location tools, is analyzed in section 4.12[7].

9.03[3][D] Extra-Judicial Remedies Available to Copyright Owners under the DMCA

In addition to affording Service Providers protection from copyright liability for linking, the Digital Millennium Copyright Act provides copyright owners with a specific extra-judicial mechanism to obtain the removal of unwanted links

[Section 9.03[3][C]]

¹See *supra* § 4.12.

²17 U.S.C.A. § 512(k).

³17 U.S.C.A. § 512(k) § 512(d).

⁴See *supra* § 4.12[7].

alleged to be infringing.¹ If a site that has established a link has chosen to comply with the Act, copyright owners may be entitled to have the link removed merely by serving a substantially complying statutory “Notification” on the site’s registered agent.² This extra-judicial remedy is potentially quite valuable given how difficult it would be in most instances for a plaintiff to obtain a comparable court order based on copyright law.

The DMCA liability limitations are analyzed extensively in section 4.12.

9.03[4] Significance of Web Linking Agreements

Entering into an express Web linking agreement may be advisable when the owner of a popular site wants to maintain control over the manner in which other sites link to it. Likewise, a linking agreement may be appropriate if a trademark owner seeks to impose quality controls on the use of its marks.¹

If a website owner expressly declines permission to link to its site, its refusal could negate any inference of an implied license, although it would have no bearing on whether a link constituted a fair use or merely *de minimis* infringement, if those defenses were found applicable.² Linking to a site over the express objection of the linked site also potentially could give rise to other claims, depending on the facts of a given case. More importantly, as a practical matter, a site that aggressively seeks to prohibit links may be more likely to take legal action (regardless of whether it would actually prevail).

To the extent a site commands license fees to link to it, the argument that linking constitutes a fair use would be weaker (since the existence of a commercial market for authorized copying is a factor that weighs against a finding of fair use).³ On the other hand, the fact that so few sites in general seek to require permission to link potentially

[Section 9.03[3][D]]

¹See *supra* § 4.12[12].

²See *supra* § 4.12[12].

[Section 9.03[4]]

¹For additional considerations involving Web linking agreements, as well as sample provisions, see *infra* chapter 20.

²See *supra* § 9.03[3][B].

³See, e.g., *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2022

Ian C. Ballon

2022
UPDATES -
INCLUDING
NEW AND
IMPORTANT
FEATURES

THE PREEMINENT
INTERNET AND
MOBILE LAW
TREATISE FROM A
LEADING INTERNET
LITIGATOR — A
5 VOLUME-SET &
ON WESTLAW!



To order call **1-888-728-7677**
or visit **lanBallon.net**

Key Features of E-Commerce & Internet Law

- ◆ AI, ML, screen scraping and data portability
- ◆ Antitrust in the era of techlash
- ◆ The CPRA, Virginia, Colorado and Nevada privacy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- ◆ Software copyrightability and fair use after *Google v. Oracle*
- ◆ Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- ◆ TCPA law and litigation after *Facebook v. Duguid* - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- ◆ The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- ◆ Platform moderation and liability, safe harbors, and defenses (including the CDA and DMCA)
- ◆ Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- ◆ The law of SEO and SEM – and its impact on e-commerce vendors
- ◆ Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- ◆ IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi*, patentable subject matter, negative trade secrets, rights of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- ◆ Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- ◆ Sponsored links, embedded links, #hashtags, and internet, mobile and social media advertising
- ◆ Enforcing judgments against foreign domain name registrants
- ◆ Valuing domain name registrations from sales data
- ◆ Applying the First Sale Doctrine to virtual goods
- ◆ Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- ◆ Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- ◆ Click fraud
- ◆ Copyright and Lanham Act fair use
- ◆ Practical tips, checklists and forms that go beyond the typical legal treatise
- ◆ Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ AI/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- ◆ Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- ◆ Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- ◆ Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- ◆ Addresses both law and best practices
- ◆ Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- ◆ Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

Volume 1

Part I. Sources of Internet Law and Practice: A Framework for Developing New Law

- Chapter* 1. Context for Developing the Law of the Internet
2. A Framework for Developing New Law
3. [Reserved]

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Data Scraping, Database Protection, and the Use of Bots and Artificial Intelligence to Gather Content and Information
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names

Volume 2

- Chapter* 8. Internet Patents
9. Unique Intellectual Property Issues in Search Engine Marketing, Optimization and Related Indexing, Information Location Tools and Internet and Social Media Advertising Practices
10. Misappropriation of Trade Secrets in Cyberspace
11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property
12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace
13. Idea Submission, Protection and Misappropriation
- Part III. Licenses and Contracts**
14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: The Federal eSign Statute, Uniform Electronic Transactions Act, UCITA, and the EU Distance Selling Directive
16. Internet Licenses: Rights Subject to License and Limitations Imposed on Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content Licensing Pre-Existing Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements

Volume 3

- Chapter* 24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements
- Part IV. Privacy, Security and Internet Advertising**
25. Introduction to Consumer Protection in Cyberspace
26. Data Privacy
27. Cybersecurity: Information, Network and Data Security
28. Advertising in Cyberspace

Volume 4

- Chapter* 29. Email and Text Marketing, Spam and the Law of Unsolicited Commercial Email and Text Messaging
30. Online Gambling

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. State and Local Sales and Use Taxes on Internet and Mobile Transactions
34. Antitrust Restrictions on Technology Companies and Electronic Commerce
35. Dormant Commerce Clause and Other Federal Law Restrictions on State and Local Regulation of the Internet
36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

Part VI. Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption

37. Defamation, Torts and the Good Samaritan Exemption (47 U.S.C.A. § 230)
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression in Cyberspace

Part VII. Obscenity, Pornography, Adult Entertainment and the Protection of Children

40. Child Pornography and Obscenity
41. Laws Regulating Non-Obscene Adult Content Directed at Children
42. U.S. Jurisdiction, Venue and Procedure in Obscenity and Other Internet Crime Cases

Part VIII. Theft of Digital Information and Related Internet Crimes

43. Detecting and Retrieving Stolen Corporate Data
44. Criminal and Related Civil Remedies for Software and Digital Information Theft
45. Crimes Directed at Computer Networks and Users: Viruses and Malicious Code, Service Disabling Attacks and Threats Transmitted by Email

Volume 5

- Chapter* 46. Identity Theft
47. Civil Remedies for Unlawful Seizures
- Part IX. Liability of Internet Sites and Service (Including Social Networks and Blogs)**
48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Content Moderation and Platform Liability: Service Provider and Website, Mobile App, Network and Cloud Provider Exposure for User Generated Content and Misconduct
50. Cloud, Mobile and Internet Service Provider Compliance with Subpoenas and Court Orders
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites
- Part X. Civil Jurisdiction and Litigation**
52. General Overview of Cyberspace Jurisdiction
53. Personal Jurisdiction in Cyberspace
54. Venue and the Doctrine of Forum Non Conveniens
55. Choice of Law in Cyberspace
56. Internet ADR
57. Internet Litigation Strategy and Practice
58. Electronic Business and Social Network Communications in the Workplace, in Litigation and in Corporate and Employer Policies
59. Use of Email in Attorney-Client Communications

“Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet.”

Jay Monahan

General Counsel, ResearchGate

ABOUT THE AUTHOR

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator in the firm's Silicon Valley Los Angeles and Washington, DC offices. He defends data privacy, cybersecurity breach, AdTech, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database, AI and other intellectual property cases, including disputes involving safe harbors and exemptions, platform liability and fair use.



Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top Intellectual Property litigators in every year the list has been published (2009-2021), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was selected as the Lawyer of the Year for information technology law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. He also serves as Executive Director of Stanford University Law School's Center for the Digital Economy.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

Mr. Ballon is also the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.IanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@IanBallon).

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2022

- > **Antitrust in the era of techlash** (chapter 34)
- > **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- > **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- > **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurity breach, data privacy, AdTech and TCPA class action suits.**
- > **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- > **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- > **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- > **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States*, 141 S. Ct. 1648 (2021)** (ch5)
- > **FOSTA-SESTA and ways to maximize CDA protection** (ch 37)
- > **IP aspects of the use of #hashtags in social media** (ch 6)
- > **The CLOUD Act** (chapter 50)
- > **Virginia, Colorado and Nevada privacy laws** (ch 26)
- > **Applying the single publication rule to websites, links and uses on social media** (chapter 37)
- > **Digital economy litigation strategies**
- > **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- > **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- > **Website and mobile accessibility under the ADA and state laws** (chapter 48)
- > **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- > **Updated *Defend Trade Secrets Act* and UTSA case law** (chapter 10)
- > **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- > **AdTech law** (chapter 28, Darren Abernethy)
- > **The risks of being bound by the CASE Act's ostensibly *voluntary* jurisdiction over small copyright cases**
- > **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- > **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- > **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- > **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 26)
- > **Patent law** (updated by Josh Raskin) (chapter 8)
- > **Idea protection & misappropriation** (ch 13)
- > **Revisiting links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- > **eSIGN case law** (chapter 15)

**SAVE 20% NOW!! To order call 1-888-728-7677
or visit IanBallon.net
enter promo code **WPD20** at checkout**

List Price: \$3,337.00
Discounted Price: \$2,669.60

THE INTERSECTION OF IP LAW AND THE CDA

Excerpted from the forthcoming 2022 updates to Chapter 37 (Defamation, Torts and
the Good Samaritan Exemption (47 U.S.C.A. § 230))

E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition

A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

(These excerpts are unrevised page proofs for the current update and may contain errors. Please
email the author at ballon@gtlaw.com for a complimentary copy of the final published version.)

IP LAW YEAR IN REVIEW

4TH ANNUAL HBCU TECH LAW SUMMIT AND 19TH ANNUAL IP AND SOCIAL JUSTICE CLE SEMINAR

INSTITUTE FOR INTELLECTUAL PROPERTY AND SOCIAL JUSTICE
HOWARD UNIVERSITY SCHOOL OF LAW
MARCH 3-4, 2022

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles: 1840 Century Park East, Ste. 1900 Los Angeles, CA 90067 Direct Dial: (310) 586-6575 Direct Fax: (310) 586-0575	Silicon Valley: 1900 University Avenue, 5th Fl. East Palo Alto, CA 914303 Direct Dial: (650) 289-7881 Direct Fax: (650) 462-7881	Washington, D.C.: 2101 L Street, N.W., Ste. 1000 Washington, D.C. 20037 Direct Dial: (202) 331-3138 Fax: (202) 331-3101
--	---	--

Ballon@gtlaw.com

<www.ianballon.net>

LinkedIn, Twitter, Facebook: IanBallon

This paper has been excerpted from *E-Commerce and Internet Law: Treatise with Forms 2d Edition*
(Thomson West 2022 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (888) 728-7677
www.ianballon.net



Ian C. Ballon

Shareholder

Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal
Circuits

U.S. Supreme Court

JD, LLM, CIPP/US

Ballon@gtlaw.com

LinkedIn, Twitter, Facebook: IanBallon

Los Angeles

1840 Century Park East
Suite 1900

Los Angeles, CA 90067

T 310.586.6575

F 310.586.0575

Silicon Valley

1900 University Avenue
5th Floor

East Palo Alto, CA 94303

T 650.289.7881

F 650.462.7881

Washington, D.C.

2101 L Street, N.W.

Suite 1000

Washington, DC 20037

T 202.331.3138

F 202.331.3101

Ian C. Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice Group and represents internet, mobile, entertainment and technology companies in intellectual property and technology-related litigation and in the defense of data privacy, security breach and TCPA class action suits.

Ian is also the author of the leading treatise on internet and mobile law, [E-Commerce and Internet Law: Treatise with Forms 2d edition](#), the 5-volume set published by West (www.IanBallon.net) and available on Westlaw, which includes extensive coverage of intellectual property law issues. In addition, he serves as [Executive Director of Stanford University Law School's Center for the Digital Economy](#). He also chairs [PLI's annual Advanced Defending Data Privacy, Security Breach and TCPA Class Action Litigation](#) conference. Ian previously served as an Advisor to ALI's Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transactional Disputes (ALI Principles of the Law 2007) and as a member of the consultative group for ALI's Principles of Data Privacy Law (ALI Principles of Law 2020).

Ian was named the Lawyer of the Year for Information Technology Law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of Best Lawyers in America (including lawyer of the year for 2022). In 2020, 2019 and 2018 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder's* 2017 Litigation Departments of the Year Awards. He was also recognized as the 2012 [New Media Lawyer of the Year](#) by the Century City Bar Association. In 2010, he was the recipient of the California State Bar Intellectual Property Law section's [Vanguard Award for significant contributions to the development of intellectual property law](#). Ian was listed in *Variety's* "Legal Impact Report: 50 Game-Changing Attorneys" and has been named by the *LA and San Francisco Daily Journal* as one of the Top 75 intellectual property litigators in California in every year that the list has been published (2009 through 2021), and has been listed as a Northern California Super Lawyer every year from 2004 through 2021 and as one of the top 100 lawyers in California. He is also listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology.

Ian holds JD and LLM degrees and the [CIPP/US certification from the International Association of Privacy Professionals \(IAPP\)](#).

E-COMMERCE & INTERNET LAW

Treatise with Forms—2d Edition

IAN C. BALLON

Volume 4



THOMSON REUTERS®

For Customer Assistance Call 1-800-328-4880

Mat #42478435

37.05[5][B] The Exclusion for “Any Law Pertaining to Intellectual Property”

Section 230(e)(2) provides that “[n]othing in this section shall be construed to limit or expand any law pertaining to intellectual property.”¹ In 2016, Congress enacted the Defend Trade Secrets Act (DTSA),² providing expressly that provisions of that federal law “shall not be construed to be a law pertaining to intellectual property for purposes of any other Act of Congress.”³ Thus, section 230(e)’s exclusion from CDA immunity for *any law pertaining to intellectual property* does not apply to any claim brought under the DTSA. A suit under the DTSA against an interactive computer service provider or user therefore may be preempted to the same extent as any other legal claim that is not excluded from the CDA’s reach by section 230(e).

By contrast, when Congress extended the protections of most aspects of the federal Copyright Act to sound recordings fixed prior to February 15, 1972 (which previously were

[Section 37.05[5][B]]

¹47 U.S.C.A. § 230(e)(2). Intellectual property laws are separately addressed in the following chapters: 4 (Copyright Protection in Cyberspace), 5 (Database Protection), 6 (Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace), 7 (Rights in Internet Domain Names), 8 (Internet Patents), 9 (Intellectual Property Aspects of Information Distribution Systems on the World Wide Web: Caching, Linking and Framing Websites, Content Aggregation, Search Engine Indexing Practices, Key Words and Metatags), 10 (Misappropriation of Trade Secrets in Cyberspace), 11 (Employer Rights in the Creation and Protection of Internet-Related Intellectual Property), 12 (Privacy and Publicity Rights of Celebrities and Others in Cyberspace) and 13 (Idea Misappropriation).

²8 U.S.C.A. §§ 1830 to 1839; *see generally supra* § 10.12[2] (analyzing the statute).

³18 U.S.C.A. §§ 1833 note, 1836 note, 1839 note; Pub L. 114-153 § 2(g), 130 Stat. 376, 382 (May 11, 2016) (“This section and the amendments made by this section shall not be construed to be a law pertaining to intellectual property for purposes of any other Act of Congress.”). This specific provision of the DTSA was codified as a note to sections 1833, 1836 and 1839. At least one court has concurred. *See Craft Beer Stellar, LLC v. Glassdoor, Inc.*, Civil Action No. 18-10510-FDS, 2018 WL 5505247, at *3 (D. Mass. Oct. 17, 2018) (dismissing plaintiff’s DTSA claim against Glassdoor for material posted by a user; “Because Congress has clearly dictated that the DTSA should *not* be construed to be a law ‘pertaining to intellectual property’ for the purposes of *any* other Act of Congress, the DTSA is clearly not such a law for the purposes of § 230(e)(2). The DTSA claim is thus subject to the immunity provisions of § 230, and accordingly that claim will be dismissed.”).

protected, if at all, by state common law or statutes⁴), in the Classics Protection and Access Act (Title II of the Orrin G. Hatch–Bob Goodlatte Music Modernization Act of 2018),⁵ Congress made clear that the provisions of 17 U.S.C.A. § 1401(a), which effectuated this change in the law, are to be considered a “law pertaining to intellectual property” within the meaning of 47 U.S.C.A. § 230(e)(2).⁶ At the same time, the statute provides that the provisions of the Digital Millennium Copyright Act apply to the protections afforded by section 1401(a).⁷ Thus, claims under federal law are excluded from CDA immunity, while common law and state statutory copyright claims were and (to the limited extent that they may still be asserted and are not preempted by the Copyright Act⁸) are subject to CDA preemption in some jurisdictions but not others, as discussed later in this subsection.

For claims arising under other intellectual property laws, there is general agreement that federal intellectual property claims (other than those brought under the DTSA) are excluded, but there is disagreement between the Ninth and Third Circuits (and district court opinions in the First and Second Circuit) over whether state laws pertaining to intellectual property are excluded from the scope of CDA immunity.

Federal intellectual property law claims under any federal law other than the DTSA— such as the Copyright Act, Lanham Act and Patent Act⁹ plainly are excluded from the scope of section 230 preemption.¹⁰ The applicability of the CDA’s Good Samaritan exemption to state intellectual prop-

⁴See *supra* § 4.18[2].

⁵The Orrin G. Hatch–Bob Goodlatte Music Modernization Act, PL 115-264, 2018 H.R. 1551, 132 Stat. 3676 (Oct. 11, 2018).

⁶17 U.S.C.A. § 1401(g).

⁷17 U.S.C.A. §§ 512, 1401(f)(3); *supra* § 4.12.

⁸The scope of preemption of state law claims after enactment of the Music Modernization Act is analyzed in section 4.18[2] in chapter 4.

⁹Federal copyright, trademark and patent laws are addressed in, respectively, chapters 4, 6 and 8. The federal Anti-Cybersquatting Consumer Protection Act, which is largely codified as part of the Lanham Act at 15 U.S.C.A. § 1125(d), is analyzed in chapter 7.

¹⁰See *Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1322 (11th Cir. 2006) (*dicta*); *Ford Motor Co. v. GreatDomains.com, Inc.*, 60 U.S.P.Q.2d 1446, 2001 WL 1176319 (E.D. Mich. Sept. 25, 2001); *Gucci America, Inc. v. Hall & Associates*, 135 F. Supp. 2d 409, 412–13 (S.D.N.Y. 2001) (domain names).

erty law claims (such as those arising under state common law and statutory trade secret,¹¹ right of publicity,¹² copyright,¹³ and trademark¹⁴ laws), however, is subject to conflicting judicial interpretations.

The Ninth Circuit¹⁵ and various district courts¹⁶ have nar-

¹¹See *supra* § 10.12[3] (discussing state law trade secret claims). State and federal trade secret law is analyzed in chapter 10.

¹²State common law and statutory right of publicity laws are analyzed in chapter 12 along with claims under the federal Lanham Act, which generally are excluded from the scope of CDA preemption (except for false advertising claims not based on federal trademark law). See *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1052-54 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020).

¹³See *supra* § 4.18[2] (outlining state common law and statutory copyright claims that are viable in light of the 1976 Copyright Act's broad preemption provision set forth in 17 U.S.C.A. § 301 and the preemption provision of the Music Modernization Act, which is codified at 17 U.S.C.A. § 1401(e)).

¹⁴State trademark claims are addressed in chapter 6.

¹⁵See *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007) (holding that the CDA preempted a state right of publicity claim); see also *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1052-54 (9th Cir. 2019) (applying and expanding on the rationale for *Perfect 10*), *cert. denied*, 141 S. Ct. 13 (2020).

¹⁶See, e.g., *Callahan v. Ancestry.com, Inc.*, Case No. 20-cv-08437-LB, 2021 WL 783524, at *5-6 (N.D. Cal. Mar. 1, 2021) (dismissing plaintiffs' California right of publicity claim under Cal. Civ. Code § 3344, and claims for intrusion upon seclusion, unjust enrichment and unlawful and unfair business practices under Cal. Bus. & Prof. Code § 17200, arising out of defendant's use of their yearbook photos and related information in its subscription database, based on CDA immunity pursuant to 47 U.S.C.A. § 230(c)(1)); *Morton v. Twitter, Inc.*, Case No. CV 20-10434-GW-JEMx, 2021 WL 1181753, at *4-5 (C.D. Cal. Feb. 21, 2021) (dismissing plaintiff's right of publicity claim under Cal. Civ. Code § 3344, and unfair competition, false light invasion of privacy, and other non-copyright claims brought against Twitter by a nude model who alleged that Twitter had failed to suspend or terminate the account of SpyIRL, an online purveyor of pornography that had disseminated her images without authorization in Tweets soliciting subscriptions to its website, where "[a]ll of Morton's non-copyright claims attempt[ed] to treat Twitter as being equivalent to SpyIRL for purposes of considering liability for the latter's tweets."); *Ripple Labs Inc. v. YouTube LLC*, Case No. 20-cv-02747-LB, 2020 WL 6822891, at *6-7 (N.D. Cal. Nov. 20, 2020) (dismissing right of publicity and unfair competition claims arising out of YouTube's alleged failure to remove impersonations of Ripple's cryptocurrency enterprise from its video-sharing platform); *Parker v. Paypal, Inc.*, No. 16-cv-04786, 2017 WL 3508759, at *6-7 (E.D. Pa. Aug. 16, 2017) (dismissing plaintiff's claims for

rowly construed the exclusion in section 230(e)(2) for “any law pertaining to intellectual property” to not reach claims arising under state law and the Ninth Circuit has further held that a false advertising claim under the federal Lanham Act is not a law “pertaining to intellectual property” if the claim at issue is not based on a trademark or other federal intellectual property law.¹⁷ By contrast, the Third Circuit (in a split opinion over a strong dissent) and some district courts outside the Ninth Circuit have held that state IP claims are

unjust enrichment and violations of California’s right of publicity and Pennsylvania’s right to privacy, brought against Amazon.com, and premised on the sale of unauthorized copies of plaintiff’s book on the Kindle store, as barred by the CDA); *Joude v. WordPress Foundation*, No. C 14–01656 LB, 2014 WL 3107441, at *7 (N.D. Cal. July 3, 2014) (applying *Perfect 10* in granting judgment on the pleadings for Automatic on plaintiff’s right of publicity claim arising from user content); *Perfect 10, Inc. v. Giganeews, Inc.*, CV11-07098 AHM SHX, 2013 WL 2109963, at *15-16 (C.D. Cal. Mar. 8, 2013) (dismissing with leave to amend plaintiff’s California right of publicity and unfair competition claims as barred by the CDA because the pornographic images found on defendant’s website that were at issue in the case originated with third parties). A more complete list is provided later in this subsection.

¹⁷See *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1052–54 (9th Cir. 2019) (holding that a false advertising claim under the Lanham Act was not a law “pertaining to intellectual property” under section 230(e); “even though the Lanham Act is known as the federal trademark statute, not all claims brought under the statute involve trademarks.”), *cert. denied*, 141 S. Ct. 13 (2020); see also *Marshall’s Locksmith Service Inc. v. Google, LLC*, 925 F.3d 1263 (D.C. Cir. 2019) (affirming dismissal of the Lanham Act false advertising claims of 14 locksmith companies, which alleged that Google, Microsoft, and Yahoo! had conspired to “flood the market” of online search results with information about so-called “scam” locksmiths, in order to extract additional advertising revenue, based on CDA immunity, where plaintiffs’ theory of liability was premised on third party content (from the scam locksmiths) and defendants merely operated neutral map location services that listed companies based on where they purported to be located, in an opinion that did not address the exclusion for matters “pertaining to intellectual property” set forth in section 230(e)(2)); *Enhanced Athlete Inc. v. Google LLC*, Case No. 19-cv-08260-HSG, 2020 WL 4732209, at *2-4 (N.D. Cal. Aug. 14, 2020) (applying *Enigma Software* in dismissing (with prejudice) plaintiff’s Lanham Act and California unfair competition claims, as barred by the CDA, because they arose out of defendant’s removal of third party fitness and health videos); *Corker v. Costco Wholesale Corp.*, No. C19-0290RSL, 2019 WL 5895430, at *6 (W.D. Wash. Nov. 12, 2019) (applying *Enigma Software* in dismissing plaintiff’s section 43(a)(1)(A) false association claim against the retailer defendants as “barred by the CDA to the extent their conduct is limited to making a product available for sale on a website.”).

laws “pertaining to intellectual property” and, therefore, the CDA does not insulate interactive computer service providers or users for claims brought under those laws, even if they otherwise might be entitled to its protections for other claims.¹⁸

The Ninth Circuit approach construes section 230(e)(2) narrowly as an exception to a provision granting broad immunity, and relies on one of the stated policy objectives codified in section 230(b). Courts that have expressly declined to follow the Ninth Circuit, by contrast, focused on the language and structure of section 230(e) to reach the opposite conclusion.¹⁹

¹⁸See *Hepp v. Facebook, Inc.*, 14 F.4th 204, 211-15 (3d Cir. 2021) (rejecting the Ninth Circuit’s analysis by a 2-1 majority over a strong dissent, holding that plaintiff’s state law right of publicity claim was not preempted by the CDA because “Section 230 does not preclude claims based on state intellectual property laws.”); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 298-304 (D.N.H. 2008) (declining to dismiss plaintiff’s right of publicity claim under New Hampshire law, holding that the plain text of the statute excludes any claim pertaining to intellectual property and severely criticizing the Ninth Circuit’s ruling in *Perfect 10*); *Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 702-04 (S.D.N.Y. 2009) (construing the language of the statute the same way as the court in *Doe* and allowing a common law copyright claim under New York law to proceed); see also *Universal Communication Systems, Inc. v. Lycos, Inc.*, 478 F.3d 413, 422-23 (1st Cir. 2007) (holding, without much analysis, that a claim for trademark infringement under Florida state law, Fla. Stat. § 495.151, was “not subject to section 230 immunity.”); *Ohio State Univ. v. Skreened Ltd.*, 16 F. Supp. 3d 905, 918 (S.D. Ohio 2014) (holding, without much analysis, that the CDA did not preempt plaintiff’s Ohio right of publicity claim).

¹⁹Compare *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), cert. denied, 522 U.S. 1062 (2007) (holding that the CDA preempted a state right of publicity claim); *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1052-54 (9th Cir. 2019) (holding that a false advertising claim under the Lanham Act was not a law “pertaining to intellectual property” under section 230(e)), cert. denied, 141 S. Ct. 13 (2020); with *Hepp v. Facebook, Inc.*, 14 F.4th 204, 211-12 (3d Cir. 2021) (rejecting the Ninth Circuit’s analysis, holding, in a 2-1 ruling over a strong dissent, that plaintiff’s state law right of publicity claim was not preempted by the CDA; “Facebook and its amici offer arguments based on the statute’s text and policy considerations. But there are strong textual and policy arguments to the contrary. Because we adhere to the most natural reading of § 230(e)(2)’s text, we hold that § 230(e)(2) is not limited to federal laws. Simply put, a state law can be a “law pertaining to intellectual property,” too.”); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 298-304 (D.N.H. 2008) (declining to dismiss plaintiff’s right of publicity claim under New Hampshire law, holding that the plain text of the

Section 230(e), as originally enacted, set out four separate provisions (which remain part of the statute today along with a fifth provision that subsequently was added as part of FOSTA/SESTA to address sex trafficking), which address the effect of the Good Samaritan exemption on other laws.²⁰ The immunity created by section 230 does not apply to “[f]ederal criminal statute[s],”²¹ “any law[s] pertaining to intellectual property,”²² or the federal Electronic Communications Privacy Act²³ “or any similar State law.”²⁴ Section 230(e) also provides that where applicable, the Good Samaritan exemption expressly preempts inconsistent state laws²⁵ (although it does not preempt those state laws that are “consistent” with its provisions).²⁶

The CDA excludes “any law pertaining to intellectual prop-

statute excludes any claim pertaining to intellectual property and severely criticizing the Ninth Circuit’s ruling in *Perfect 10*); *Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 702-04 (S.D.N.Y. 2009) (construing the literal language of the statute the same way as the court in *Doe* and allowing a common law copyright claim under New York law to proceed).

²⁰Section 230(e)(5), which was added just over 22 years later, in 2018, creates specific exclusions from some but not all of the immunities created by section 230(c), for certain federal civil claims and state law criminal charges relating to sex trafficking. *See infra* § 37.05[5][C]. While section 230(e)(2), which excludes any law pertaining to intellectual property, and section 230(e)(3), which provides that the CDA preempts inconsistent state laws, arguably leave unclear which of those two provisions should take precedence with respect to state laws pertaining to intellectual property, the exclusions relating to sex trafficking laws that are set forth in section 230(e)(5) specify that the immunity created by section 230(c)(2)(A) (for good faith actions undertaken to restrict access to certain adult material) may provide a defense for interactive computer service providers and users for the enumerated civil federal and state criminal sex trafficking claims listed in section 230(e)(5), but the defenses created by other sections of the CDA (such as the immunity for republication in section 230(c)(1) and for blocking and filtering technologies in section 230(c)(2)(B)) are inapplicable. *See* 47 U.S.C.A. § 230(e).

²¹47 U.S.C.A. § 230(e)(1).

²²47 U.S.C.A. § 230(e)(2).

²³47 U.S.C.A. § 230(e)(4); *see generally supra* § 37.05[1][A].

²⁴47 U.S.C.A. § 230(e)(4).

²⁵47 U.S.C.A. § 230(e)(3) (“No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.”).

²⁶The statute does not “prevent any State from enforcing any State law that is consistent with this section.” 47 U.S.C.A. § 230(e)(3); *see generally supra* § 37.05[1] (discussing Virginia, California and other state statu-

erty,”²⁷ which on its face suggests that the Good Samaritan exemption does not apply to either federal or state IP laws. The word *any* suggests a broad interpretation, as does the term *pertaining to* intellectual property, rather than simply intellectual property laws or more narrowly *federal* intellectual property laws (or even the Copyright Act, Lanham Act and Patent Act). This view is bolstered by Congress’s use of the term “federal” in discussing other exclusions under the statute. Subpart 230(e)(1) makes clear that the exemption has no effect on any “Federal criminal statute.” Had Congress intended to exclude only federal intellectual property claims presumably it would have used the same language in subpart (e)(2) that it did in subpart (e)(1), rather than more expansively excluding “*any* law pertaining to intellectual property.”

The structure and language of section 230(e) likewise arguably suggests that Congress intended to exclude *any* law pertaining to intellectual property (both federal and state), and not merely *federal* intellectual property laws. As previously noted, section 230(e) originally contained only the first

tory provisions that create equivalent exemptions under state law); *infra* § 51.04[2][A] (addressing revenge porn statutes enacted in Arizona, Colorado, Florida, Illinois, Indiana, Maine, Maryland, Michigan, Minnesota, Nebraska, Nevada, New Hampshire, New Mexico, North Carolina, Oklahoma, Oregon, Rhode Island, Texas, Utah, Vermont, Washington, and Wisconsin, which contain CDA-like protections for interactive computer service providers).

As stated in the statute, the purpose of 47 U.S.C.A. § 230 is to promote the development of the Internet and other interactive computer services and media, preserve the free market for the Internet and online services without state or federal government regulation, encourage the development of technologies that maximize user control over what information is received by users, remove disincentives for the development and use of blocking and filtering technologies that parents may use to restrict children’s access to objectionable or inappropriate online material and ensure the enforcement of federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer. 47 U.S.C.A. § 230(b).

²⁷47 U.S.C.A. § 230(e)(2) (emphasis added). As noted earlier in this subsection, Congress, in 2016, in the Defend Trade Secrets Act, and in 2018, in the Music Modernization Act, made express determinations about whether those laws should (in the case of the Music Modernization Act) or should not (in the case of the Defend Trade Secrets Act) be construed under section 230(e) as laws “pertaining to intellectual property.” The discussion here focuses on what Congress intended with respect to other state and federal laws arguably pertaining to intellectual property, when the law was first enacted in 1996.

four sub-parts (which, along with a fifth subpart added in 2018 to address sex trafficking claims, remain part of the statute today). Subpart (e)(1) excludes federal criminal laws, while subpart (e)(3) provides that inconsistent state laws are preempted but consistent state laws are not. Subpart (e)(4) refers to both federal and state laws in providing that “[n]othing in this section shall be construed to limit the application of the Electronic Communications Privacy Act . . . or any similar State law.” Viewed in this context—where each of the other three subparts expressly refer to state or federal law—or both—the use in section 230(e)(2) of “*any law* pertaining to intellectual property” without reference to either state or federal law strongly suggests that Congress intended to exclude all intellectual property laws, and not merely federal ones. Subpart 230(e)(5), which was added in 2018, likewise delineates its application to certain federal civil claims (in section 230(e)(5)(A)) and certain state criminal law charges (in sections 230(e)(5)(B) and 230(e)(5)(C)).

An analysis based only the text of section 230(e), without regard to the policy goals enacted as part of section 230(b), requires consideration of whether the subparts of section 230(e), captioned “[e]ffect on other laws,” constitute independent provisions, or whether they modify one another. If they are independent, the Good Samaritan exemption has no effect on federal criminal laws (subpart (1)), no effect on any law pertaining to intellectual property (subpart (2)), no effect on claims under the Electronic Communications Privacy Act or similar state laws (subpart (4)) and no effect on state laws that are consistent with the exemption (subpart (3)), but otherwise preempts all other state law civil and criminal provisions (i.e., state law claims other than IP claims, provisions consistent with the Good Samaritan exemption and state laws similar to the ECPA) and provides immunity in federal civil cases other than those arising under the ECPA. This possible interpretation is also consistent with the 2018 amendment to section 230, which creates exclusions for certain federal civil claims and state criminal charges relating to sex trafficking (although only for some parts of section 230—unlike the original four exclusions, subpart 230(e)(5) does not create an exclusion for the immunity created by section 230(c)(2)(A) (for actions undertaken in good faith to restrict access to or the availability of certain adult

content)).²⁸

The Ninth Circuit has held that, to effectuate the CDA’s “express policy of providing broad immunity . . .,” the exclusion in section 230(e)(2) should be construed narrowly.²⁹

Section 230, after all, codifies particular policy objectives in subsection 230(b) to guide its construction by courts.

In *Perfect 10, Inc. v. CCBill, Inc.*,³⁰ the Ninth Circuit construed the term “intellectual property” to mean “federal intellectual property” (which was prior to the enactment of the DTSA, a federal law that (as previously noted) is expressly exempted from section 230(e)’s exclusion, and thus potentially subject to CDA immunity) and ruled that the plaintiff’s California right of publicity claim against an Internet payment processor was preempted.³¹ Consequently, in the Ninth Circuit (and district courts that follow this approach) the CDA will be construed to preempt state law intellectual property claims, including right of publicity, common law trademark infringement and dilution and state trade secret misappropriation claims, among others,³² provided the content originated with a third party information content

²⁸See 47 U.S.C.A. § 230(e)(5); see generally *infra* § 37.05[5][C].

²⁹*Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1053 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020).

³⁰*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

³¹*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118–19 (9th Cir.), *cert. denied*, 522 U.S. 1062 (2007).

³²See, e.g., *Callahan v. Ancestry.com, Inc.*, Case No. 20-cv-08437-LB, 2021 WL 783524, at *5-6 (N.D. Cal. Mar. 1, 2021) (dismissing plaintiffs’ California right of publicity claim under Cal. Civ. Code § 3344, and claims for intrusion upon seclusion, unjust enrichment and unlawful and unfair business practices under Cal. Bus. & Prof. Code § 17200, arising out of defendant’s use of their yearbook photos and related information in its subscription database, based on CDA immunity pursuant to 47 U.S.C.A. § 230(c)(1)); *Morton v. Twitter, Inc.*, Case No. CV 20-10434-GW-JEMx, 2021 WL 1181753, at *4-5 (C.D. Cal. Feb. 21, 2021) (dismissing plaintiffs’ right of publicity claim under Cal. Civ. Code § 3344, and unfair competition, false light invasion of privacy, and other non-copyright claims brought against Twitter by a nude model who alleged that Twitter had failed to suspend or terminate the account of SpyIRL, an online purveyor of pornography that had disseminated her images without authorization in Tweets soliciting subscriptions to its website); *Ripple Labs Inc. v. YouTube LLC*, Case No. 20-cv-02747-LB, 2020 WL 6822891, at *6-7 (N.D. Cal. Nov. 20, 2020) (dismissing right of publicity and unfair competition claims arising out of YouTube’s alleged failure to remove impersonations of Ripple’s cryptocurrency enterprise from its video-sharing platform); *Lasoff v.*

Amazon.com Inc., Case No. C-151 BJR, 2017 WL 372948, at *3-4 (W.D. Wash. Jan. 26, 2017) (granting summary judgment for the defendant on plaintiff's New Jersey state law claims for, among other things, statutory and common law unfair competition and statutory trademark infringement, based on CDA preemption, in a case arising out of Amazon.com's alleged use of his mark in sponsored links advertisements), *aff'd on other grounds*, 741 F. App'x 400 (9th Cir. 2018); *Free Kick Master LLC v. Apple Inc.*, 140 F. Supp. 3d 975, 982-83 (N.D. Cal. 2015) (dismissing plaintiff's common law trademark infringement claim against Google Play and the Amazon AppStore, arising out of free apps they made available, as preempted by the CDA, where plaintiff did not allege that "either of them had any role whatsoever in the creation of the apps at issue, the choice of name for those apps, or any other action that would place either defendant in the role of speaker or author of the accused products."); *Parker v. Paypal, Inc.*, No. 16-cv-04786, 2017 WL 3508759, at *6-7 (E.D. Pa. Aug. 16, 2017) (dismissing plaintiff's claims for unjust enrichment and violations of California's right of publicity and Pennsylvania's right to privacy, brought against Amazon.com, and premised on the sale of unauthorized copies of plaintiff's book on the Kindle store, as barred by the CDA); *Joude v. WordPress Foundation*, No. C 14-01656 LB, 2014 WL 3107441, at *7 (N.D. Cal. July 3, 2014) (applying *Perfect 10* in granting judgment on the pleadings for Automattic on plaintiff's right of publicity claim arising from user content); *Parts.com, LLC v. Yahoo! Inc.*, 996 F. Supp. 2d 933, 938-39 (S.D. Cal. 2013) (dismissing with prejudice state law claims for trademark infringement and dilution and unfair competition as preempted by the CDA); *Evans v. Hewlett-Packard Co.*, C 13-02477 WHA, 2013 WL 4426359, at *2-3 (N.D. Cal. Aug. 15, 2013) (dismissing Pennsylvania unfair competition and trademark infringement and Pennsylvania and California right of publicity claims brought against the operators of the HP App Catalogue, an App store for Palm devices, as preempted by the CDA, because, although "cleverly-worded," the complaint did "not allege that defendants created the app at issue here. Rather, it appears that the app was created entirely by third parties."); *Evans v. Hewlett-Packard Co.*, No. C 13-02477, 2013 WL 5594717 (N.D. Cal. Oct. 10, 2013) (denying plaintiffs' motion to amend the complaint to "plead around the CDA" by alleging that the defendants did not merely operate an App store for apps used on Palm devices but actually developed the allegedly infringing "Chubby Checker" App, holding that plaintiffs' proposed, amended California and Pennsylvania state law trademark, unfair competition, right of publicity, and emotional distress claims were preempted by section 230); *Stevo Design, Inc. v. SBR Mktg. Ltd.*, 919 F. Supp. 2d 1112, 1128 (D. Nev. 2013) (holding that a sports betting website operator was immune from state law claims for misappropriation of trade secrets, misappropriation of licensable commercial property, civil theft, and tortious interference with contractual relations, because it was not a "developer" of user-generated content under the CDA, even though it awarded loyalty points for user posts); *Perfect 10, Inc. v. Giganeews, Inc.*, CV11-07098 AHM SHX, 2013 WL 2109963, at *15-16 (C.D. Cal. Mar. 8, 2013) (applying *CCBill* in dismissing with leave to amend plaintiff's California right of publicity and unfair competition claims as barred by the CDA because the pornographic images found on defendant's website originated with third parties). *But see Cybersitter*,

provider and was not created or developed by the defendant itself.³³

In *CCBill*, the Ninth Circuit spent most of the opinion on issues of first impression under the Digital Millennium Copyright Act,³⁴ giving short shrift to its holding that the plaintiff's California right of publicity claim was preempted by the Good Samaritan exemption. Judge Milan Smith, Jr., writing for the panel, explained that:

While the scope of federal intellectual property law is relatively well-established, state laws protecting 'intellectual property,' however defined, are by no means uniform. Such laws may bear various names, provide for varying causes of action and remedies, and have varying purposes and policy goals. Because material on a website may be viewed across the Internet, and thus in more than one state at a time, permitting the reach of any particular state's definition of intellectual property to dictate the contours of this federal immunity would be contrary to Congress's expressed goal of insulating the

LLC v. Google, Inc., 905 F. Supp. 2d 1080, 1086–87 (C.D. Cal. 2012) (narrowly applying the CDA without much analysis in denying in part the defendant's motion to dismiss and holding that the CDA preempted claims for state law trademark infringement, contributory infringement pursuant to Cal. Bus. & Prof. Code § 14245(a)(3) and unfair competition under Cal. Bus. & Prof. Code § 17200, based on the contents of advertisements, to the extent not developed by the defendant, but not claims arising out of the alleged sale of plaintiff's "Cybersitter" mark as a key word to trigger sponsored link advertisements).

³³*See, e.g., Stevo Design, Inc. v. SBR Mktg. Ltd.*, 968 F. Supp. 2d 1082, 1090-91 (D. Nev. 2013) (denying the defendant's motion to dismiss plaintiff's amended complaint where plaintiff alleged that the website provider "acted as a 'developer' within the meaning of the CDA by promoting the publication of protected 'service plays' and thereby contributing to the misappropriation of Plaintiffs' trade secrets and commercial property."); *Cybersitter, LLC v. Google, Inc.*, 905 F. Supp. 2d 1080, 1086–87 (C.D. Cal. 2012) (denying in part the defendant's motion to dismiss and holding that the CDA preempted claims for state law trademark infringement, contributory infringement pursuant to Cal. Bus. & Prof. Code § 14245(a)(3) and unfair competition under Cal. Bus. & Prof. Code § 17200, based on the contents of advertisements, to the extent not developed by the defendant, but not claims arising out of the alleged sale of plaintiff's "Cybersitter" mark as a key word to trigger sponsored link advertisements); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 801-02 (N.D. Cal. 2011) (denying Facebook's motion to dismiss plaintiff's right of publicity claim arising out of the use of user names and images in connection with advertisements for pages that users "liked" on Facebook because the court concluded that the advertisements, which were comprised of user content, had been developed by Facebook).

³⁴17 U.S.C.A. § 512(c); *see generally supra* § 4.12 (analyzing the statute and discussing the case).

development of the Internet from the various state-law regimes.³⁵

More than a decade later, in *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*,³⁶ the Ninth Circuit held that “the intellectual property exception contained in § 230(e)(2) encompasses claims pertaining to an established intellectual property right under federal law, like those inherent in a patent, copyright, or trademark.”³⁷ Accordingly, the panel held that the exception does not apply “to false advertising claims brought under § 1125(a) of the Lanham Act, unless the claim itself involves intellectual property.”³⁸ The D.C. Circuit, in a different case, also found plaintiffs’ Lanham Act false advertising claim precluded by the CDA, albeit in an opinion that did not address the exclusion created by section 230(e)(2).³⁹

In *Enigma Software*, the Ninth Circuit explained its analysis as follows:

We have observed before that because Congress did not define the term “intellectual property law,” it should be construed narrowly to advance the CDA’s express policy of providing broad immunity. See *Perfect 10*, 488 F.3d at 1119. One of these express policy reasons for providing immunity was, as Congress stated in § 230(b)(2), “to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.” 47 U.S.C. § 230(b)(2). The intellectual property exception is a limitation on immunity, and the CDA’s

³⁵*Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

³⁶*Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040 (9th Cir. 2019), cert. denied, 141 S. Ct. 13 (2020).

³⁷*Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1053 (9th Cir. 2019), cert. denied, 141 S. Ct. 13 (2020).

³⁸*Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1053 (9th Cir. 2019), cert. denied, 141 S. Ct. 13 (2020).

³⁹See *Marshall’s Locksmith Service Inc. v. Google, LLC*, 925 F.3d 1263 (D.C. Cir. 2019) (affirming dismissal of the Lanham Act false advertising claims of 14 locksmith companies, which alleged that Google, Microsoft, and Yahoo! had conspired to “flood the market” of online search results with information about so-called “scam” locksmiths, in order to extract additional advertising revenue, based on CDA immunity, where plaintiffs’ theory of liability was premised on third party content (from the scam locksmiths) and defendants merely operated neutral map location services that listed companies based on where they purported to be located, in an opinion that did not discuss or consider the exclusion in section 230(e)(2) for claims “pertaining to intellectual property”).

stated congressional purpose counsels against an expansive interpretation of the exception that would diminish the scope of immunity. If the intellectual property law exception were to encompass any claim raised under the Lanham Act—including false advertising claims that do not directly involve intellectual property rights—it would create a potential for new liability that would upset, rather than “preserve” the vibrant culture of innovation on the internet that Congress envisioned.⁴⁰

Subsequent district court opinions have also applied *Enigma Software* to hold interactive computer service providers immune under the CDA from false advertising claims that are not premised on federal trademark infringement.⁴¹ A district court within the Ninth Circuit also held that a plaintiff’s section 43(a)(1)(A) Lanham Act false association claim against retailer defendants was barred by the CDA to the extent their conduct was limited to making a product available for sale on a website (but not for certain acts undertaken by them in the physical world).⁴²

While other courts have not challenged the Ninth Circuit’s analysis of the CDA’s potential applicability to Lanham Act false advertising claims that are not based on use of a trademark, the Third Circuit, in a 2-1 ruling over a vigorous dissent, disagreed with the Ninth Circuit’s holding in *Perfect 10* that CDA immunity potentially applies to state IP claims,

⁴⁰*Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 946 F.3d 1040, 1053 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020).

⁴¹*See, e.g., Enhanced Athlete Inc. v. Google LLC*, Case No. 19-cv-08260-HSG, 2020 WL 4732209, at *2-4 (N.D. Cal. Aug. 14, 2020) (dismissing (with prejudice) plaintiff’s Lanham Act and California unfair competition claims, as barred by the CDA, because they arose out of defendant’s removal of fitness and health videos containing information about unregulated substances that had not yet been approved by the FDA).

⁴²*See Corker v. Costco Wholesale Corp.*, No. C19-0290RSL, 2019 WL 5895430, at *6 (W.D. Wash. Nov. 12, 2019) (dismissing plaintiff’s section 43(a)(1)(A) false association claim against the retailer defendants as “barred by the CDA to the extent their conduct is limited to making a product available for sale on a website.”). As the court explained,

plaintiffs’ claims in this case do not involve an intellectual property right or trademark: the false association claim that survives this motion to dismiss does not, therefore, fall within the CDA’s intellectual property exception to immunity under the analysis recently adopted by the Ninth Circuit in *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, 938 F.3d 1026, 1038-39 (9th Cir. 2019) (noting that Section 43(a) is one of the few provisions of the Lanham Act that goes beyond trademark protection and holding that a claim of false advertising is barred by the CDA unless it involves an intellectual property right).

2019 WL 5895430, at *6.

holding, in *Hepp v. Facebook, Inc.*⁴³ that a Pennsylvania state law right of publicity claim was not preempted by the CDA because “Section 230 does not preclude claims based on state intellectual property laws.”⁴⁴ The majority in *Hepp* characterized *Perfect 10* as resting on “the statute’s text and policy considerations. But there are strong textual and policy arguments to the contrary. Because we adhere to the most natural reading of § 230(e)(2)’s text, we hold that § 230(e)(2) is not limited to federal laws. Simply put, a state law can be a ‘law pertaining to intellectual property,’ too.”⁴⁵ Judge Robert Cowen, dissenting in relevant part, wrote that section 230(e)(2) is best understood as excluding from the CDA’s reach only federal intellectual property claims (or, at most, state law claims that are co-extensive with federal claims, such as state trademark law causes of action) based on the Congressional findings and policy objectives expressly set forth in the statute itself, in sections 230(a) and 230(b).⁴⁶ Judge Cowen observed that state IP laws vary from state to state and what even constitutes an IP claim under state law is not always clear. He elaborated that “[t]he application of § 230(e)(2) to various state ‘intellectual property’ laws would be inconsistent with the objectives of § 230. . . . ‘state laws protecting ‘intellectual property,’ however defined, are by no means uniform,’ with such laws bearing various names (e.g., trademark, unfair competition, dilution, and right of publicity), legal elements, remedies, and purposes. . . . Such confusion is only magnified by the fact that ‘material on a website may be viewed across the Internet, and thus in more than one state at a time,’ and ‘defendants that are otherwise entitled to CDA immunity will usually be subject to the law of numerous states.’”⁴⁷ Judge Cowen wrote that “[t]his web of inconsistent state laws is the very definition of the ‘fetter-

⁴³*Hepp v. Facebook, Inc.*, 14 F.4th 204 (3d Cir. 2021).

⁴⁴*Hepp v. Facebook, Inc.*, 14 F.4th 204, 211-15 (3d Cir. 2021).

⁴⁵*Hepp v. Facebook, Inc.*, 14 F.4th 204, 211-15 (3d Cir. 2021).

⁴⁶*Hepp v. Facebook, Inc.*, 14 F.4th 204, 216-26 (3d Cir. 2021) (Cowen, J. dissenting in relevant part). Judge Cowen’s reference to federal claims tracks the Ninth Circuit’s analysis in *Perfect 10* and should be understood as referencing federal claims other than the Defend Trade Secrets Act. *Perfect 10* was decided before Congress enacted the DTSA, which expressly provides for CDA immunity to DTSA claims, where applicable.

⁴⁷*Hepp v. Facebook, Inc.*, 14 F.4th 204, 222 (3d Cir. 2021) (Cowen, J. dissenting in relevant part), quoting *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1118-19 & n.5 (9th Cir.), cert. denied, 522 U.S. 1062 (2007).

ing’ state regulation that Congress sought to avoid in enacting Section 230.”⁴⁸ Nevertheless, the two judge majority prevailed (although, as of the time this update went to press, the opinion potentially could be subject to *en banc* review or a petition for *certiorari* to the U.S. Supreme Court).

Between 2007, when *CCBill* was decided, and 2021, when the Third Circuit issued its opinion in *Hepp*, no other circuit court had ruled on the CDA’s potential applicability to state IP claims. *CCBill*, however, had been criticized in two district opinions from outside the Ninth Circuit for ignoring the structure of section 230(e). In *Doe v. Friendfinder Network, Inc.*,⁴⁹ a district court opinion from New Hampshire, Judge Joseph N. LaPlante denied the defendant’s motion to dismiss claims for false advertising and false designation of origin under the Lanham Act and violations of the plaintiff’s right of publicity under New Hampshire law, but dismissed plaintiff’s other state law claims under the Good Samaritan exemption. He ruled that the language of section 230(e)(2) was clear and did not suggest any limitation to *federal* intellectual property law. In addition, the use of the expansive modifier *any* offered no indication that Congress intended a limiting construction of the statute.⁵⁰

Judge LaPlante wrote that “[t]he Ninth Circuit made no attempt to reckon with the presence of the term ‘any’—or for that matter, the absence of the term ‘federal’—in section 230(e)(2) when limiting it to federal intellectual property laws.”⁵¹ He further criticized the Ninth Circuit for failing to “make any effort to reconcile its reading of section 230(e)(2) with other limiting provisions of section 230 which specifically identify federal or state law as such The content of these provisions indicates that, where Congress wished to

⁴⁸*Hepp v. Facebook, Inc.*, 14 F.4th 204, 222 (3d Cir. 2021) (Cowen, J. dissenting in relevant part) (quoting Facebook’s Brief and 47 U.S.C.A. § 230(b)(2)).

⁴⁹*Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D.N.H. 2008).

⁵⁰See *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 299 (D.N.H. 2008). He wrote that “[s]tatutory interpretation begins with the language of the statute. Where . . . that language is clear and ambiguous, the inquiry is at an end.” *Id.* quoting *Ruiz v. Bally Total Fitness Holding Corp.*, 496 F.3d 1, 8 (1st Cir. 2007), citing *United States v. Ron Pair Enterprises, Inc.*, 489 U.S. 235, 241 (1989).

⁵¹*Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 299 (D.N.H. 2008).

distinguish between state and federal law in section 230, it knew how to do so.”⁵² Judge LaPlante explained:

[T]he use of “any” in § 230(e)(2), in contrast to the use of “federal” elsewhere in the CDA, suggests that Congress did not intend the terms to be read interchangeably. “It is well settled that where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.” *Duncan v. Walker*, 533 U.S. 167, 173, 121 S. Ct. 2120, 150 L. Ed. 2d 251 (2001) (internal quotation marks and bracketing omitted) (declining to read “federal” into section of statute where it did not appear because Congress had “denominat[ed] expressly both ‘State’ and ‘Federal’ . . . in other parts of the same statute”)⁵³

Finally, Judge LaPlante criticized the Ninth Circuit’s rationale for construing “intellectual property” to mean “federal intellectual property”—Congress’s expressed goal of insulating the development of the Internet from the various state-law regimes—writing that “[h]owever salutary this ‘goal’ might be on its own merits, it is not among those ‘expressed’ in § 230.”⁵⁴

Other cases had previously discussed⁵⁵ the issue or held without specifically analyzing that state intellectual prop-

⁵²*Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 299–300 (D.N.H. 2008).

⁵³*Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 300 (D.N.H. 2008).

⁵⁴*Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288, 300 (D.N.H. 2008).. He explained that:

While the text of § 230 identifies one of its purposes as freeing the Internet from “government regulation,” 47 U.S.C.A. § 230(a)(4), this plain language restricts regulation by any government, not just those of the states. One of § 230’s announced policies, in fact, is “to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation.” *Id.* § 230(b)(2) (emphasis added) As the presence of § 230(e)(2) indicates, however, Congress also believed that laws protecting intellectual property rights should nevertheless remain in effect—that the potential costs to those rights, in essence, outweighed the benefits of the alternative.

Id. The court further wrote that “while Congress often acts to protect interstate commerce from the burden of nonuniform state laws, there is nothing in the language of section 230 effecting that protection here. ‘Courts are not free to disregard the plain language of a statute and, instead, conjure up legislative purposes and intent out of thin air’ under the guise of statutory interpretation.” *Id.*, quoting *Ruiz v. Bally Total Fitness Holding Corp.*, 496 F.3d 1, 8 (1st Cir. 2007) (footnote omitted).

⁵⁵See *Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1320–24 (11th Cir.

erty claims, like federal intellectual property claims, are excluded from section 230 and are not preempted.⁵⁶

In *Atlantic Recording Corp. v. Project Playlist, Inc.*,⁵⁷ Second Circuit Judge Denny Chin, while he was still a Southern District of New York district court judge, reached the same conclusion as Judge LaPlante, in denying defendant's motion to dismiss state law claims for common law copyright infringement and unfair competition under New York law. Project Playlist, a site that created links to music files found on the Internet, had been sued by major record labels for copyright infringement and state law claims.

Judge Chin held that the plain text of section 230(e) was clear in excluding *any* law pertaining to intellectual property and characterized the Ninth Circuit's ruling in *Perfect 10* as rooted "not in the text of the statute but the public policy underlying it."⁵⁸ He explained:

The problem with Playlist's argument is that it lacks any support in the plain language of the CDA. In four different points in section 230(e), Congress specified whether it intended a subsection to apply to local, state, or federal law. *See* 47 U.S.C. § 230(e)(1) ("any other *Federal* criminal statute"), (3) ("any *State* law" and "any *State* or *local* law"), (4) ("any similar *State* law") (emphasis added in all). It is therefore clear from the statute that if Congress wanted the phrase "any law pertaining to intellectual property" to actually mean "any *federal* law pertaining to intellectual property," it knew how to make that clear, but chose not to.⁵⁹

By contrast, he noted that "[t]he Ninth Circuit did not

2006) (suggesting in *dicta* that section 230(e)(2) would not preempt a right of publicity claim). The court's discussion in *Almeida*, however, was based in part on the lower court opinion in *Perfect 10* that was subsequently reversed on this very point by the Ninth Circuit and therefore has little value even as *dictum*.

⁵⁶*See Universal Communication Systems, Inc. v. Lycos, Inc.*, 478 F.3d 413, 422–23 (1st Cir. 2007) (holding a claim for trademark infringement under Florida state law, Fla. Stat. § 495.151, "not subject to section 230 immunity.").

⁵⁷*Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690 (S.D.N.Y. 2009).

⁵⁸*Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 703 (S.D.N.Y. 2009) (characterizing Project Playlist's argument, which "relie[d] heavily" on *Perfect 10*).

⁵⁹*Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 703 (S.D.N.Y. 2009) (footnote omitted; emphasis in original).

engage in a textual analysis in *Perfect 10*.⁶⁰

Judge Chin explained that “the modifier ‘any’ in section 230(e)(2), employed without any limiting language, ‘amounts to’ expansive language [that] offers no indication whatsoever that Congress intended [a] limiting construction.”⁶¹ Further, he wrote that this conclusion was “bolstered by the fact that . . . the ‘surrounding statutory language’ [discussed above] supports the conclusion that Congress intended the word ‘any’ to mean any state or federal law pertaining to intellectual property.”⁶² Because “the plain language of the CDA is clear, as ‘any law’ means both state and federal law,” Judge Chin concluded, “the Court need not engage in an analysis of the CDA’s legislative history or purpose.”⁶³

Judge Chin’s analysis was subsequently followed by a state court trial judge in New York, in granting the plaintiff’s motion to dismiss the defendant’s CDA affirmative defense in a common law copyright infringement suit.⁶⁴ Other courts have similarly held that the CDA does not preempt state law IP claims.⁶⁵

Given the sharp divergence of views on the proper scope of section 230(e)’s exclusion for any law pertaining to intellectual property, some courts have been disinclined to find right of publicity or other state I.P. claims necessarily preempted, at least at an early stage in the proceedings, and have found ways to decide pending motions without having

⁶⁰*Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 704 n.11 (S.D.N.Y. 2009).

⁶¹*Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 704 (S.D.N.Y. 2009), quoting *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D.N.H. 2008), quoting *Harrison v. PPG Industries, Inc.*, 446 U.S. 578, 589 (1980).

⁶²*Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 704 (S.D.N.Y. 2009), quoting *American Civil Liberties Union v. Department of Defense*, 543 F.3d 59, 69 (2d Cir. 2008) (holding that the word any in a statute “deserves an expansive application where the surrounding statutory language and other relevant legislative context support it.”).

⁶³*Atlantic Recording Corp. v. Project Playlist, Inc.*, 603 F. Supp. 2d 690, 704 (S.D.N.Y. 2009).

⁶⁴See *UMG Recordings, Inc. v. Escape Media Group, Inc.*, 948 N.Y.S. 881, 888-89 (N.Y. Sup. Ct. 2012), rev’d on other grounds, 107 A.D.3d 51, 964 N.Y.S.2d 106 (N.Y. App. 2013).

⁶⁵See, e.g., *Ohio State Univ. v. Skreened Ltd.*, 16 F. Supp. 3d 905, 918 (S.D. Ohio 2014) (holding, without much analysis, that the CDA did not preempt plaintiff’s Ohio right of publicity claim).

to reach the issue.⁶⁶

⁶⁶See, e.g., *Doe No. 1 v. Backpage.com, LLC*, 817 F.3d 12, 26-27 & n.9 (1st Cir. 2016) (affirming dismissal of plaintiff's Massachusetts and Rhode Island right of publicity claims because there was no basis to infer that Backpage appropriated the commercial value of underage girls whose images were displayed in sex trafficking ads found on the site, where a publisher is merely a conduit and the party who actually benefits from the misappropriation was the advertiser, but noting the split of authority over whether the CDA preempts right of publicity claims and plaintiff's argument that a right of publicity claim properly should not be thought of as an intellectual property claim); *Obado v. Magedson*, Civil No. 13-2382 (JAP), 2014 WL 3778261, at *7 & n.5 (D.N.J. July 31, 2014) (noting the Ninth Circuit's position but finding that the plaintiff failed to state a claim for a right of publicity violation and therefore it was unnecessary to decide whether the claim was excluded from CDA preemption), *aff'd on other grounds*, 612 F. App'x 90, 92 (3d Cir. 2015); *Nieman v. Versuslaw, Inc.*, No. 12-3104, 2012 WL 3201931, at *8 (C.D. Ill. Aug. 3, 2012) (writing in *dicta* that plaintiff's right of publicity claim would not be barred by the CDA, but granting defendant's motion on other grounds), *aff'd*, 512 F. App'x 635 (7th Cir. 2013); *Amerigas Propane, L.P. v. Opinion Corp.*, Civil Action No. 12-713, 2012 WL 2327788, at *13 n.10 (E.D. Pa. June 19, 2012) (declining to consider whether plaintiff's claims arose from laws that pertain to intellectual property and were therefore excluded from CDA preemption because the court found that plaintiff adequately alleged that the claims arose from the defendant's own conduct to justify denying defendant's motion to dismiss); *Gauck v. Karamian*, 805 F. Supp. 2d 495 (W.D. Tenn. 2011) (assuming, for purposes of plaintiff's motion for preliminary injunction, that plaintiff's publicity rights claim fell within the CDA's statutory exclusion for claims that arise "from any law pertaining to intellectual property"); *Parisi v. Sinclair*, 774 F. Supp. 2d 310 (D.D.C. 2011) (declining "to extend the scope of the CDA immunity as far as the Ninth Circuit . . .," but nonetheless dismissing plaintiff's right of publicity claim as barred by the newsworthiness exception analyzed in section 12.05[4][B]), *appeal dismissed*, Appeal No. 11-7077, 2012 WL 3068437 (D.C. Cir. 2012); *Stayart v. Yahoo! Inc.*, 651 F. Supp. 2d 873 (E.D. Wis. 2009) (declining to exercise supplementary jurisdiction over state law claims and explaining in *dicta* the split of authority on the issue of whether a right of publicity claim based on third party content is preempted by the CDA), *aff'd on other grounds*, 623 F.3d 436 (7th Cir. 2010).

Stayart involved claims brought under Wisconsin law, which recognizes a common law tort for appropriation of a person's name or likeness and a statutory right based on "use, for advertising purposes or purposes of trade, of the name, portrait, or picture of any living person, without having first obtained the written consent of the person." 651 F. Supp. 2d at 887, *quoting* Wis. Stat. Ann. § 995.50(2)(b). Chief Judge Rudolph Rada noted that a right of publicity claim "is really an offshoot of the more general 'appropriation' tort, which compensates 'bruised feelings' or other injuries to the 'psyche,' whereas the right of publicity 'takes the next logical step' and gives individuals the 'right of control over commercial use of one's identity . . . regardless of the infliction of emotional distress.'" 651 F. Supp. 2d at 887, *quoting* J. Thomas McCarthy, *The Rights of Public-*

Even under the narrow (Ninth Circuit) view of the exclusion for “any law pertaining to intellectual property,” CDA immunity will only apply where third party content is at issue and the other elements of section 230(c) have been met. Thus, in *Fraley v. Facebook, Inc.*,⁶⁷ Judge Lucy Koh of the Northern District of California, applying Ninth Circuit law, held that Facebook was not entitled to CDA immunity in a right of publicity case where the plaintiffs alleged that Facebook displayed user images next to brands that users had “liked” as a form of endorsement on their friend’s profile pages and that Facebook itself had created this content, rather than merely editing user submissions. In that case, when plaintiffs clicked on a “Like” button on a company’s Facebook page, Facebook allegedly translated this act into the words “Plaintiff likes [Brand]” and combined that text with plaintiff’s photograph, the company’s logo and the label “Sponsored Story” in an advertisement. In denying Facebook’s motion to dismiss, Judge Koh ruled that Facebook’s alleged actions in creating Sponsored Stories went beyond a publisher’s traditional editorial functions “such as deciding whether to publish, withdraw, postpone or alter content.”⁶⁸ She emphasized that plaintiffs did not allege merely that Facebook edited user content—“such as by correcting spelling, removing obscenity or trimming for length.”⁶⁹ Judge Koh concluded that “Facebook transformed the character of Plaintiffs’ words, photographs, and actions into a commercial endorsement to which they did not consent.”⁷⁰ As explained by Judge Alsup in a later district court opinion that applied *CCBill* to hold common law trademark infringement and right of publicity claims preempted by the CDA, “Facebook

ity and Privacy §§ 5.60, 5.67 (2d ed. 2008). Writing in *dicta*, Judge Rada explained that “the distinction between an appropriation theory and a right of publicity theory is . . . relevant to CDA immunity.” 651 F. Supp. 2d at 887.

Even though Judge Rada previously had ruled that Yahoo! was entitled to CDA immunity, he wrote that a right of publicity claim “is generally considered an intellectual property claim, . . . which implicates that exception in § 230(e)(2).” 651 F. Supp. 2d at 887–88.

⁶⁷*Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011).

⁶⁸*Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 802 (N.D. Cal. 2011), quoting *Batzel v. Smith*, 333 F.3d 1018, 1031 n.18 (9th Cir. 2003).

⁶⁹*Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 802 (N.D. Cal. 2011), quoting *Fair Housing Council v. Roommate.com, LLC*, 521 F.3d 1157, 1169 (9th Cir. 2008) (en banc).

⁷⁰*Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 802 (N.D. Cal. 2011).

created new content with information that it took from plaintiffs without their consent—Facebook was therefore a content provider as well as a service provider, and thus not entitled to immunity under Section 230.⁷¹ Had the court concluded that sponsored ads merely involved republication of user content, plaintiffs’ right of publicity claims would have been preempted in the Ninth Circuit under *CCBill*.

Subsequently, in *Perkins v. LinkedIn Corp.*,⁷² Judge Koh denied LinkedIn’s motion to dismiss plaintiffs’ right of publicity claim based on CDA preemption in a case brought over reminder emails sent by LinkedIn after plaintiffs initially sent their friends invitations to join LinkedIn. LinkedIn had argued that because plaintiffs provided the substantive content for the initial invitation emails, and consented to those emails being sent, LinkedIn merely was republishing that content in the reminder emails. Judge Koh held, however, that plaintiffs plausibly alleged development. Judge Koh wrote that “[t]he mere fact that Plaintiffs provided their names, photographs, and email contacts for purposes of the initial invitation email, does not confer blanket CDA immunity on LinkedIn for the alleged harm caused by LinkedIn’s unilateral decision to send subsequent reminder emails.”⁷³ This narrow view of CDA immunity could be challenged given that the statute preempts claims based on republishing information that originated with another information content provider—and the decision to republish does not change the essential nature of the act of republication.⁷⁴ Plaintiffs alleged that the emails were “written, designed, and formatted” in whole or in part by LinkedIn, but design and formatting are traditional editorial functions immunized by the CDA and the content of the emails largely republished plaintiffs’ own material.

⁷¹*Evans v. Hewlett-Packard Co.*, C 13-02477 WHA, 2013 WL 4426359, at *3 (N.D. Cal. Aug. 15, 2013) (dismissing Pennsylvania unfair competition and trademark infringement and Pennsylvania and California right of publicity claims brought against the operators of the HP App Catalogue, an app store for Palm devices, as preempted by the CDA, because, although “cleverly-worded,” the complaint did “not allege that defendants created the app at issue here. Rather, it appears that the app was created entirely by third parties.”).

⁷²*Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1222, 1246-49 (N.D. Cal. 2014).

⁷³*Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1222, 1248 (N.D. Cal. 2014).

⁷⁴See *supra* § 37.05[3] (analyzing publication and development).

Judge Koh also based her ruling on her conclusion that the reminder emails were not “substantively identical to the initial invitation email.”⁷⁵ Specifically, the initial invitation email, written in the first person, read: “I’d like to add you to my professional network.” The first reminder email, written in the third person, stated: “This is a reminder that on [date of initial email], [LinkedIn user] sent you an invitation to become part of their professional network at LinkedIn.” The second reminder email, also written in the third person, read: “[LinkedIn user] would like to connect on LinkedIn. How would you like to respond?” Judge Koh explained:

Contrary to Defendant’s assertions, then, the first reminder email appears to transform the substance of the initial invitation email from “Do you want to connect with me?” to “You never responded to the user’s first invitation so let us ask you again, do you want to connect with her?” The second reminder email is arguably more transformative still, as the substance changes from “Do you want to connect with me?” to “You never responded to the user’s first invitation or to our reminder concerning that invitation, so let us ask you for a third time, do you want to connect with her?” It is precisely this changed character of the reminder emails—from invitation at first to potentially annoying by the end—that the Court found could contribute to the additional harm the reminder emails allegedly caused. First MTD Order at 31 (noting that “individuals who receive second and third email invitations to join LinkedIn after declining one or two previous email invitations to join LinkedIn from the same sender may become annoyed at the sender”); *see also Fraley*, 830 F. Supp. 2d at 802 (rejecting CDA immunity where Facebook allegedly “transformed the character” of Plaintiffs’ submissions). For these reasons, the Court rejects LinkedIn’s claim that the reminder emails are substantively identical to the initial invitation email.⁷⁶

Identicality, however, should not be the relevant test, given that the CDA broadly immunizes traditional editorial functions,⁷⁷ including editing, which involves some rewriting and reorganization of material, as anyone who has ever

⁷⁵*Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1222, 1248 (N.D. Cal. 2014).

⁷⁶*Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1222, 1248 (N.D. Cal. 2014) (footnote omitted).

⁷⁷*See, e.g., Green v. America Online (AOL)*, 318 F.3d 465, 470-71 (3d Cir.) (holding that section 230 “bars lawsuits seeking to hold a service provider liable for its exercise of a publisher’s traditional editorial functions—such as deciding whether to publish, withdraw, postpone or alter content”), *cert. denied*, 540 U.S. 877 (2003); *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997), *cert. denied*, 524 U.S. 937 (1998); *Jones*

worked on a publication or published an article can attest.

Judge Koh also focused on the fact that LinkedIn decided whether when and how many reminder emails to send and added a photo to the last one. Here again, these are the type of decisions traditionally made by publishers who decide whether to publish an article once in a morning edition or in multiple editions of a newspaper and may change the heading, title, photograph or prominence when the article is republished.

Ultimately, it is likely that other judges—especially in the Fourth or Sixth Circuits—would have viewed LinkedIn’s changes as editorial in nature, not amounting to development.⁷⁸ Outside the Ninth Circuit, however, a right of publicity claim may be found excluded from CDA protection, depending which interpretation a court chooses to follow, as previously discussed in this subsection.

In *Cybersitter, LLC v. Google, Inc.*,⁷⁹ Central District of California Senior Judge Lew narrowly applied the CDA without much analysis in denying in part the defendant’s motion to dismiss and holding that the CDA preempted claims for state law trademark infringement, contributory infringement pursuant to Cal. Bus. & Prof. Code § 14245(a)(3) and unfair competition under Cal. Bus. & Prof. Code § 17200, based on the contents of advertisements, to the extent not developed by the defendant, but not claims arising out of the alleged sale of plaintiff’s “Cybersitter” mark as a key word to trigger sponsored link advertisements.

In defense of the Ninth Circuit’s rule from *CCBill*, it could be argued that Congress had not considered state intellectual property claims in articulating two bright line rules—a general rule preempting most state law claims (in section 230(e)(3)) and a general exclusion from preemption for intellectual property claims (in section 230(e)(2))—and thus

v. Dirty World Entertainment Recordings, LLC, 755 F.3d 398, 407 (6th Cir. 2014) (holding that traditional editorial functions are immunized under the CDA); *Ben Ezra, Weinstein & Co., Inc. v. America Online Inc.*, 206 F.3d 980, 986 (10th Cir. 2000) (holding that, in enacting the CDA, Congress sought to protect the exercise of a publisher’s “editorial and self-regulatory functions.”); see generally *supra* § 37.05[3].

⁷⁸See *supra* § 37.05[3] (analyzing CDA case law, its development and nuanced differences in how CDA law is applied in different jurisdictions).

⁷⁹*Cybersitter, LLC v. Google, Inc.*, 905 F. Supp. 2d 1080, 1086-87 (C.D. Cal. 2012).

intended that the exclusion for intellectual property claims not impact the general rule of preemption of state law claims.⁸⁰ When Congress passed the CDA in 1995 (prior to the time it was signed into law in January 1996), it was primarily focused on the risks to the development of Internet commerce posed by secondary copyright infringement (which eventually was addressed by the Digital Millennium Copyright Act⁸¹) and liability for defamation. Federal copyright law and state tort claims for defamation were viewed as posing potential impediments to the development of internet businesses. A court therefore could conclude that laws “pertaining to intellectual property” are necessarily federal laws, because state IP claims typically are tort or tort-like claims.⁸² Congress’s subsequent decision, in 2016, when the Defend Trade Secrets Act was adopted, to expressly treat trade secret misappropriation as outside the CDA’s exclusion for laws *pertaining to intellectual property*, supports this view, and the Ninth Circuit’s holding in *Perfect 10*. Prior to that time, trade secret claims could only be brought under state law. Specifying that a trade secret claim under the DTSA is not excluded from the potential preclusive effect of the Good Samaritan provision is consistent with a reading of section 230(e)(2) that considers any law *pertaining to intellectual property* to mean any law that in 1995, when the CDA was enacted, was a federal law pertaining to intellectual property—namely the Copyright Act, the Lanham

⁸⁰The statute treats preemption of state causes of action in a separate clause from the provision stating that the Act is intended to have no effect on any law pertaining to intellectual property. The other two subsections of section 230(e) both primarily address issues of federal law. Section 230(e)(1), captioned “No Effect on Criminal Law,” expressly is limited to federal criminal statutes. Subsection 230(e)(4), captioned “No Effect on Communications Privacy Law,” refers to a specific federal statute, although it also states that the Act is not intended to affect any similar state laws. Thus, it could be argued that 47 U.S.C.A. § 230(e)(3), which addresses and is captioned “State Law” and itself does not expressly exclude intellectual property claims, states an absolute rule and that 47 U.S.C.A. § 230(e)(2), which is captioned “No Effect on Intellectual Property Law,” in light of the focus of subsection (e)(3) and the other subsections, arguably means federal intellectual property laws.

⁸¹17 U.S.C.A. § 512; see generally *supra* § 4.12.

⁸²For example, the U.S. Supreme Court adopted the definition of a trade secret taken from the Restatement of Torts, implicitly recognizing trade secret protection as a creature of state tort law. See, e.g., *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141 (1989); *Aronson v. Quick Point Pencil Co.*, 440 U.S. 257 (1979).

Act and the Patent Act.

Support for this interpretation is bolstered by Congress's extension of federal protection to pre-1972 sound recordings in the Classics Protection and Access Act (Title II of the Orrin G. Hatch–Bob Goodlatte Music Modernization Act of 2018),⁸³ which provides that the provisions of 17 U.S.C.A. § 1401—which extend most aspects of federal copyright protection to these works—shall be considered to be a “law pertaining to intellectual property” within the meaning of 47 U.S.C.A. § 230(e)(2).⁸⁴ In other words, by extending federal protection to sound recordings fixed prior to February 15, 1972 (which previously were protected, if at all, by state common law or statutes⁸⁵), claims of infringement of those works against intermediaries would be subject to the Digital Millennium Copyright Act⁸⁶—like other federal copyright claims—and not the CDA.

Intellectual property laws, including even federal copyright and trademark laws, have their origin in state tort law. While rights of publicity,⁸⁷ state trade secret law,⁸⁸ common law copyrights,⁸⁹ state trademarks⁹⁰ and potentially even idea protection⁹¹ laws usually are considered intellectual property laws, they also often arise under state tort laws or statutory enactments of claims that first arose as common law torts⁹² (and, unlike federal copyright, trademark and patent laws, provide no independent basis for federal

⁸³The Orrin G. Hatch–Bob Goodlatte Music Modernization Act, PL 115-264, 2018 H.R. 1551, 132 Stat. 3676 (Oct. 11, 2018).

⁸⁴17 U.S.C.A. § 1401(g).

⁸⁵See *supra* § 4.18[2].

⁸⁶17 U.S.C.A. §§ 512, 1401(f)(3); *supra* § 4.12.

⁸⁷See *supra* chapter 12.

⁸⁸See *supra* chapter 10.

⁸⁹See *supra* § 4.18[2].

⁹⁰See *supra* § 6.04.

⁹¹See *supra* chapter 13.

⁹²A majority of states have adopted the Uniform Trade Secrets Act and a number of states have enacted right of publicity statutes. See *supra* §§ 10.01, 10.12[3] (trade secrets), 12.03[2] (right of publicity statutes). These statutes, like federal intellectual property statutes, have their origins in tort law remedies. State trademark claims likewise may be asserted based on common law or statute, and also have their antecedents in tort law. Common law copyright claims likewise may be based on state tort or unfair competition law, at common law or pursuant to state statutes. See *supra* § 4.18[2]. Idea protection remedies may arise under

court jurisdiction). Rights of publicity are an outgrowth of state common law privacy law⁹³ and trade secret law is often defined (even in U.S. Supreme Court case law) by reference to the Restatement of Torts.⁹⁴ Common law copyright claims, to the extent still viable and not preempted by the Copyright Act,⁹⁵ likewise frequently arise under state tort or unfair competition laws.⁹⁶ Thus, Congress may not have even considered these claims as “pertaining to intellectual property.”

Although not stated in the legislative history, Congress, in excluding intellectual property laws from the scope of the Good Samaritan exemption, undoubtedly had in mind the issues of vicarious and contributory copyright liability raised in *Religious Technology Center v. Netcom Online Communication Service, Inc.*,⁹⁷ and the Clinton Administration’s National Information Infrastructure White Paper, which issued in draft form in September 1995, shortly before the CDA was enacted, and recommended no change to existing third-party copyright liability doctrines.⁹⁸ Along with vicarious liability for defamation, at that time secondary copyright infringement was viewed as the principal threat to the expansion of e-commerce (and in particular to interactive computer services, which were then known as *access providers* or *content providers*, depending on the nature of their online offerings).⁹⁹ The major Internet law cases in 1995 when Congress considered the Good Samaritan exemption

tort or contract law or other state common law or statutory remedies, such as breach of fiduciary duty or unfair competition. *See supra* chapter 13.

⁹³*See supra* § 12.01. The U.S. Supreme Court, while acknowledging that privacy and publicity rights arise from state tort law, has characterized publicity claims at least as “closely analogous to the goals of patent and copyright law, focusing on the right of the individual to reap the reward of his endeavors” *Zacchini v. Scripps-Howard Broadcasting Co.*, 433 U.S. 562, 573 (1977) (footnote omitted).

⁹⁴*See, e.g., Bonito Boats, Inc. v. Thunder Craft Boats, Inc.*, 489 U.S. 141 (1989); *Aronson v. Quick Point Pencil Co.*, 440 U.S. 257 (1979).

⁹⁵*See* 17 U.S.C.A. §§ 301, 1401(e); *see generally supra* § 4.18 (analyzing the scope of Copyright Act preemption).

⁹⁶*See supra* § 4.18[2].

⁹⁷*Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 907 F. Supp. 1361, 1375 (N.D. Cal. 1995).

⁹⁸U.S. Department of Commerce, National Information Infrastructure White Paper (Sept. 1995), available at <http://www.uspto.gov/go/com/doc/ipnii/>.

⁹⁹Concern about potential exposure for secondary copyright infringe-

(and as late as January 1996 when the statute was enacted into law) were *Cubby, Inc. v. CompuServe, Inc.*,¹⁰⁰ and *Stratton Oakmont v. Prodigy Services, Inc.*,¹⁰¹ which addressed defamation,¹⁰² and *Religious Technology Center v. Netcom Online Communication Service, Inc.*,¹⁰³ which analyzed direct, contributory and vicarious copyright liability. Congress also potentially could have considered secondary trademark liability in light of *Playboy Enterprises, Inc. v. Frena*.¹⁰⁴ At that time, there simply were no cases that held out the risk of vicarious liability being imposed on interactive computer service providers or users for third-party content under state intellectual property laws.¹⁰⁵ Indeed, the only online trade secret¹⁰⁶ and right of publicity¹⁰⁷ cases either decided or then-pending raised issues of direct, not vicarious liability. In all likelihood, Congress never considered the risk of exposure for state law intellectual property

ment eventually led to the enactment of the Digital Millennium Copyright Act in 1998. See generally *supra* § 4.12.

¹⁰⁰*Cubby, Inc. v. CompuServe, Inc.*, 776 F. Supp. 135 (S.D.N.Y. 1991).

¹⁰¹*Stratton Oakmont v. Prodigy Services, Inc.*, 23 Media L. Rep. (BNA) 1794, 1995 WL 323710 (Nassau County, N.Y. Sup. Ct. May 26, 1995).

¹⁰²See *supra* § 37.04 (discussing these cases).

¹⁰³*Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 923 F. Supp. 1231 (N.D. Cal. 1995).

¹⁰⁴*Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552 (M.D. Fla. 1993).

¹⁰⁵This assertion is based on numerous Lexis-Nexis database searches conducted by the author between May 1995 and the time the Good Samaritan exemption was signed into law in January 1996. See generally Ian C. Ballon, "The Emerging Law of the Internet" in *The Performing Art of Advocacy: Creating A New Spirit* (A.B.A. Section of Litigation August 1995); Ian C. Ballon, "The Emerging Law of the Internet" in *The Emerging Law of the Internet* (Continuing Education of the Bar Jan. 1996) (chronicling Internet law as of those dates).

¹⁰⁶The Church of Scientology had filed several trade secret cases in the early 1990s, but by 1995 there was already ample case law standing for the proposition that third parties could not be held accountable for the actions of others. See *Religious Technology Center v. Lerma*, 908 F. Supp. 1362, 1368 (E.D. Va. 1995); *Religious Technology Center v. F.A.C.T.NET, Inc.*, 901 F. Supp. 1519, 1526 (D. Colo. 1995); *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, 923 F. Supp. 1231, 1256 (N.D. Cal. 1995); see generally *supra* § 14.11[2] (discussing the cases).

¹⁰⁷See *Stern v. Delphi Internet Services Corp.*, 165 Misc. 2d 21, 626 N.Y.S.2d 694 (N.Y. Sup. Ct. 1995). *Stern* involved an issue of direct liability (Delphia's use of a picture of Howard Stern to promote its service). See generally *supra* § 12.08[2] (discussing the case).

claims at the time the CDA was enacted.

While it is possible that Congress simply never contemplated whether right of publicity, state trade secret or other state law intellectual property claims would be preempted in crafting the Good Samaritan exemption, courts in practice need to construe the statute as enacted to determine its scope.¹⁰⁸ As a different Ninth Circuit panel commented in a later case construing a different provision of the CDA, the “sound and fury on the congressional intent of the immunity under section 230 . . . ultimately signifies nothing. It is the language of the statute that defines and enacts the concerns and aims of Congress; a particular concern does not rewrite the language.”¹⁰⁹

If right of publicity, trade secret and other claims are viewed as tort or state statutory claims, they are plainly not excluded and are potentially preempted by section 230. If, however, they are viewed as laws “pertaining to intellectual property” then they are excluded and not preempted, based on the structure of section 230(e), unless section 230(e)(2) is modified by section 230(e)(3), such that section 230(e)(2)’s exclusion for any law pertaining to intellectual property necessarily means any *federal* law, because any state law is nec-

¹⁰⁸See *Chicago Lawyers’ Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*, 519 F.3d 666, 671 (7th Cir. 2008) (holding that even though Congress undoubtedly never considered whether section 230 would preempt a federal Fair Housing Act claim the plain text of the statute would control). As Chief Judge Easterbrook explained in *Craigslist*:

The Lawyers’ Committee responds that “nothing in section 230’s text or history suggests that Congress meant to immunize an ISP from liability under the Fair Housing Act. In fact, Congress did not even remotely contemplate discriminatory housing advertisements when it passed section 230.” That’s true enough, but the reason a legislature writes a general statute is to avoid any need to traipse through the United States Code and consider all potential sources of liability, one at a time. The question is not whether Congress gave any thought to the Fair Housing Act, but whether it excluded section 3604(c) from the reach of section 230(c)(1). Cf. *Blanchette v. Connecticut General Ins. Corporations*, 419 U.S. 102, 126–27, 95 S. Ct. 335, 42 L. Ed. 2d 320 (1974) (Congress need not think about a subject for a law to affect it; effect of general rules continues unless limited by superseding enactments).

519 F.3d at 671.

¹⁰⁹*Barnes v. Yahoo!, Inc.*, 570 F.3d 1096, 1105 (9th Cir. 2009). This observation is consistent with the skepticism expressed about legislative history by Justice Scalia (attributing the words to Judge Harold Leventhal), when he wrote that “the use of legislative history [i]s the equivalent of entering a crowded cocktail party and looking over the heads of the guests for one’s friends.” *Conroy v. Aniskoff*, 507 U.S. 511, 519 (1993).

essarily preempted by section 230(e)(3) (or unless, as suggested by the dissenting judge in *Hepp v. Facebook, Inc.*, a narrow reading of section 230(e)(2) is compelled by the Congressional findings and policy objectives set forth in section 230(a) and 230(b)¹¹⁰).

Courts that read section 230(e)(2) expansively to exclude federal *and* state laws pertaining to intellectual property from the broad preemption afforded by the CDA, nevertheless may hold that some state IP claims, such as those for idea misappropriation¹¹¹ and unfair competition (including common law copyright claims in many states) may not be excluded because they are more akin to tort than intellectual property claims.

Even in these courts, negligence or other tort actions arising from state intellectual property laws should be treated as preempted as a tort law and not a law *pertaining to intellectual property*. For example, an interactive computer service or user could not be sued for trade secret misappropriation based on the misconduct of another because to make out a claim based on secondary (or third party liability), a plaintiff would almost certainly have to allege a duty undertaken to the trade secret owner, which likely would be premised on state tort law, or possibly contract or quasi-contract law or breach of fiduciary duty—but not intellectual property law.¹¹² In similar contexts, courts have construed claims as preempted by the CDA if, regardless of how framed, the cause of action sounds in negligence.¹¹³ Consistent with this view, a district court dismissed as preempted

¹¹⁰See *Hepp v. Facebook, Inc.*, 14 F.4th 204, 216-26 (3d Cir. 2021) (Cowen, J. dissenting in relevant part).

¹¹¹See *supra* §§ 13.01–13.04.

¹¹²A breach of contract claim would not be preempted to the extent that an interactive computer service provider or user was accused of its own breach, unless the claim was premised on acting as a publisher or speaker of material originating with another information content provider or as a result of any action voluntarily taken to restrict access to or the availability of material deemed, among other things, harassing or otherwise objectionable. See *supra* § 37.05[1]. For purposes of clarity, the rest of the discussion in this section focuses on the more typical case where a claim is premised on negligence.

¹¹³See, e.g., *Green v. America Online (AOL)*, 318 F.3d 465 (3d Cir.), *cert. denied*, 540 U.S. 877 (2003); *Doe v. MySpace, Inc.*, 528 F.3d 413 (5th Cir.), *cert. denied*, 555 U.S. 1031 (2008); *Doe v. MySpace, Inc.*, 629 F. Supp. 2d 663 (E.D. Tex. 2009); *Doe II v. MySpace Inc.*, 175 Cal. App. 4th 561, 96 Cal. Rptr. 3d 148 (2d Dist. 2009); *Doe v. America Online, Inc.*, 783 So. 2d

by the CDA a New Jersey state law unfair competition claim arising out of the republication of allegedly infringing material.¹¹⁴

Ultimately, the Ninth Circuit, which for fourteen years was the only circuit to consider the issue, had concluded that section 230(e)(2), as an exclusion to a provision affording immunity, should be narrowly construed to apply only to federal claims pertaining to intellectual property (other than the DTSA), consistent with the policy directives set forth in the statute itself, in section 230(b). Whether that view, or the perspective of the majority of the Third Circuit panel in *Hepp*, prevails, remains to be seen.

37.05[5][C] The Exclusion for Sex Trafficking Claims (and Related Advertising)

The Good Samaritan exemption was amended in 2018¹ to carve out exclusions from some—but not all—of the immuni-

1010 (Fla. 2001); *supra* § 37.05[1] (citing additional cases).

Some might argue that preempting a negligence claim based on an interactive computer service provider or user's failure to protect against a state intellectual property right would in effect "limit or expand" a "law pertaining to intellectual property" within the meaning of section 230(e)(2) and therefore could *not* be preempted as merely a negligence claim. Ultimately, however, if a state intellectual property law does not permit a claim for secondary liability to be brought against an interactive computer service or user, any theory of recovery based on negligence or similar theories should be viewed for what it is—a tort claim—and preempted to the extent that a party seeks to impose liability under state tort law for an interactive computer service or user acting as a publisher or speaker of another party's content or undertaking any action voluntarily in good faith to restrict access to or the availability of content enumerated in section 230(c)(2), including material that is harassing or otherwise objectionable. The underlying claim—negligence, for example—is not a law "pertaining to intellectual property" and treating it as such would expand the scope of the state intellectual property law.

¹¹⁴*See Inventel Products, LLC v. Li*, Civ. No. 2:19-9190, 2019 WL 5078807, at *8 (D.N.J. Oct. 10, 2019) (dismissing plaintiff's New Jersey Consumer Fraud Act claim against Google, premised on Google's alleged provision of AdWords and analytics services arising out of publication of third-parties' allegedly infringing material, as preempted by the CDA; "While the CDA does not limit laws pertaining to intellectual property, 47 USC § 230(e)(2), the CFA is not an intellectual property statute, *see* N.J.S. § 56:8-2 (banning use of improper business practices).").

[Section 37.05[5][C]]

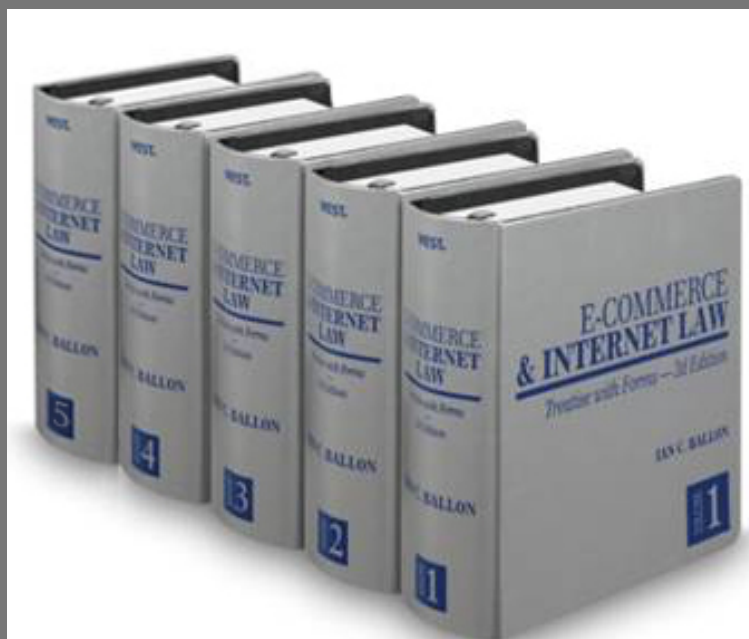
¹*See* The Allow States and Victims to Fight Online Sex Trafficking Act of 2017. Pub. L. No. 115-164, 132 Stat. 1253 (2018); 47 U.S.C.A. § 230(e)(5).

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2022

Ian C. Ballon

2022
UPDATES -
INCLUDING
NEW AND
IMPORTANT
FEATURES

THE PREEMINENT
INTERNET AND
MOBILE LAW
TREATISE FROM A
LEADING INTERNET
LITIGATOR — A
5 VOLUME-SET &
ON WESTLAW!



To order call **1-888-728-7677**
or visit **lanBallon.net**

Key Features of E-Commerce & Internet Law

- ◆ AI, ML, screen scraping and data portability
- ◆ Antitrust in the era of techlash
- ◆ The CPRA, Virginia, Colorado and Nevada privacy laws, GDPR, California IoT security statute, state data broker laws, and other privacy and cybersecurity laws
- ◆ Software copyrightability and fair use after *Google v. Oracle*
- ◆ Mobile and online contract formation, unconscionability and enforcement of arbitration and class action waiver clauses in an era of mass arbitration
- ◆ TCPA law and litigation after *Facebook v. Duguid* - the most comprehensive analysis of the statute, regulations, and conflicting case law found anywhere
- ◆ The Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and the Defend Trade Secrets Act (DTSA) -- and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, & privacy
- ◆ Platform moderation and liability, safe harbors, and defenses (including the CDA and DMCA)
- ◆ Dormant Commerce Clause restrictions on state law regulation of online and mobile commerce
- ◆ The law of SEO and SEM – and its impact on e-commerce vendors
- ◆ Defending cybersecurity breach and data privacy class action suits – case law, trends & strategy
- ◆ IP issues including Copyright and Lanham Act fair use, *Rogers v. Grimaldi*, patentable subject matter, negative trade secrets, rights of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of hashtags in social media marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- ◆ Online anonymity and pseudonymity – state and federal laws governing permissible disclosures and subpoenas
- ◆ Sponsored links, embedded links, #hashtags, and internet, mobile and social media advertising
- ◆ Enforcing judgments against foreign domain name registrants
- ◆ Valuing domain name registrations from sales data
- ◆ Applying the First Sale Doctrine to virtual goods
- ◆ Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions for certain IP & FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- ◆ Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- ◆ Click fraud
- ◆ Copyright and Lanham Act fair use
- ◆ Practical tips, checklists and forms that go beyond the typical legal treatise
- ◆ Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ AI/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- ◆ Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- ◆ Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- ◆ Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- ◆ Addresses both law and best practices
- ◆ Includes the hottest issues, such as IP and privacy aspects of artificial intelligence & machine learning, social media advertising, cloud storage, platform liability, and more!
- ◆ Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

Volume 1

Part I. Sources of Internet Law and Practice: A Framework for Developing New Law

- Chapter* 1. Context for Developing the Law of the Internet
2. A Framework for Developing New Law
3. [Reserved]

Part II. Intellectual Property

4. Copyright Protection in Cyberspace
5. Data Scraping, Database Protection, and the Use of Bots and Artificial Intelligence to Gather Content and Information
6. Trademark, Service Mark, Trade Name and Trade Dress Protection in Cyberspace
7. Rights in Internet Domain Names

Volume 2

- Chapter* 8. Internet Patents
9. Unique Intellectual Property Issues in Search Engine Marketing, Optimization and Related Indexing, Information Location Tools and Internet and Social Media Advertising Practices
10. Misappropriation of Trade Secrets in Cyberspace
11. Employer Rights in the Creation and Protection of Internet-Related Intellectual Property
12. Privacy and Publicity Rights of Celebrities and Others in Cyberspace
13. Idea Submission, Protection and Misappropriation
- Part III. Licenses and Contracts**
14. Documenting Internet Transactions: Introduction to Drafting License Agreements and Contracts
15. Drafting Agreements in Light of Model and Uniform Contract Laws: The Federal eSign Statute, Uniform Electronic Transactions Act, UCITA, and the EU Distance Selling Directive
16. Internet Licenses: Rights Subject to License and Limitations Imposed on Content, Access and Development
17. Licensing Pre-Existing Content for Use Online: Music, Literary Works, Video, Software and User Generated Content Licensing Pre-Existing Content
18. Drafting Internet Content and Development Licenses
19. Website Development and Hosting Agreements
20. Website Cross-Promotion and Cooperation: Co-Branding, Widget and Linking Agreements
21. Obtaining Assent in Cyberspace: Contract Formation for Click-Through and Other Unilateral Contracts
22. Structuring and Drafting Website Terms and Conditions
23. ISP Service Agreements

Volume 3

- Chapter* 24. Software as a Service: On-Demand, Rental and Application Service Provider Agreements
- Part IV. Privacy, Security and Internet Advertising**
25. Introduction to Consumer Protection in Cyberspace
26. Data Privacy
27. Cybersecurity: Information, Network and Data Security
28. Advertising in Cyberspace

Volume 4

- Chapter* 29. Email and Text Marketing, Spam and the Law of Unsolicited Commercial Email and Text Messaging
30. Online Gambling

Part V. The Conduct and Regulation of Internet Commerce

31. Online Financial Transactions and Payment Mechanisms
32. Online Securities Law
33. State and Local Sales and Use Taxes on Internet and Mobile Transactions
34. Antitrust Restrictions on Technology Companies and Electronic Commerce
35. Dormant Commerce Clause and Other Federal Law Restrictions on State and Local Regulation of the Internet
36. Best Practices for U.S. Companies in Evaluating Global E-Commerce Regulations and Operating Internationally

Part VI. Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption

37. Defamation, Torts and the Good Samaritan Exemption (47 U.S.C.A. § 230)
38. Tort and Related Liability for Hacking, Cracking, Computer Viruses, Disabling Devices and Other Network Disruptions
39. E-Commerce and the Rights of Free Speech, Press and Expression in Cyberspace

Part VII. Obscenity, Pornography, Adult Entertainment and the Protection of Children

40. Child Pornography and Obscenity
41. Laws Regulating Non-Obscene Adult Content Directed at Children
42. U.S. Jurisdiction, Venue and Procedure in Obscenity and Other Internet Crime Cases

Part VIII. Theft of Digital Information and Related Internet Crimes

43. Detecting and Retrieving Stolen Corporate Data
44. Criminal and Related Civil Remedies for Software and Digital Information Theft
45. Crimes Directed at Computer Networks and Users: Viruses and Malicious Code, Service Disabling Attacks and Threats Transmitted by Email

Volume 5

- Chapter* 46. Identity Theft
47. Civil Remedies for Unlawful Seizures
- Part IX. Liability of Internet Sites and Service (Including Social Networks and Blogs)**
48. Assessing and Limiting Liability Through Policies, Procedures and Website Audits
49. Content Moderation and Platform Liability: Service Provider and Website, Mobile App, Network and Cloud Provider Exposure for User Generated Content and Misconduct
50. Cloud, Mobile and Internet Service Provider Compliance with Subpoenas and Court Orders
51. Web 2.0 Applications: Social Networks, Blogs, Wiki and UGC Sites
- Part X. Civil Jurisdiction and Litigation**
52. General Overview of Cyberspace Jurisdiction
53. Personal Jurisdiction in Cyberspace
54. Venue and the Doctrine of Forum Non Conveniens
55. Choice of Law in Cyberspace
56. Internet ADR
57. Internet Litigation Strategy and Practice
58. Electronic Business and Social Network Communications in the Workplace, in Litigation and in Corporate and Employer Policies
59. Use of Email in Attorney-Client Communications

“Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet.”

Jay Monahan

General Counsel, ResearchGate

ABOUT THE AUTHOR

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator in the firm's Silicon Valley Los Angeles and Washington, DC offices. He defends data privacy, cybersecurity breach, AdTech, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database, AI and other intellectual property cases, including disputes involving safe harbors and exemptions, platform liability and fair use.



Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top Intellectual Property litigators in every year the list has been published (2009-2021), Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was selected as the Lawyer of the Year for information technology law in the 2022, 2021, 2020, 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., Law Dragon and Chambers and Partners USA Guide. He also serves as Executive Director of Stanford University Law School's Center for the Digital Economy.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

Mr. Ballon is also the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.IanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@IanBallon).

Contributing authors: Parry Aftab, Darren Abernethy, Viola Bensinger, Ed Chansky, Francoise Gilbert, Rebekah Guyon, Tucker McCrady, Josh Raskin, & Tom Smedinghoff.

NEW AND IMPORTANT FEATURES FOR 2022

- > **Antitrust in the era of techlash** (chapter 34)
- > **Platform moderation and liability, safe harbors and defenses** (ch. 49, 4, 6, 8, 37)
- > **Privacy and IP aspects of Artificial Intelligence (AI) and machine learning** (ch. 5, 26)
- > **How *TransUnion v. Ramirez* (2021) changes the law of standing in cybersecurity breach, data privacy, AdTech and TCPA class action suits.**
- > **90+ page exhaustive analysis of the CCPA and CPRA, all statutory amendments and final regulations, and how the law will change under the CPRA – the most comprehensive analysis available!** (ch 37)
- > **Text and other mobile marketing under the TCPA following the U.S. Supreme Court's ruling in *Facebook, Inc. v. Duguid*, 141 S. Ct. 1163 (2021) – and continuing pitfalls companies should avoid to limit exposure**
- > **Software copyrightability and fair use in light of the U.S. Supreme Court's 2021 decision in *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021)** (ch 4)
- > **Rethinking 20 years of database and screen scraping case law in light of the U.S. Supreme Court's opinion in *Van Buren v. United States*, 141 S. Ct. 1648 (2021)** (ch5)
- > **FOSTA-SESTA and ways to maximize CDA protection** (ch 37)
- > **IP aspects of the use of #hashtags in social media** (ch 6)
- > **The CLOUD Act** (chapter 50)
- > **Virginia, Colorado and Nevada privacy laws** (ch 26)
- > **Applying the single publication rule to websites, links and uses on social media** (chapter 37)
- > **Digital economy litigation strategies**
- > **Circuit-by-circuit, claim-by-claim analysis of CDA opinions**
- > **How new Copyright Claims Board proceedings will disrupt DMCA compliance for copyright owners, service providers and users** (ch 4)
- > **Website and mobile accessibility under the ADA and state laws** (chapter 48)
- > **Online and mobile Contract formation – common mistakes by courts and counsel** (chapter 21)
- > **Updated Defend Trade Secrets Act and UTSA case law** (chapter 10)
- > **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- > **AdTech law** (chapter 28, Darren Abernethy)
- > **The risks of being bound by the CASE Act's ostensibly voluntary jurisdiction over small copyright cases**
- > **Rethinking approaches to consumer arbitration clauses in light of mass arbitration and case law on representative actions.**
- > **Dormant Commerce Clause challenges to state privacy and other laws – explained**
- > **First Amendment protections and restrictions on social media posts and the digital economy – important new case law**
- > **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert and Viola Bensinger) (ch. 26)
- > **Patent law** (updated by Josh Raskin) (chapter 8)
- > **Idea protection & misappropriation** (ch 13)
- > **Revisiting links, embedded links, sponsored links, and SEO/SEM practices and liability** (chapter 9)
- > **eSIGN case law** (chapter 15)

**SAVE 20% NOW!! To order call 1-888-728-7677
or visit IanBallon.net
enter promo code **WPD20** at checkout**

List Price: \$3,337.00
Discounted Price: \$2,669.60