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

Excerpted from the forthcoming 2023 update 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.)

TRANSFORMATION IN PRACTICE: ASSESSING FAIR USE IN THE WAKE OF *ORACLE V. GOOGLE* AND *WARHOL V. GOLDSMITH*

THE 2023 COPYRIGHT SYMPOSIUM
TRANSFORM – A NEW HORIZON IN COPYRIGHT
COPYRIGHT SYMPOSIUM, THE MCCARTHY INSTITUTE AT ASU LAW AND THE UCLA INSTITUTE FOR TECHNOLOGY, LAW AND POLICY
LOS ANGELES
MARCH 16, 2023

Ian C. Ballon
Greenberg Traurig, LLP

Los Angeles:	Silicon Valley:	Washington, D.C.:
1840 Century Park East, Ste. 1900	1900 University Avenue, 5th Fl.	2101 L Street, N.W., Ste. 1000
Los Angeles, CA 90067	East Palo Alto, CA 914303	Washington, D.C. 20037
Direct Dial: (310) 586-6575	Direct Dial: (650) 289-7881	Direct Dial: (202) 331-3138
Direct Fax: (310) 586-0575	Direct Fax: (650) 462-7881	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 2023 Annual Update), a 5-volume legal treatise by Ian C. Ballon, published by West, (888) 728-7677
www.ianballon.net

GT GreenbergTraurig

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 a litigator who 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 AdTech class action suits.

Ian 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 2022). He has been listed in Best Lawyers in America consistently every year since 2003 and was named Lawyer of the Year for Information Technology in 2023, 2022, 2020, 2019, 2018, 2016 and 2013. In 2022, 2021, 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 2022, Ian was named to Lawdragon's list of the Top 500 Lawyers in America and he has been included on the *Daily Journal's* annual list of the Top 100 Lawyers in California. 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 a Northern California Super Lawyer every year from 2004 through 2021 and a Southern California Super Lawyer for every year from 2007-2021. He has also been 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 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 is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009). 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 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

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 Act[1]

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]

[1]Portions 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 defense[1] to claims

---

[Section 4.12[1]]

[1]The 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 statutory[2]) 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 prerequisites[5] 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).

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

[3]*See 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).

[5]*See infra* § 4.12[3].

[6]*See infra* § 4.12[4].

[7]*See 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 nonprofit 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

---

[8] *See infra* § 4.12[6].

[9] *See infra* § 4.12[7].

[10] *See infra* § 4.12[8].

[11] *See 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]

---

[13]*See 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].

[14]It 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 [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

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-

[15]A 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.

[17]*See, 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].

[18]The 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.

[19]*See supra* §§ 4.11[1] to 4.11[6].

[20]*See* 17 U.S.C.A. § 512(c).

old requirements.[21] It must adopt, reasonably implement and inform subscribers and account holders[22] 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 tools[25] safe harbors (and in limited circumstances the caching[26] 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

---

[21] *See infra* § 4.12[3].

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

[23] *See infra* § 4.12[3].

[24] *See 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).

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

[26] *See infra* § 4.12[5].

[27] *See 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]

---

[28]*See, 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).

[29]*See 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).

[31]*See 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].

[32]*See* 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 blindness[35] or evidence of inducement[36] 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).

[33]*See* 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).

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

[35]*See, 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].

[36]*See 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] Fourth[40] and Ninth[41] 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).

[37]*See infra* § 4.12[6][D].

[38]*See infra* § 4.12[6][D].

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

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

[41]*See 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).

[43]*See 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 apparent[46]—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].

[46]17 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

---

[47] *See 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).

[50] *See 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.

[51] In *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 holders[56] 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).

---

[55] *See infra* § 4.12[9][C].

[56] *See 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].

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

[58] 17 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-

[59]Whether 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

---

[60]*See* 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.

[61]*See* 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-

---

[62]*See* 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.

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

[64]*See, 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

---

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

[66] *See, 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).

[67]Case 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 infringement[68]—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.

[68]*See 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.

[70]Google 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

---

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

[72] *See* https://www.google.com/transparencyreport/removals/copyright/ (visited October 12, 2015).

[73] *See* https://www.google.com/transparencyreport/removals/copyright/ (visited June 25, 2016).

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

[75] *See* https://transparency.twitter.com/copyright-notices/2015/jul-dec (visited June 25, 2016).

[76] *See* 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-*

---

[79] *See* 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 Act[88]—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 infringement[92] (even though the latter theory of recovery was judicially adopted approximately six-and-a-half years after the DMCA

---

[88]*See* 17 U.S.C.A. §§ 1501 to 1511.

[89]*See 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).

[90]15 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].

[91]*See 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).

[92]*See 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

---

[93]The 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.

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

[96]The 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

---

[101]*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).

[102]Sanctions 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).

[104]*See, 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-

[105]Google 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.

[106]A 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-

---

[107] *See* http://www.copyrightinformation.org/

[108] *See* http://2013ippractices.com/

[109] *See* 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

---

[110]In *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).

[111]One 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 internationally[112] 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.

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

[113]*See, 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).

[114]*See* 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.

[115]*See* 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 limitation[1]) 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]]

[1]17 U.S.C.A. § 512(a); *infra* § 4.12[4].

[2]17 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 crimped 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

[10] *See 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]]

[1] Subsection (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

---

[2]17 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).

[2]17 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).

[4]For 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].

[2]Employer 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 employment[3] 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

---

[3]An 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).

[8]Suggestions 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

---

[9]For 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).

[2]*See* 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

---

[3]*See 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.").

[4]*See* 17 U.S.C.A. § 512(e).

[5]*See Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

[6]*See 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 policy[13] 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).

[10]*See 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).

[13]*See infra* § 4.12[3][B][iv].

[14]*See 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]).

[15]*See 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).

[18]*See 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-

[21] *See infra* § 4.12[9][D].

[22] The *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

[23]Except 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]]

[1]Although 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).

[2]Adoption 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-

---

[6]*See 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 *un*reasonable,[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).

[9]In *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

---

[12]*See 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

---

[20]The 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).

[30]As 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 deficient[36] 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

---

[36] *See 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).

[41]Veoh 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).

[48] Audible 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).

[53]Vendors 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-

---

[66] *See 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

---

[67]*See 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).

[68]*See 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).

[69]*See 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).

[70]*See 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).

[71]*See 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).

[73]*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; "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 plaintiff's 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

---

[80] 633 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]]

[1] 17 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

---

[2]17 U.S.C.A. § 512(i)(2)(A).

[3]17 U.S.C.A. §§ 512(i)(2)(B), 512(i)(2)(C).

[4]The 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* itself[8]—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-

---

[10]*See 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]]

[1]17 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

---

[5]17 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—Naptser did not "transmit, route, or provide connections through its system . . . .").

[7]17 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

---

[8]17 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.*

[9]17 U.S.C.A. § 512(a)(3).

[10]17 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).

[11]17 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]

---

[12]H.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 tracker[16]) or where transmissions occur directly between users, rather than "through a system or network controlled or operated by or for" a service provider[17] (such as a Peer-to-Peer network[18]), 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*).

[16]*See Columbia Pictures Industries, Inc. v. Fung*, 710 F.3d 1020, 1041–42 (9th Cir. 2013).

[17]17 U.S.C.A. § 512(a).

[18]In *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.

[19]*See 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 modifies[21] a transmission, stores it[22] 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-

---

[20]*See, 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)).

[21]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 wrote in *dicta* that the Aimster peer-to-peer service "modified" content by encrypting all information transferred between users.

[22]*See 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]

---

[24]H.R. Conf. Rep. No. 796, 105th Cong., 2d Sess. 73 (1998), *reprinted in* 1998 U.S.C.C.A.N. 639, 649.

[25]Service 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]]

[1]17 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

---

[3]With 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 network[6] 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].

[4]17 U.S.C.A. § 512(b)(1)(A).

[5]17 U.S.C.A. § 512(b)(1)(A).

[6]The 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).

[7]17 U.S.C.A. § 512(b)(1)(B).

[8]*See* 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.

[9]*See* 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 protocol[10] 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

---

[10]The 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."

[11]17 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.

[12]17 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

[13]17 U.S.C.A. § 512(b)(1)(A).

[14]17 U.S.C.A. § 512(b)(2)(C).

[15]17 U.S.C.A. § 512(b)(2)(D).

[16]*See* 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

---

[17] 17 U.S.C.A. § 512(b)(2)(E).

[18] *Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1123–25 (D. Nev. 2006).

[19] *See Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1111 (D. Nev. 2006).

[20] *See Ellison v. Robertson*, 357 F.3d 1072, 1081 (9th Cir. 2004); *supra* § 4.12[4].

[21] What 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 in 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]]

[1] 17 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

---

[3]H.R. Rep. No. 105-551, 105th Cong., 2nd Sess. (1998) (emphasis added); S. Rep. No. 105-190, 105th Cong., 2nd Sess. (1998) (emphasis added).

[4]*See, e.g.*, Nimmer on Copyright § 12B.03.

[5]*See, 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

---

[6] *See generally infra* § 9.02 (analyzing caching).

[Section 4.12[5][C]]

[1] H.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*

---

[2]H.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).

[8]*See 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").

[9]*Compare* 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]]

[1] 17 U.S.C.A. § 512(c).

[2] *See 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] Fourth[5] and Ninth[6] 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].

---

[4]*See Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 37–38 (2d Cir. 2012).

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

[6]*See 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).

[9]*See 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).

[10]*See* 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]

---

[11]What it means to disable access to or remove material is addressed in section 4.12[6][C].

[12]Some 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

---

[15]*See* 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).

[16]*See* 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).

[17]*See 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).

[18]*See, 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.").

[19]*See, 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

---

[20]*See* 17 U.S.C.A. § 512(m).

[21]*See, 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

---

[23] *See 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)).

[26]The 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).

[27]17 U.S.C.A. § 512(c)(1).

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

[29]That 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

---

[30]*See 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.' ").

[31]*See, 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).

[33]According 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).

[40]17 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.

[44]A 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.

---

[49]*See 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 crimped 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).

[52] *See supra* § 4.11[2] (analyzing direct liability).

[53] *See 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-

---

[54]17 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

---

[57]*See 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.

[58]*See UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1015–20 (9th Cir. 2013).

[59]17 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 website[62]—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

---

[60]17 U.S.C.A. § 512(c)(1).

[61]This 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).

[62]If 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]

---

[63]17 U.S.C.A. § 512(c)(1).

[64]In 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 plaintiff's 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]

---

[68] *See supra* § 4.12[4].

[69] 586 F. Supp. 2d at 1147, *quoting* 17 U.S.C.A. § 512(k)(1)(A) (emphasis added by the court).

[70] 17 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).

[77] The 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 law[80] 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).

[90] *See* 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).

[98]Judge 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*C, 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 damages[107] or potentially even secondary liability, where safe harbor protection is inapplicable[108]) 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.

[109]The 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.

[110]17 U.S.C.A. § 512(c)(1).

[111]17 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]]

[1] 17 U.S.C.A. § 512(c)(2).

[2] http://www.copyright.gov/onlinesp/list/s_agents.html

[3] *See* 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 expeditiously[6] disabling access to or removing material identified in substantially complying notifications[7] (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

---

[4]*See, 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).

[5]*See, 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).

[6]*See, 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).

[7]17 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]]

[1]*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) ("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).

[3]*See* 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).

[4]17 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).

[5]*See 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.").

[8]*See 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).

ficult 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 expeditiously[12] 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).

[12] In *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.

[13]*See* 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].

[14]*See, e.g.*, *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001).

[15]*See* 17 U.S.C.A. § 512(c)(1)(C) (emphasis added).

in a lawsuit between the copyright owner and poster[16] 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

---

[16]*See 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)).

[17]The 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).

[19]The 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].

[23] Although 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 infringement[25] (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

---

[24] *See supra* § 4.11[3].

[25] *See supra* § 4.11[6].

[26] 17 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.

[27] 17 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]

---

[29]*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); *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).

[40]*See 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).

[43]*See 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

---

[59] *See 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

---

[61]*See 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).

[69]The 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 benefitting 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 Preferson 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.

[71]A 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 passive[75] 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).

[75]The 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 Circuit[77] 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).

[77]*See 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.").

[78]*See 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).

[79]*See* 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 found[82] or declined to find[83] 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.oficerjellnutz.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

[84]YouTube 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]

---

[85] *See 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.

[88]*See, 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 infringement[91]—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

---

[94]*See 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

---

[108]*See 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)).

[109]One district court imposed a higher burden of proof for a copyright owner to establishe 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

---

[110]*See Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 93-99 (2d Cir. 2016) (discussing shifting burdens of proof under the DMCA).

[111]As 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).

[113]*See 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 awarness 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 site[127] 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).

[125]In *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).

[127]*See 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.").

[128]*See 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).

[139]Evidence 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).

[143]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 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).

[146] *See 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 control[4] *or* if it

---

[Section 4.12[6][D]]

[1]17 U.S.C.A. § 512(c)(1)(B).

[2]*See, 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).

[3]*See, 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 . . . .").

[4]*See, 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 interest[5] (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

---

[7]*See 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].

[8]*See 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 purchases[13] 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

---

[11]*See, 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).

[12]*See Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

[13]*See, 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 VeRO[17] 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]

---

[17]Additional information on eBay's Verified Rights Owner's—or VeRO—program may be found in section 6.10[2][I] and in chapter 50.

[18]The 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].

[25]586 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).

[29] 586 F. Supp. 2d at 1153.

[30] 586 F. Supp. 2d at 1153.

[31] *See supra* § 4.11[9][F] (analyzing the *Napster* case).

[32] 586 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

---

[33]586 F. Supp. 2d at 1154.

[34]586 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

---

[48] Judge 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).

[49] *See 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).

[51] *See 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 understand 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).

[62]H.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

---

[76]*See 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).

[77]*See 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[ied] 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).

[110]In 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

---

[112]*See Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 612-13 (9th Cir. 2018).

[113]*See Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 613 (9th Cir. 2018) (quoting *UMG* and *Viacom v. YouTube*).

[114]*See 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 SunFog 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).

[117]*See 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 awareness[127] or reasonably implement a repeat infringer policy[128] 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).

[126]*See 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].

[127]17 U.S.C.A. § 512(c)(1)(A); *see generally supra* § 4.12[6][C].

[128]17 U.S.C.A. § 512(i); *see generally supra* § 4.12[3][B].

[129]*See supra* § 4.11[4].

[130]H. 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

---

[131]H. Rep. No. 105-796, 105th Cong. 2d Sess. 1, 72 (1998).

[132]H. Rep. No. 105-796, 105th Cong. 2d Sess. 1, 72 (1998).

[133]Section 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.

[134]H.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*

---

[136] *See supra* § 4.11[4] (analyzing vicarious liability).

[137] H.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-

---

[141] *See 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).

[143] *See 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]

---

[155]For 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 *Ellison* 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]]

[1]17 U.S.C.A. § 512(d).

[2]One 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-

---

[3] 17 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

---

[5]*See 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).

[6]*See* 17 U.S.C.A. § 512(g)(2).

[7]*See* 17 U.S.C.A. § 512(g)(1); *see generally infra* § 4.12[9][C].

[8]*See 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

---

[9]*See 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).

[11]*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."); *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 photographs[14] 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 use[16] 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.

[15]*See 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).

[16]*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, 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 Paparrazzi 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*

license[17]).[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].

[19] *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, 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]]

[1] *See supra* § 4.12[3].

[2] 17 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

---

[3] *See, e.g.*, *English v. General Elec. Co.*, 496 U.S. 72, 79 (1990).

[4] A *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,

---

[5] 17 U.S.C.A. § 512(g)(1).

[6] 17 U.S.C.A. § 512(m)(1). *Standard technical measures* are discussed above in § 4.12[3][C].

[7] 17 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 limitations[1] 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-

---

[10] *See* 47 U.S.C.A. § 230(c)(2); *see generally infra* § 37.05.

[Section 4.12[9][A]]

[1] Whether 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].

[2] The 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.

[3]17 U.S.C.A. § 512(g).

[4]17 U.S.C.A. § 512(c)(2).

[5]The 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).

[6]17 U.S.C.A. § 512(c)(2); 73 Fed. Reg. 29654, 29668 (May 21, 2008).

[7]In *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.

[8]37 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 agents[10] 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 Offices 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

---

[10] *See* Notice of Proposed Rulemaking, 76 Fed. Reg. 59,953 (Sept. 28, 2011).

[11] *See* 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.

[12] 37 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]

---

[17]Designation of Agent to Receive Notification of Claimed Infringement, 63 Fed. Reg. 59233, 59234 (Nov. 3, 1998).

[18]*See supra* § 4.08[2]; *infra* § 4.19.

[19]*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 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).

[21] 17 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

[22] *See 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-

---

[24] *See infra* chapter 53 (analyzing personal jurisdiction over U.S. and foreign entities).

[Section 4.12[9][B]]

[1] 17 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 tools[3] 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

---

[2] *See* 17 U.S.C.A. § 512(d)(2)(E).

[3] *See* 17 U.S.C.A. § 512(d)(3).

[4] 17 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).

[7] *See, 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 notification[10] 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).

[8]*See 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).

[9]*See 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.").

[10]17 U.S.C.A. § 512(g)(2)(A) (emphasis added).

[11]*See* 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 authorized[16] 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).

[15]In *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.

[16]In *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

---

quiry 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).

[17] 17 U.S.C.A. § 512(c)(3)(A) (emphasis added).

[18] *See* 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.pictures.erotica.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

---

[19]17 U.S.C.A. § 512(c)(3)(B)(ii).

[20]Although 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 material[23] 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]

---

[22]RemarQ 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.

[23]As 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."

[24]*See* 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.

[26]*See 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).

[34]In 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.

[35]*See 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).

[37]As 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.

[38]Among 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).

[47]An 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].

[48]*See* 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].

[49]These three requirements are set forth in sections 512(c)(3)(A)(ii), 512(c)(3)(A)(iii) and 512(c)(3)(A)(iv).

[50]*See* 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 act[53] (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

---

[51] 17 U.S.C.A. § 512(c)(3)(B)(i).

[52] 17 U.S.C.A. § 512(c)(3)(B)(ii).

[53] *See 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).

[54] As 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 DMCA[55] 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

---

[55] *See infra* § 4.12[9][D].

[56] *See infra* § 4.12[9][F].

[57] *See, 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]]

[1] 17 U.S.C.A. § 512(g)(1).

[2] *See 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).

[4]17 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 Act[1]—infringement claims or counterclaims initiated with the Copyright Claims Board may also suffice to meet the

---

[5]*See* 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).

[6]*See* 17 U.S.C.A. § 512(g)(3).

[7]17 U.S.C.A. § 512(g)(2).

[1]*See* 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 court[3] but who could initiate a claim or counterclaim before the Copyright Claims Board and hold it in abeyance potentially for a year or more[4]) 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

---

[2] *See* 17 U.S.C.A. § 1507(d).

[3] *See supra* § 4.08[2].

[4] *See* 17 U.S.C.A. § 1505; *see generally supra* § 4.08[8] (explaining this provision and analyzing the CASE Act).

[5] *See* 17 U.S.C.A. § 1506(i).

[6] *See* 17 U.S.C.A. § 1504(d)(4).

[7] *See* 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 DMCA[9] 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.

---

[8]*See* 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.").

[8]*See supra* § 1.06.

[9]*See infra* § 4.12[9][D].

[10]*See 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 notifications[1] (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]]

[1]Although 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 nonresident 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-

---

[6]According 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).

[7]*See 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.

[8]17 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)).

[13]In *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 DMCA[16] 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).

[16]The 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.

[27]The *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 plaintiff's 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

[32] *See* 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. Crossly-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.

[37]In 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).

[38]The 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

---

[41]*See Biosafe-One, Inc. v. Hawks*, 639 F. Supp. 2d 358, 369–70 n.3 (S.D.N.Y. 2009).

[42]*See, 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].

[43] *See supra* § 4.12[9][C].

[44] *See supra* § 4.12[9][C].

[45] *See, 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'

---

[47]That 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.

[48]558 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).

[50]This 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 section[52]—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).

[52]*See 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).

[53]*See, 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].

[54]*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-

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]]

[1]17 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).

[2]It is unclear whether Congress meant by this language to authorize national jurisdiction. *See infra* chapter 53.

[3]17 U.S.C.A. § 512(h)(1).

[4]17 U.S.C.A. § 512(h)(2).

[5]17 U.S.C.A. § 512(h)(4).

[6]17 U.S.C.A. § 512(h)(3).

[7]17 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 communications[10] safe harbor).[11]

Hence, in cases involving peer-to-peer file sharing where

---

[8]For more information on suing anonymous and pseudonymous Internet actors, *see infra* §§ 37.02, 50.06, 57.03.

[9]*See, 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).

[10]17 U.S.C.A. § 512(a).

[11]*See, 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).

[12]*See, 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 "focuse[d] 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).

[14]17 U.S.C.A. § 512(h)(2)(A).

[15]17 U.S.C.A. § 512(h)(2)(C).

[16]17 U.S.C.A. § 512(h)(5).

[17]17 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).

[18]If 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.

[19]*See, 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 pseuonynous 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).

[20]*See, 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).

[22]*See, 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).

[23]*See 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).

[24] *See 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

---

[25]*See 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).

[26]*See 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 embarrassment[27]—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]

---

[27]*See, 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.").

[29]*See, 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.").

[30]*See, 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 statutes[1] 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 claim[4] or on summary judgment. In at least one case, a state court in Califor-

---

[Section 4.12[9][F][i]]

[1]Anti-SLAPP statutes are analyzed more extensively in section 37.02[3].

[Section 4.12[9][F][ii]]

[1]*See* 17 U.S.C.A. § 512(g); supra § 4.12[8].

[2]*See* 17 U.S.C.A. § 512(f); supra § 4.12[9][D].

[3]*See, e.g.*, *Gade v. National Solid Wastes Management Ass'n*, 505 U.S. 88, 98 (1992).

[4]*See, 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).

[5]*See 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 law[11] 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).

[11]Cal. 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).

[12]*See 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.").

[13]*See infra* § 37.02[3] (analyzing the anti-SLAPP Statute).

[14]*See 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 DMCA[18] and for cybersquatting, trademark cancellation, trade libel, interference with contract and prospective economic advantage and a declaratory ruling of noninfringement 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

---

[15]*See infra* chapter 35 (analyzing the case and others in the context of field preemption).

[16]*See, 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).

[18]*See supra* § 4.12[9][D].

[19]*See, 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]), *Fatwallet, 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

---

[20] *See generally supra* § 4.12[9][C]; *infra* § 22.05[2][F].

[21] *See* 17 U.S.C.A. §§ 1501 to 1511.

[Section 4.12[9][F][iii]]

[1] Copy 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.

[5]*See, 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).

[6]*See Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082 (C.D. Cal. 2001); *see generally supra* § 4.12[6][A].

[7]*See 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]]

[1]17 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].

[2]17 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 storage[2] or information location tools[3] 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]]

[1] *See supra* § 4.12[5].

[2] *See supra* § 4.12[6].

[3] *See supra* § 4.12[7].

[4] 17 U.S.C.A. § 512(j)(1)(A).

[5] 17 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

[6] *See 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

---

[7] *See* 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].

[9] *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].

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 statute[4] 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]]

[1]*See supra* § 4.12[9].

[2]*See 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).

[3]*See* 17 U.S.C.A. § 512(l).

[4]*See 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

---

[5] *See supra* § 4.12[9][C].

[6] The 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

[7] 17 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

[8]Unscrupulous 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 limitation[2] 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]]

[1] *See supra* § 4.12[8].

[2] *See 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

---

[3] *See infra* § 4.12[14].

[4] *See 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

---

[5] *See 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.

[6] *See* 17 U.S.C.A. § 512(l).

[Section 4.12[14]]

[1] The 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:

---

[3] *See Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984); *see generally supra* § 4.10.

[4] *See supra* § 4.11[8][C].

[Section 4.12[15]]

[1] This 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

[2]*See 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

---

[3]Where 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].

[4]Although 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]]

[1]If 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).

[2]Copyright 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]]

[1]17 U.S.C.A. § 512(c).

[2]*See 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 Principles[1]

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]]

[1]Available 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 statistics[1] 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]]

[1]*See 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 cases[3] 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).

[3]The 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 case[7] 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

---

[5]633 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 06-1093FMCJCX, 2007 WL 2080419 (C.D. Cal. May 29, 2007).

[9]Spoliation 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 Grooveshark 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).

[14]253 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).

[16]*See generally infra* §§ 58.03[5] (spoliation), 58.03[6] (fee shifting), 58.04[4] (discovery sanctions).

[Section 4.12[19]]

[1]*See* 17 U.S.C.A. § 301; *see generally infra* § 4.18.

[2]The Orrin G. Hatch–Bob Goodlatte Music Modernization Act, PL 115-264, 2018 H.R. 1551, 132 Stat. 3676 (Oct. 11, 2018).

[3]*See* 17 U.S.C.A. § 1401(f)(3).

[4]*See* 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).

[7] *See 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 2023

Ian C. Ballon

2023 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 IanBallon.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 pricy 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

SUMMARY OF CONTENTS

Volume 1

Volume 2

Volume 3

Volume 4

Volume 5

"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 2023, 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.lanBallon.net).

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

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 2023

- **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 cybersecurty 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)