Convergence and Conflation in Online Copyright

Christopher A. Cotropia[*] *& James Gibson*[**]

ABSTRACT: The Digital Millennium Copyright Act ("DMCA") is showing its age. Enacted in 1998, the DMCA succeeded in its initial goal of bringing clarity to wildly inconsistent judicial standards for online copyright infringement. But as time has passed, the Act has been overtaken—not by developments in technology, but by developments in copyright's case law. Those cases are no longer as divergent as they were in the last millennium. Instead, over time the judicial standards and the statutory standards have converged, to the point where the differences between them are few. The statute whose ascendance was once central to the governance of copyright online is therefore now diminished in importance.

At first glance, this development seems unproblematic. After all, uniformity was the DMCA's goal, and convergence gets us closer to it. But a deeper look reveals that convergence has significantly changed the cost/benefit calculus for those whom the Act governs. The benefits of complying with the Act's regulatory requirements have decreased, because convergence means that one can ignore the statute and rely solely on the case law. And the costs of complying have increased, because convergence has paradoxically given rise to a new, troubling phenomenon: the mixing and matching of statutory and judicial standards in unpredictable and counterproductive ways, which create new, unintended forms of copyright liability and immunity. In short, convergence has led to conflation, which means that the best course for today's online community is to steer clear of the DMCA altogether.

---

[*] Dennis I. Belcher Professor of Law and Director of the Intellectual Property Institute, University of Richmond School of Law. The authors would like to acknowledge the considerable help they received from Shyam Balganesh, Sandra Braman, AnneMarie Bridy, Dan Burk, Jud Campbell, Hank Chambers, Erin Collins, Kenny Crews, Graeme Dinwoodie, Stacey Dogan, Jessica Erickson, Dave Fagundes, Linda Fairtile, Joe Fishman, Jeanne Fromer, Kristelia Garcia, Lolly Gasaway, Cathy Gellis, Deborah Gerhardt, Andrew Gilden, Eric Goldman, Laura Heymann, Justin Hughes, Dmitry Karshtedt, Daphne Keller, Doug Lichtman, Lucretia McCulley, Tyler Ochoa, Jack Preis, Jennifer Rothman, Noah Sachs, Matt Sag, Jessica Silbey, Shannon Sinclair, Scott Tilghman, Rebecca Tushnet, Rob Tyler, Fred Yen, and Peter Yu. They would also like to thank Brad Stringfellow for his excellent research assistance.

[**] Sesquicentennial Professor of Law, University of Richmond School of Law. In addition to those acknowledged above, Jim would like to thank Jane Savoca, his safe harbor from all storms.

I. INTRODUCTION

The Digital Millennium Copyright Act[1] ("DMCA") is the most important piece of copyright legislation of the last 40 years. Enacted in 1998, the DMCA did many things, but its hallmark achievement was to immunize the routine operations of online service providers from (most) liability for copyright infringement.[2] By doing so, the Act used statutory law to create national

1. Digital Millennium Copyright Act, Pub. L. No. 105-304, § 1, 112 Stat. 2860, 2860 (1998); *see also* JESSICA LITMAN, DIGITAL COPYRIGHT 143 (2001) (discussing in detail the creation of the DMCA).

2. *See* Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 COLUM. L. REV. 1194, 1195–96 (2011) ("Not surprisingly, the congressional solution represented a compromise between the demands of the content industries to impose liability on internet intermediaries and the pleas of the internet industries to afford them sufficient breathing room

uniformity, replacing judicial standards that varied greatly from jurisdiction to jurisdiction and paving the way for the user-content platforms that dominate modern culture and commerce.[3] It is no exaggeration to say that YouTube, Facebook, and the like might not exist were it not for the rise of the DMCA.[4]

What the Act did not do, however, was set the standards for online copyright infringement. Instead, it established four safe harbors—telling us what conduct did not infringe copyright, rather than telling us what conduct did infringe.[5] Federal courts therefore retained considerable power to define what actually constituted infringement online.[6] When a service provider's conduct fell within a safe harbor, a court could still find infringement, because the safe harbor merely limited the available remedies rather than providing absolute immunity.[7] The inverse was true as well: Conduct that fell outside a safe harbor would not qualify as infringing unless the courts said so.[8] What this meant is that even after passage of the legislation, courts were free to fashion liability standards that favored service providers or copyright owners, as they saw fit.

Nevertheless, over the past 20 years courts have declined this opportunity. No independent case law of online copyright infringement has developed. Instead, the judicial standards and the statutory standards have converged. The case law's standards for liability have become the mirror image of the safe harbor standards for immunity. In other words, when a service provider is liable for copyright infringement, it also fails to fall within

---

to operate and grow."); *see also* Niva Elkin-Koren, *Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 15, 17 (2005) ("The safe harbor regime provided ISPs with a shield that mostly kept them out of copyright wars.").

3. *See* Matthew Sag, *Internet Safe Harbors and the Transformation of Copyright Law*, 93 NOTRE DAME L. REV. 499, 510 (2017) ("As the term 'safe harbor' suggests, Title II of the DMCA was intended to offer legal certainty to internet service providers and online platforms if their conduct stayed within certain parameters.").

4. *See, e.g.*, *id.* at 504–05 ("The DMCA safe harbors have been a tremendous benefit to the U.S. copyright system and to the U.S. economy. . . . [T]he internet safe harbors have propelled the growth of social networking and other 'Web 2.0' businesses."); Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 269 (2009) ("[T]he DMCA safe harbors have helped to foster tremendous growth in web applications.").

5. *See* 17 U.S.C. § 512(a)–(d) (2012) (defining the substantive requirements for falling within one of the four the safe harbors).

6. H.R. REP. NO. 105-796, at 73 (1998) ("Section 512 is not intended to imply that a service provider is or is not liable as an infringer either for conduct that qualifies for a limitation of liability or for conduct that fails to so qualify. Rather, the limitations of liability apply if the provider is found to be liable under existing principles of law.").

7. *See* 17 U.S.C. § 512(j) (allowing for injunctive relief even against service providers who qualify for immunity under one of the safe harbors).

8. *See id.* § 512(l) (noting that "[t]he failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense").

the safe harbors—and those that do fall into the safe harbors are never found liable.

At first glance, this convergence of statute and case law seems unproblematic. After all, Congress clearly expressed a policy preference when it defined the safe harbors, so why wouldn't courts simply take the cue and mold liability standards to mimic the contours of the statutory safe harbors? Moreover, uniformity was the DMCA's goal, and convergence gets us closer to it.

On closer inspection, however, convergence has had two dubious effects. First, it has altered the cost/benefit calculus inherent in the statutory scheme. The benefits side of the calculus has changed because service providers can now rely on the case law alone to immunize them from liability, without having to incur the regulatory costs of DMCA compliance. (Indeed, we will present some empirical evidence suggesting that many online service providers are already taking this path.) And the cost side of the calculus has changed because convergence has begun to paradoxically cause courts to conflate irrelevant DMCA provisions with the substantive law of infringement, giving rise to new, unintended, and unwarranted forms of both copyright liability and copyright immunity. In short, convergence has led to conflation, and the result is a statute that may now be doing more harm than good.

This Article proceeds as follows. In Part II, we explain why and how the DMCA was originally enacted, the important role it played at the time, and the power that courts had to define liability even after the Act's passage. Part III shows that over the ensuing two decades, the case law's liability definitions converged with the DMCA's safe harbor standards, leaving almost no daylight between the statute and the case law. Part IV demonstrates that this convergence has decreased the upside of the DMCA safe harbors, increased the downside, and produced harmful conflation of legal standards that should have remained separate. In the end, then, the once-vital DMCA may now be a net loss for copyright law.

II. CREATION

A. COURTS

Back in the early days of the Internet, long before Instagram, Twitter and Reddit, there was Usenet. Essentially a vast electronic message board organized into subject-specific "newsgroups," Usenet may seem pedestrian today, when almost every website has user forums and threaded discussions. But at the time, the main sources of online content were closed communities like America Online, where the variety of material was limited by the fact that the provider had to develop everything itself. In contrast, Usenet was entirely user-generated. It was the first platform that revealed the mind-boggling diversity of content that the Internet could supply through the collective

efforts of millions of everyday users.[9] One could find Usenet newsgroups on topics as varied as homebuilt airplanes, non-parasitic transparent nematodes, and real and imaginary bunnies who cause trouble.[10]

As with any platform based on user-generated content, Usenet came with the risk that unlicensed copyrighted material would make its way into the system. That's what happened in 1994, when Dennis Erlich, a minister-turned-critic of the Church of Scientology, posted several critiques of the Church in Usenet's alt.religion.scientology newsgroup. The critiques included excerpts from the writings of Scientology's founder, L. Ron Hubbard, whose copyrights were owned by Religious Technology Center ("RTC"), the Church's publishing arm.[11] RTC filed a federal lawsuit in California, and the court soon issued a preliminary injunction against Erlich's continued posting of the Scientology material, finding it likely that he had violated copyright law.[12]

The case got really interesting, however, when the court considered RTC's claims against two other parties, Tom Klemesrud and Netcom On-Line Communication Services. Klemesrud operated a small electronic bulletin board service through which his subscribers (of which Erlich was one) could access the Internet. And Klemesrud's bulletin board was able to provide that access because it was itself a customer of Netcom, which at the time was one of the country's largest Internet service providers.[13] To put it simply, Erlich's excerpts of the Scientology material were able to reach Usenet subscribers because Klemesrud connected Erlich to his electronic bulletin board and because Netcom connected the bulletin board to the Internet. So the networks the two parties operated had played an undeniable role in providing Erlich's postings to the many servers around the world that carried Usenet content. The question was whether that intermediary role warranted the imposition of copyright liability.[14]

The precedents on this question were few. The previous year, in *Sega Enterprises Ltd. v. MAPHIA*, a judge in the same California district had issued a preliminary injunction against the operator of an electronic bulletin board

9. This bottom-up, user-controlled nature of Usenet is reflected in its name, which derived from "Unix Users' Network"—a network of Unix programmers who created the platform in 1979 to discuss the problems and experiences with the popular programming language. *See* Michael Hauben, *The Social Forces Behind the Development of Usenet*, *in* RONDA HAUBEN & MICHAEL HAUBEN, NETIZENS: ON THE HISTORY AND IMPACT OF USENET AND THE INTERNET 31–39 (1997).

10. Those would be the Usenet newsgroups rec.aviation.homebuilt, bionet.celegans, and alt.devilbunnies, respectively.

11. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1365 (N.D. Cal. 1995).

12. *Id.* at 1365 n.3.

13. *Id.* at 1366.

14. *Id.* at 1367.

on which users had posted unlicensed copies of videogames.[15] But the defendant in that case was hardly an unknowing intermediary; he had actively solicited the infringing content, going so far as to reward users who uploaded copyrighted material.[16] In contrast, neither Klemesrud nor Netcom had any idea that Erlich had posted the Scientology material until RTC contacted them.[17]

The only case on the books that involved an online intermediary unaware of its user's infringement was a short opinion from a federal court across the country in Florida, *Playboy Enterprises v. Frena*.[18] George Frena, an operator of an online bulletin board much like Klemesrud's, had been sued by Playboy for hosting user-submitted photos that had been copied from the well-known pornography magazine. Frena claimed that he had not uploaded the photos himself, had deleted them as soon as he learned of them, and had subsequently monitored the bulletin board to ensure that his subscribers uploaded no more Playboy material.[19] The court assumed that these assertions were true, but it made no difference; the fact that Frena oversaw the network that hosted the photos was enough to merit summary judgment for Playboy.[20] Frena's protestations—that others had done the actual uploading and downloading, and that he knew nothing of it—fell on deaf ears. Copyright infringement was a strict liability transgression, and so Frena's lack of knowledge was irrelevant to the question of liability.[21]

---

15. Sega Enters. Ltd. v. MAPHIA, 857 F. Supp. 679, 682 (N.D. Cal. 1994). There was also a second case in which RTC sued the operators of an electronic bulletin board for posting copyrighted Scientology materials without a license, but it was not a case of intermediary liability; the operators were anti-Scientology activists who had posted the materials themselves. *See* Religious Tech. Ctr. v. F.A.C.T.NET, Inc., 901 F. Supp. 1519, 1524 (D. Colo. 1995); *see also* Religious Tech. Ctr. v. Lerma, 897 F. Supp. 260, 267 (E.D. Va. 1995) (rejecting preliminary injunction against activist's posting of Scientology materials online).

16. *MAPHIA*, 857 F. Supp. at 683–84. The same was true of a post-*Netcom* case with facts and reasoning quite similar to *MAPHIA*. *See also* Sega Enters. Ltd. v. Sabella, No. C 93-04260 CW, 1996 WL 780560, at *7–8 (N.D. Cal. Dec. 18, 1996). Today we would refer to such cases as involving inducement liability, a form of contributory liability. *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005) ("One infringes contributorily by intentionally inducing or encouraging direct infringement.").

17. *Netcom*, 907 F. Supp. at 1374 ("It is undisputed that Netcom did not know that Erlich was infringing before it received notice from plaintiffs."); *id.* at 1382 ("A letter attached to the complaint indicates that such notice was first sent to Klemesrud on December 30, 1994.").

18. Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993). We will refer to this case as *Frena*, rather than *Playboy*, because Playboy was the plaintiff in at least a half dozen other seminal Internet law cases. *See* Christopher A. Cotropia & James Gibson, *The Upside of Intellectual Property's Downside*, 57 UCLA L. REV. 921, 964 n.188 (2010).

19. *Frena*, 839 F. Supp. at 1554.

20. *Id.* at 1559.

21. *Id.* (recognizing that "[i]t does not matter that Defendant Frena may have been unaware of the copyright infringement" but rather intent and knowledge are relevant only to determining the proper remedy for infringement).

In contrast, the court in *Religious Technology Center v. Netcom On-Line Communications Services, Inc.* looked much more closely at the role that the intermediaries had played in making the infringing content available. That Erlich himself was liable was not seriously in question. His uploading of the Scientology material clearly constituted unauthorized reproduction under 17 U.S.C. § 106(1), and the court had already found it unlikely that he would be able to mount a fair use defense.[22] Once the excerpts were uploaded, however, more reproduction took place. Klemesrud's bulletin board system automatically created an additional copy and sent it along to Netcom's servers, which then made and transmitted copies to other nodes in the Usenet network.[23] Indeed, within a few hours of Erlich's initial upload, copies of the Scientology materials had appeared on every Usenet server around the world.[24]

The question was whether Klemesrud and Netcom were liable for those additional unauthorized reproductions.[25] That liability could come in two forms. First, they might be directly liable. In other words, by virtue of operating the computer systems that made the copies, Klemesrud and Netcom might be seen as having made copies themselves, much as Erlich had.[26] Second, they might be secondarily liable; even if Erlich was the only direct infringer, Klemesrud and Netcom might have facilitated or profited from his direct infringement in a manner that made them legally responsible for it.

With regard to the direct infringement question, the *Netcom* court did not dispute that infringing copies were made, but it found that Klemesrud and Netcom had not made them.[27] Both parties merely maintained a computer "system that automatically and uniformly create[d] temporary copies of all data sent through it," much like "the owner of a copying machine who lets the public make copies with it."[28] Neither party initiated the copying of the Scientology materials—that was Erlich's doing—and the propagation of

22. *Netcom*, 907 F. Supp. at 1367.

23. *Id.*

24. *Id.* at 1367–68.

25. *Id.* at 1368.

26. We focus here, as the *Netcom* court did, on liability for unauthorized reproduction of the Scientology materials, because it is indisputable that posting content to Usenet creates multiple new copies of that content—and making new copies is the essence of unauthorized reproduction. *See* 17 U.S.C. § 101 (2012) (definition of "copies"); *id.* § 106(1) (defining reproduction as the making of "copies"); *Netcom*, 907 F. Supp. at 1368–71 (addressing direct liability for unauthorized reproduction). Curiously, the *Frena* court had not addressed whether the defendant there had engaged in unauthorized reproduction, focusing instead on unauthorized distribution under § 106(3) and unauthorized public display right under § 106(5). *Frena*, 839 F. Supp. at 1556–57. That said, *Netcom*'s focus on reproduction did not keep it from addressing the possibility of direct infringement of the distribution and display rights as well; it disposed of them on the same basis as the reproduction right. *Netcom*, 907 F. Supp. at 1371–72.

27. *See Netcom*, 907 F. Supp. at 1383.

28. *Id.* at 1369.

copies into Usenet happened mechanically and indiscriminately once Erlich posted, without any further intervention by Klemesrud or Netcom.[29] Like *Frena*, the *Netcom* court acknowledged that copyright infringement was a strict liability offense, but it asserted nevertheless that "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."[30] (As we will see, this volitional requirement would prove important later, when Congress took up the issue.)

As for secondary infringement, it too came in two varieties. The first was contributory liability, which applied to parties who knowingly and substantially participated in another's direct infringement.[31] The court held that providing the means by which Erlich's Usenet posts were copied and disseminated to the world constituted substantial participation.[32] But the requisite knowledge was not present when Klemesrud and Netcom set up their systems and signed up customers like Erlich; at the time, they had no idea whether a customer would use Usenet at all, let alone post infringing Scientology material (as opposed to, say, sharing advice on homebuilt airplanes or stories about real and imaginary bunnies).[33] Later, however, RTC notified them of Erlich's doings. Once that happened, the court held, it was harder for Klemesrud and Netcom to plead ignorance, and there was accordingly a triable issue of fact regarding whether they then knowingly contributed to the infringement by continuing to host the infringing material.[34]

The second variety of secondary infringement was vicarious liability, which focused not on knowledge but on whether the defendants had the right and ability to control Erlich's infringement and received a direct financial benefit from it.[35] The plaintiff introduced evidence that both Klemesrud and Netcom could suspend subscribers and delete postings, creating a triable issue on their right and ability to control what Erlich did.[36] But the court found no direct financial benefit as a result of Erlich's postings—no causal connection between his infringement and Klemesrud and Netcom's revenues.[37]

---

29. *Id.*

30. *Id.* at 1370.

31. *Id.* at 1373–75.

32. *Id.* at 1375.

33. *Id.* at 1374. This enabled the court to distinguish *Sega v. MAPHIA*, in which the defendant knew and even encouraged the uploading of infringing content. *Id.* at 1371 & n.17 (citing Sega Enters. Ltd. v. MAPHIA, 857 F. Supp. 679, 683 (N.D. Cal. 1994)).

34. *Id.* at 1374–75, 1382.

35. *Id.* at 1375.

36. *Id.* at 1375–76, 1382 (discussing the *Netcom* and *Klemesrud* cases).

37. *Id.* at 1376–77, 1382 (discussing *Netcom* and *Klemesrud*). This too helped the court distinguish *Sega v. MAPHIA*, where the defendant's business model was built on soliciting uploads of video games and then charging for downloads. *Id.* at 1371, 1379. Note also that in Klemesrud's case, the court gave RTC leave to amend the complaint to include allegations of "direct financial benefit" sufficiently specific to revive the vicarious liability claim. *Id.* at 1382.

In the end, then, the court ruled as a matter of law that Klemesrud and Netcom did not directly infringe RTC's copyrights. This represented a clear break with *Frena*, which had imposed direct liability for the exact same kind of conduct.[38] The *Netcom* court also opined on secondary liability (which *Frena* had not done), finding no vicarious liability as a matter of law but leaving room for the possibility of contributory liability once RTC informed the defendants of Erlich's conduct.[39]

The small scale of the infringements here makes it easy to overlook the significance of the issue that these holdings addressed. In the 1990s, online connectivity was transforming from a niche market into a ubiquitous utility. A new generation of Internet users was looking to create, rather than just consume, online content. Hypertext Markup Language had recently arrived on the scene, allowing unskilled users to create modern-day, multimedia websites.[40] An explosion of user-generated content lurked right around the corner—GeoCities, Blogger, Friendster, MySpace, Digg, Bebo, and other now-forgotten but once-dominant platforms—the Facebooks and YouTubes of their day. Whether the explosion would happen, however, depended on the direction copyright law would take. If *Frena* were the governing standard, those who provided the connectivity indispensable to Web 2.0 would be answerable for the liability of whoever used those platforms to violate copyright law.[41] Under *Netcom*, on the other hand, the providers could operate without fear of liability, at least until a copyright owner alerted them to a specific instance of infringement. The stakes could not be higher. And all we

38. As mentioned *supra* notes 19–25 and accompanying text, *Frena* based direct liability on the distribution and public display of the plaintiff's copyrighted works, whereas *Netcom* was more about reproduction. For the purposes of allocating responsibility between user and intermediary, however, that's a distinction without a difference. The *Netcom* court seemed to understand this; it made some half-hearted attempts to distinguish *Frena*, but it did not seem to convince even itself. *Netcom*, 907 F. Supp. at 1370–72 (noting that the distribution and display argument "suffers from the same problem of causation as the reproduction argument"). The same goes for *Sega v. MAPHIA*. *See id.* at 1371 & n.17 (proposing ways to distinguish the case but also stating that "[t]o the extent that *Sega* holds that BBS operators are directly liable for copyright infringement when users upload infringing works to their systems, this court respectfully disagrees").

39. The *Netcom* court also split with *Frena* in finding a triable fair use defense. *Compare Netcom*, 907 F. Supp. at 1380–81 (finding triable issue on "market effect" fair use factor), *with* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1558-59 (M.D. Fla. 1993) (rejecting fair use defense due to no triable issue on any fair use factor). As will become apparent below, however, fair use has not played a significant role in mediating these conflicts between copyright owners and online service providers; instead, the most important defense has been the DMCA safe harbors.

40. *See, e.g.*, Karen Kaplan & Charles Piller, *Yahoo to Buy GeoCities for $3.9 Billion in Stock*, L.A. TIMES (Jan. 29, 1999, 12:00 AM), https://www.latimes.com/archives/la-xpm-1999-jan-29-fi-2730-story.html [https://perma.cc/E598-UXV8] (noting how GeoCities was founded in November 1994).

41. "Web 2.0" refers to the modern-day online environment that emphasizes user-generated content—and the hardware and software connectivity necessary to make such content possible. *See* Grant Blank & Bianca C. Reisdorf, *The Participatory Web: A User Perspective on Web 2.0*, 15 INFO. COMM. & SOC'Y 537, 537–39 (2012).

had to guide us was two district court cases from opposite sides of the country, and opposite sides of the issue.

B. CONGRESS

1. The Road to Legislation

The Internet, by its very nature, is transjurisdictional. Having one legal standard in one jurisdiction and a second, conflicting legal standard in a second jurisdiction therefore presented online service providers with a thorny risk-management situation. The conservative approach would be to default to the more demanding *Frena* standard and simply not host Usenet posts and other user-generated content. But doing so would throttle the growth of Web 2.0, all based on a single judge's opinion. And even if *Frena* had agreed with *Netcom*, uncertainty would still prevail, because the next court to take up the issue might have a different approach.[42] Online service providers and copyright owners alike deserved a uniform, national standard.

The case law might eventually produce such a standard. Federal district court opinions like *Netcom* and *Frena* could give rise to federal circuit court opinions, and then perhaps to a Supreme Court opinion that would settle the matter. That would take time, however, and there would be no guarantee that the Supreme Court would take the case. It didn't help that neither *Frena* nor *Netcom* was appealed. Nor did either approach immediately begin to dominate in other jurisdictions; some courts liked *Netcom*,[43] whereas others favored *Frena*.[44]

In the end, given the importance of a timely, certain resolution of the issue, there was no reason to leave it to the judiciary. Congress was the obvious alternative. And as it happened, the Clinton Administration had created the Information Infrastructure Task Force ("IITF") just a few months before the *Frena* ruling.[45] Comprising representatives from various federal agencies, the IITF was responsible for developing a National Information Infrastructure, "a seamless web of communications networks, computers, databases, and consumer electronics" that would "change forever the way people live, work,

---

42. Prior to the enactment of the DMCA, federal statutory law was silent regarding the copyright issues that arose in *Frena* and *Netcom*; all the relevant law originated in court decisions. *See Netcom*, 907 F. Supp. at 1373 (noting that "there is no statutory rule of liability for infringement committed by others").

43. *See, e.g.*, Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1177–79 (N.D. Ill. 1997).

44. *See, e.g.*, Playboy Enters., Inc. v. Webbworld, Inc., 991 F. Supp. 543, 551–54 (N.D. Tex. 1997), *aff'd*, 168 F.3d 486 (5th Cir. 1999). *Webbworld* represented one of the few appellate court decisions on the issue, but the Fifth Circuit's opinion consisted of a single sentence: "We affirm essentially for the reasons stated by the trial judge." *Webbworld*, 168 F.3d at 486.

45. The National Information Infrastructure: Agenda for Action, 58 Fed. Reg. 49,025, 49,035 (Sept. 21, 1993).

and interact with each other."[46] Among the subgroups of the task force was the Working Group on Intellectual Property Rights, which focused primarily on the role copyright would play in this new infrastructure.[47] The idea was to translate the Working Group's findings into federal legislation that would fulfill the need for national standards governing online copyright.

In July 1994, the Working Group released a preliminary draft report, commonly known as the Green Paper.[48] The report covered a multitude of issues, but it consistently characterized the existing law in ways that favored copyright owners over users, and its recommendations were similarly one-sided.[49] On the specific issue of online intermediary liability, however, the Green Paper was more circumspect; it acknowledged the uncertainty over direct versus secondary liability claims and over which particular kind of infringement was implicated online.[50] But by the time the Working Group issued its final report (the so-called White Paper), the uncertainty was gone. The report favorably cited *Frena* and *MAPHIA* (the unlicensed videogame distribution case)[51] and firmly concluded that "the best policy is to hold the service provider liable" for its users' copyright infringement.[52] The fact that such liability would require reviewing all user-submitted content before it was posted was simply one of the "costs of doing business,"[53] excused only in the vanishingly rare instance in which a user encrypted the content.[54]

The Clinton Administration then took the White Paper to Congress, expecting that its recommendations would quickly become federal legislation

---

46. *Id.* at 49,025.

47. *See* INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 2 (1995) [hereinafter WHITE PAPER].

48. INFORMATION INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: A PRELIMINARY DRAFT OF THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS (1994) [hereinafter GREEN PAPER].

49. *See* LITMAN, *supra* note 1, at 91 (noting that the report's suggestions largely "echoed those made by [copyright] industry representatives" and that "what it characterized as minor clarifications . . . appeared to many interested observers to attempt a radical recalibration of the intellectual property balance"). It is noteworthy that all but one of the report's seven law-related recommendations would have expanded copyright owner rights—and the one exception was merely a call for a conference to discuss the narrow topic of fair use in libraries and schools. *See* GREEN PAPER, *supra* note 48, at 120–39.

50. GREEN PAPER, *supra* note 48, at 40–42, 76; *see also supra* notes 26–39 and accompanying text (explaining direct and secondary liability issues); *supra* note 26 (explaining § 106 issues).

51. WHITE PAPER, *supra* note 47, at 120–21. When the final report was released in September 1995, *Netcom* had not yet been decided. *See id.* at 122 n.391 (referencing pending case).

52. *Id.* at 117.

53. *Id.* at 118; *see also* LITMAN, *supra* note 1, at 128 ("The clear implication was that henceforth, this sort of liability would give content owners a deep pocket to sue; fear of liability would drive service providers to agree to a variety of measures designed to choke off, deter, or avenge infringement by their customers.").

54. WHITE PAPER, *supra* note 47, at 122 (allowing for possibility of exemption from liability "for an on-line service provider who unknowingly transmitted encrypted infringing material").

and thereby provide the much-needed national standard governing copyright online.[55] It turned out, however, that Internet service providers and others in the telecommunications industry were not going down without a fight. Adding fuel to the fire, *Netcom* was decided just a few months after the White Paper was published, giving the opposition a blueprint for an approach very different from the White Paper's.[56] In the end, then, Congress did address the need for a uniform standard for online intermediary liability. But as we will now see, notwithstanding the Clinton Administration's efforts, that national standard looked a lot more like *Netcom* than it did *Frena*.

2. The DMCA's Structure

Congress provided the solution to the problem of intermediary liability in Title II of the Digital Millennium Copyright Act. Its official title is the Online Copyright Infringement Liability Limitation Act,[57] but Title II is generally known simply as the DMCA safe harbors. Indeed, the phrase "safe harbor"—although it does not actually appear in the statute—is key to understanding exactly how the legislation addressed the liability problem. Rather than defining the standards for copyright liability in the online world, as *Netcom* and *Frena* had each attempted to do, the DMCA established four specific kinds of conduct for which service providers would enjoy limited immunity from copyright liability. In other words, Congress defined liability in the negative, setting forth four categories of online conduct that would not lead to liability, but remaining silent as to liability for conduct that fell outside those four safe harbors.

i. The "Access" Safe Harbors

The main concern of *Netcom*, *Frena*, and their progeny was the role that online intermediaries played in providing ongoing access to infringing materials. It is therefore unsurprising that three of the four safe harbors dealt directly with such access and addressed the difference between providing access as a result of an automatic, technical process and providing access knowingly.

We will begin with the safe harbor found at 17 U.S.C. § 512(c), both because it deals most directly with the scenario that *Netcom* and *Frena*

55. Jessica Litman has written the definitive account of the battle over the White Paper's recommendations—including those having nothing to do with intermediary liability. *See generally* LITMAN, *supra* note 1 (describing the battle). Indeed, her book is an excellent overview of many other aspects of copyright law's development at the end of the millennium.

56. *Id.* at 127–28; *see also* Pamela Samuelson, *The U.S. Digital Agenda at WIPO*, 37 VA. J. INT'L L. 369, 429 (1997) (noting that "the White Paper's legislative package encountered such substantial opposition in the U.S. Congress that it did not even get reported out of the relevant subcommittees").

57. *See* Digital Millennium Copyright Act, Pub. L. No. 105-304, § 201, 112 Stat. 2860, 2877 (1998).

presented and because it has proved to be the most consequential. This safe harbor applies to "Information Residing on Systems or Networks At Direction of Users"—what we will call System Storage.[58] In other words, this is the safe harbor that deals with the fact pattern in which a service provider itself hosts copies of infringing content posted by its users. So this is the safe harbor that would help resolve the split in the case law discussed above and provide a uniform, national standard.

The System Storage safe harbor demonstrates that the White Paper's opponents had won the battle on this issue: Congress clearly chose *Netcom*'s approach over *Frena*'s. Recall that *Frena* treated copies made, distributed, and displayed by users as having been made, distributed, and displayed by the service provider as well, thus leading to strict liability for direct infringement by user and service provider alike. To avoid liability for user-generated content, then, service providers would have to affirmatively monitor all such content and preemptively remove anything that might be infringing.

In contrast, § 512(c) begins by broadly exempting service providers from liability "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."[59] To emphasize this choice of *Netcom* over *Frena*, a later subsection—§ 512(m)—explicitly states that the availability of the safe harbors was not conditioned on "a service provider['s] monitoring its service or affirmatively seeking facts indicating infringing activity."[60] In essence, then, Congress adopted *Netcom*'s approach to direct infringement, requiring something more volitional on the service provider's part before allowing for liability.

The rest of the System Storage safe harbor focuses on secondary infringement. As we saw in the discussion above, secondary infringement occurs when one party is liable for another party's direct infringement, and it takes two forms: vicarious and contributory.[61] The *Netcom* court had addressed each form, and here again the System Storage safe harbor followed the court's lead. The statute reiterates the two vicarious infringement elements from *Netcom* by stating that the safe harbor applies only if the 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."[62] Likewise with contributory infringement; the statute acknowledges that the safe harbor would not protect a service provider who gains actual or constructive knowledge of its user's posting of copyrighted materials and yet

58. 17 U.S.C. § 512(c) (2012).
59. *Id.* § 512(c)(1).
60. *Id.* § 512(m)(1).
61. *See supra* notes 31–37 and accompanying text.
62. 17 U.S.C. § 512(c)(1)(B).

fails to expeditiously remove them.[63] This mirrors the *Netcom* court's approach, which denied summary judgment to the two service providers on the contributory claim due to their failure to take down Erlich's postings after receiving notice of the infringement from the copyright owner.[64]

Indeed, System Storage envisions an important role for notices like those in *Netcom*. From the copyright owner's perspective, the main obstacle to contributory liability was the service provider's lack of knowledge regarding what its users were doing. The most obvious way to overcome this obstacle was for the copyright owner to tell the service provider about the infringement. Once the service provider had that knowledge, its failure to take down the infringing materials would open it up to contributory liability. The System Storage safe harbor therefore explicitly sets forth what specific information such a notice would have to contain (e.g., identification of the infringed work, location of the allegedly infringing material, contact information) in order to comply with the statute.[65] Additionally, the safe harbor required service providers to register an agent for receipt of any notices; failure to do so would mean the safe harbor was unavailable.[66]

In essence, then, the System Storage safe harbor codifies the sort of notice-and-takedown system that *Netcom* implied, but at a higher level of specificity. The core idea is that once the service provider knows of particular infringing material, it can do something about it—namely, stop hosting it. But as in *Netcom*, the burden is on the copyright owner to alert the provider to the ongoing infringement and give it the specific information it needed to take it down.

Two of the other three safe harbors likewise focus on the online availability of infringing materials and were accordingly modeled on System Storage and its notice-and-takedown regime. The safe harbor in § 512(b) addresses System Caching, a process through which a service provider's computers automatically create a local copy of frequently needed data so they can access it more easily. If the data contains copyrighted material, making a copy would ordinarily raise the specter of copyright infringement; as in System Storage, the provider's network itself would essentially be providing the infringing material. The statute therefore treated cached data much like

63. *See id.* § 512(c)(1)(A).

64. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1374–75, 1382 (N.D. Cal. 1995) (discussing first Netcom's denial of its motion for summary judgment and then the denial of Klemsrud's motion for judgment on the pleadings). Of course, knowledge is only one of two elements of contributory infringement. The other element, substantial participation, was satisfied by Netcom and Klemesrud providing the digital networks that allowed Erlich to copy and disseminate the Scientology materials, *id.* at 1375, 1382, and § 512(c) likewise assumes that storage of infringing materials "on a system or network controlled or operated by or for the service provider" constitutes substantial participation, notwithstanding that the storage was "at the direction of a user," 17 U.S.C. § 512(c)(1).

65. 17 U.S.C. § 512(c)(3).

66. *Id.* § 512(c)(2).

hosted data. It granted immunity for caching that truly results from an "automatic technical process" initiated by the selection of data by a user, not by the service provider.[67] But notice and takedown applies here, too: If the source of the cached data is taken down in response to a compliant notice, the cached data is subject to takedown as well.[68]

The safe harbor in § 512(d) also mirrors the System Storage approach to notice and takedown. This safe harbor, which we refer to as Information Location, targets service providers who do not necessarily store infringing material themselves, but who help users gain access to infringing material posted elsewhere, such as search engines or websites with indexed links to pirated movies.[69] Other than that distinction, the Information Location safe harbor is very similar to its System Storage cousin; it does not shield service providers from liability for secondary infringement, and it piggybacks on its cousin's notice-and-takedown framework for streamlining the sending of notices from copyright owners to service providers.[70]

In sum, then, Congress recognized the difficulties that courts like *Netcom* and *Frena* had encountered in applying theories of direct and secondary liability to online infringement, opted for *Netcom*'s approach, and widened its reach to encompass those that not only store material but also cache it and help users locate it. The result was a set of three safe harbors that broadly protected service providers from liability—but only if those providers registered an agent for receipt of notices and responded to compliant notices by taking down access to the infringing material.

ii. The "Transmission" Safe Harbor

The remaining safe harbor stands alone. Found in § 512(a), it addresses liability for online service providers who engage in Transitory Communications—i.e., those who simply act as conduits for the infringing transmissions of others.[71] Suppose that Netcom had not stored the infringing Scientology material itself, but had merely transmitted it from Erlich's computer to some distant destination elsewhere in the Internet, through a process that Erlich initiated and that created no lasting copy on Netcom's servers. Section 512(a) severely limits the liability for such conduct; indeed,

67. *Id.* § 512(a)–(b).

68. *Id.* § 512(b)(2)(E).

69. *Id.* § 512(d) (referencing "information location tools, including a directory, index, reference, pointer, or hypertext link" that "refer[] or link[] users to an online location containing infringing material or infringing activity").

70. *Id.* § 512(d)(1)–(3).

71. Although it does not appear in the statute itself, the term "conduit" is a common shorthand for the kind of conduct § 512(a) addresses. *See, e.g.*, S. REP. NO. 105-190, at 41 (1998); *see also* Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1041 (9th Cir. 2013); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 39 (2d Cir. 2012); *In re* Charter Commc'ns, Inc., 393 F.3d 771, 775 (8th Cir. 2005).

to gain the safe harbor's protection, all a service provider must do is demonstrate that it is indeed simply a conduit.[72]

The Transitory Communications safe harbor therefore addresses a fact pattern that was not at issue in *Netcom* or *Frena*, both of which involved a provider that went beyond mere transmission and instead hosted lasting copies of infringing material. Yet this safe harbor, like the others, is consistent with the principles of *Netcom*. Consider direct liability: *Netcom* held that lack of volition would relieve the owner of a computer system from direct liability when the "system . . . automatically and uniformly creates temporary copies of all data sent through it" a perfect description of Transitory Communications.[73] Nor would vicarious liability be a concern, as a conduit's fees for its transmissions would have no relation to the transmission's content.[74] As for contributory liability, under *Netcom* a conduit would never simultaneously have both the requisite knowledge and the ongoing participation; unless it somehow learned about the transmission of infringing material ahead of time, knowledge of any infringement would come after its substantial participation (i.e., the transmission) had ended.[75] This is why Transitory Communications is the only one of the four safe harbors that imposes no notice-and-takedown and agent registration obligation on the service provider. When the provider is simply a conduit, its involvement with the material is so fleeting that a notice from a copyright owner could not realistically reach an agent in time to make a difference.

Congress's adoption of *Netcom* principles in § 512(a), however, should not obscure the fact that Transitory Communications is different in kind from the other safe harbors. That difference is rooted in the fact that the other three safe harbors all involve access to lasting copies of infringing materials, through hosting, caching, or locating. In contrast, a provider that qualifies for the Transitory Communications safe harbor has at most a momentary connection to infringement. Indeed, whether or not the courts required volition, a true conduit would not be liable for reproducing a transmitted work, because the transmission would remain in the conduit's servers for only a few seconds (if not less), such that it would be too transient to qualify as an

---

72. The statute sets forth the conditions that provider must satisfy to establish its conduit bonafides—i.e., that it is indifferent to and uninvolved in the content of the transmission. *See* 17 U.S.C. § 512(a)(1)–(5).

73. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1369 (N.D. Cal. 1995).

74. *See id.* at 1376 (finding "no direct financial benefit" and thus "no vicarious liability" "where a defendant rents space or services on a fixed rental fee that does not depend on the nature of the activity of the lessee").

75. Contrast this with the *ongoing* participation that was the basis of the contributory liability holding in *Netcom*. *See id.* at 1375 ("[I]t is fair . . . to hold Netcom liable for contributory infringement where Netcom has knowledge of Erlich's infringing postings yet continues to aid in the accomplishment of Erlich's purpose of publicly distributing the postings.").

infringing copy under the copyright statute.[76] Even the authors of the Green Paper and White Paper, with their expansionist bent, had to admit that such ephemeral "copies" were not really copies at all.[77]

Black-letter copyright law was not the only thing distinguishing conduits from other service providers. The same distinction was present in other fields. Defamation provides the best example. Even before the digital age, the law of defamation had its own struggles regarding the liability of intermediaries that had more than a momentary involvement in the publication of defamatory material.[78] Those struggles continued when defamation moved online, with courts splitting on whether the liability of a provider that *hosted* defamatory material depended on its knowledge of the material.[79] But in no context,

---

76. *See* 17 U.S.C. § 101 (requiring "copies" to be "fixed"—i.e., an "embodiment . . . sufficiently permanent or stable to permit it to be . . . communicated for a period of more than transitory duration"); Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 130 (2d Cir. 2008) (holding that transmission stored in computer system's active memory for 1.2 seconds was not fixed and that system operator therefore did not violate copyright owner's right to reproduce). In contrast, the case most often cited for the proposition that storage in active memory can qualify as an infringing copy, *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518–19 (9th Cir. 1993), involved RAM storage that lasted long enough for humans to interact with the content—i.e., far longer than would be the case in a transmission.

77. *See* GREEN PAPER, *supra* note 48, at 37 (asserting that "a copy is made" "[w]hen a work is placed" in computer memory "for more than a very brief period"); WHITE PAPER, *supra* note 47, at 65 (same). At the international level, the Clinton Administration did briefly push for standards that arguably put conduits in jeopardy, but they eventually fell by the wayside. *See* Samuelson, *supra* note 56, at 383–85, 390, 397 (discussing Article 7 of proposed WIPO treaty, the demise of Article 7, and changes to proposed communication right that put conduits out of jeopardy).

78. *Compare* Auvil v. CBS "60 Minutes," 800 F. Supp. 928, 931–32 (E.D. Wash. 1992) (holding that television network affiliate which declined to exercise editorial control over a network broadcast was not liable for republishing defamatory statements), *with* RESTATEMENT (SECOND) OF TORTS § 581(2) (AM. LAW INST. 1977) ("One who broadcasts defamatory matter by means of radio or television is subject to the same liability as an original publisher."). Note that defamation law sometimes uses the term "conduit" to refer to any intermediary who does not control the content—even if it stores the content rather than merely transmitting it. *See, e.g.*, WHITE PAPER, *supra* note 47, at 115 n.371; Susan Freiwald, *Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation*, 14 HARV. J.L. & TECH. 569, 589 n.83 (2001) (noting inconsistent use of term); Lucy H. Holmes, Note, *Making Waves in Statutory Safe Harbors: Reevaluating Internet Service Providers' Liability for Third-Party Content and Copyright Infringement*, 7 ROGER WILLIAMS U. L. REV. 215, 219–20 (2001) (referring to CompuServe as a "conduit" in a case—*Cubby, Inc. v. CompuServe Inc.*—in which it hosted "allegedly defamatory" posts on its message board (citing Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135, 138 (S.D.N.Y. 1991))). To remain consistent with our use of the term in the DMCA context, however, we will use it here only to refer to intermediaries who merely transmit content—storing it, if at all, only so long as needed to effect the transmission.

79. The two cases most often cited for this issue are *Cubby*, 776 F. Supp. at 140–41 (holding online service provider not liable for allegedly libelous third-party content it unknowingly made available to subscribers), and *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 1995 WL 323710, at *4–5 (N.Y. Sup. Ct. May 24, 1995) (holding online service provider strictly liable under similar circumstances due to its policy of monitoring third-party content). Section 230 of the Communications Decency Act later rendered the issue academic. *See* Zeran v. Am. Online, Inc., 129 F.3d 327, 332–33 (4th Cir. 1997).

online or off, did any court hold a conduit liable for its fleeting transmission of defamatory content.[80] When a slander occurred over the phone, no one credibly claimed that the telephone company was liable.[81] Nor had a post office or private delivery service ever been held liable for the libelous contents of the material they delivered, although their role in transmitting material was much less fleeting than an online conduit's.[82] When it came to online defamation, then, even those who favored expanding service provider liability accordingly acknowledged that mere conduits should be excepted.[83]

Similarly, in privacy law, Congress had already recognized the important technological distinction between transmitting digital information and hosting it. The Electronic Communications Privacy Act ("ECPA")[84] set forth very different approaches to privacy protection depending on whether the communication at issue was intercepted mid-transmission or was accessed from digital storage.[85] Likewise, the statute prohibiting the transmission of child pornography imposed liability on intermediaries only when they had the practical ability to examine the transmission's content.[86]

The extent to which these parallel legal regimes provided an explicit model for the Transitory Communications safe harbor is unclear. The Green Paper and White Paper briefly discussed defamation standards, but not with

---

80. The one online case in which this issue was raised ended in a win for the service provider. *See* Lunney v. Prodigy Servs. Co., 723 N.E.2d 539, 542 (N.Y. 1999) (finding no liability for transmitting defamatory email because "[defendant's] role in transmitting e-mail is akin to that of a telephone company").

81. *See* RESTATEMENT (SECOND) OF TORTS § 581 cmt. b (AM. LAW INST. 1977) (confirming no defamation liability for "one who merely makes available to another equipment or facilities that he may use himself for general communication purposes," including "a telephone company"); *id.* at § 612 cmt. g ("Since it is the user of a telephone rather than the telephone company who is treated as transmitting a telephone message . . . the company is not subject to liability for a defamatory statement communicated by a customer." (citation omitted)). The closest case we could find was *Anderson v. N.Y. Tel. Co.*, 320 N.E.2d 647, 647 (N.Y. 1974), in which the telephone company was held not liable for allegedly defamatory messages that could be heard by dialing certain telephone numbers. The company arguably hosted the messages, in that it was the lessor of the equipment on which they were stored, yet it still escaped liability. *Id.* at 649 (Gabrielli, J., concurring).

82. At least, we could find no case in which such an allegation was even made, let alone succeeded.

83. *See, e.g.*, Freiwald, *supra* note 78, at 585 (arguing against defamation immunity for online intermediaries but acknowledging that "entities that merely pass information from computer to computer on the Internet without a meaningful opportunity to check or change the data should not be considered intermediaries, even though they are technically situated in the middle of the transmission process").

84. Electronic Communications Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

85. *See* David J. Loundy, *E-Law: Legal Issues Affecting Computer Information Systems and Systems Operator Liability*, 3 ALB. L.J. SCI. & TECH. 79, 113–17 (1993) (contrasting section 2511 and section 2701 of EPCA).

86. *See* Noah Levine, Note, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526, 1557 (1996).

regard to conduits,[87] and the DMCA legislative history makes no mention of defamation at all.[88] The ECPA merited a brief mention in the legislative history, but again not in the context of the host-conduit distinction.[89] But reasoning by analogy definitely played a part in copyright law's unique treatment of conduits. The White Paper itself made the telephone comparison, noting that "[i]f an entity provided only the wires and conduits —such as the telephone company, it would have a good argument for an exemption . . . ."[90] The *Netcom* case quoted this language and analogized conduit liability to "holding the owner of the highway, or at least the operator of a toll booth, liable for the criminal activities that occur on its roads."[91] Those who successfully opposed to the Clinton Administration's efforts to expand liability cited the post office analogy.[92] And the references to "common carriers" were everywhere—an acknowledgement that communication works best when those transmitting communications do not pick and choose who gets to communicate and what they get to say.[93]

In short, liability for the online *hosting* of material—infringing material, defamatory material, pornographic material, etc.—was hotly contested and very much in flux when the DMCA was taking shape. But there was no flux when it came to conduits. No court had so much as suggested that those providing temporary data connections should have to monitor their transmissions for defamatory material or illegal pornography. Why then would they have to be on the lookout for copyright infringement? Given this history, it is entirely unsurprising that the Transitory Communications safe harbor protected conduits *qua* conduits, with none of the complicated

87. *See* GREEN PAPER, *supra* note 48, at 77–78; WHITE PAPER, *supra* note 47, at 115 n.371.

88. *See* S. REP. NO. 105-190 (1998); H.R. REP. NO. 105-551, pt. 1 (1998); H.R. REP. NO. 105-551, pt. 2 (1998); H.R. REP. NO. 105-796 (1998).

89. *See* S. REP. NO. 105-190, at 55; H.R. REP. NO. 105-551, pt. 2, at 64–65.

90. WHITE PAPER, *supra* note 47, at 122. Nor did any of White Paper's legislative proposals, expansive though they were, purport to assign liability to service providers acting as mere conduits. *See id.* at 211–36; *cf.* Samuelson, *supra* note 56, at 385, 397 (noting that telephone companies were among those concerned about attempts—ultimately unsuccessful—to adopt international standards that might have exposed conduits to liability).

91. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., 907 F. Supp. 1361, 1369 n.12 (N.D. Cal. 1995).

92. *See* Ad Hoc Alliance for a Digital Future, Suggested Revisions to the Chairman's Basic Proposal for the Treaty Formerly Known as the Berne Protocol 3 (Oct. 31, 1996) ("Just like the postal service cannot (and indeed should not) monitor the contents of all the envelopes it handles, it is simply not possible for an infrastructure provider to monitor whether the millions of electronic messages it transmits daily have been authorized."), *cited in* Samuelson, *supra* note 56, at 386 (discussing successful efforts to remove from international negotiations certain provisions that might have implicated conduits).

93. *See, e.g.*, *Netcom*, 907 F. Supp. at 1369 n.12; WHITE PAPER, *supra* note 47, at 122; Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345, 377 (1995); Freiwald, *supra* note 78, at 589; David J. Loundy, *E-LAW 4: Computer Information Systems Law and System Operator Liability*, 21 SEATTLE U. L. REV. 1075, 1090–92 (1998).

knowledge elements, agent registration, or notice-and-takedown obligations that one sees in the other safe harbors.

iii. The Best-Practice Thresholds

The final part of the DMCA's structure involves two threshold requirements, so-called because a service provider must satisfy them in order to take advantage of any of the safe harbors.[94] The first requires the service provider to accommodate "standard technical measures,"[95] which refer to industry-wide technological standards designed to protect copyrighted works.[96] The second requires the service provider to adopt and reasonably implement a policy under which it terminates the accounts of any users who repeatedly infringe copyright.[97]

Unlike the safe harbors, these threshold requirements are not related to the data-processing functions of computer networks. Instead, they represent Congress's desire to create a set of best practices for those who provide online services, and to encourage compliance therewith. If an industry were to create robust technological standards through which computers could automatically identify copyrighted works, check to see if their use was licensed, and so forth, Congress wanted to incentivize service providers to get on board. And if a provider had reliable evidence that one of its users was repeatedly infringing copyright, Congress wanted that user to know that loss of Internet access was a real possibility.[98]

---

94. There are arguably two other statutory provisions that might be viewed as threshold requirements, in addition to those discussed in the main text—but which do not apply equally to all four safe harbors. First, in order to take advantage of any safe harbor, a service provider must meet the definition of "service provider" in § 512(k). Fortunately, the definition is very broad ("a provider of online services or network access, or the operator of facilities therefor") except when the Transitory Communications safe harbor is at issue, when the definition is slightly narrower, albeit not particularly constraining. *See* 17 U.S.C. § 512(k)(1) (2012). Second, as already mentioned, in order to use the three "access" safe harbors a service provider must register an agent with the U.S Copyright Office for receipt of notices from copyright owners. We are making the assumption here—justified, we think—that the reference to the System Storage notice-and-takedown process in the System Caching and Information Location safe harbors means that agent registration is required for the latter, as it is in the former. *See id.* § 512(c)(2) (including agent registration as part of System Storage notice-and-takedown process); *id.* § 512(b)(2)(E) (incorporating that process by reference); *id.* § 512(d)(3) (same). But because agent registration is completely irrelevant to the Transitory Communications safe harbor, it is not properly classified as a threshold requirement for the DMCA generally.

95. *Id.* § 512(i)(1)(B).

96. *Id.* § 512(i)(2).

97. *Id.* § 512(i)(1)(A). Service providers must also ensure that their users are aware of the repeat-infringer policy. *Id.*

98. *See* S. REP. NO. 105-190, at 52 (1998) (recognizing both that a provider should not have to "make difficult judgments as to whether conduct is or is not infringing" and that "those who repeatedly or flagrantly abuse their access to the Internet through disrespect for the intellectual property rights of others should know that there is a realistic threat of losing that access"). The House Report had almost identical language. *See* H.R. REP. NO. 105-551, pt. 2, at 61 (1998).

In both instances, however, the DMCA stopped short of making it illegal not to comply with these two requirements. Ignoring standard technical measures or doing nothing about repeat infringers would not itself lead to a service provider's being liable for infringement. Instead, the provider would simply not be able to claim the protection of the safe harbors. In other words, the threshold requirements simply incentivized a healthy and helpful attitude toward copyright law without imposing significant consequences for noncompliance. Thus, the term "best practices."

The two threshold requirements have played divergent roles since the Act's passage. Standard technical measures have been largely irrelevant; no court has ever recognized the existence of such a measure in the 20 years since the DMCA was enacted.[99] As we will see in Part IV, however, the repeat-infringer provision has proved to be more consequential.

* * *

So there we have it: four carefully delineated categories of conduct in which online service providers could engage without fear of liability, plus two threshold requirements.[100] Three of the four safe harbors deal with ongoing access to third-party content, so they also provide for takedown of such content upon notice. The fourth does not. Overall, this structure protects the kinds of automatic, indiscriminate data processing in which computer networks commonly engage, and which is necessary for the operation of any digital platform that handles content that originates with others.

3. The DMCA's Lacunae

With the passage of the DMCA, Congress had told the country what sorts of online activity would not constitute infringement. But because the statute merely established safe harbors, courts retained the power to define liability whenever the safe harbors didn't apply. Indeed, the statute itself explicitly

---

99. *See, e.g.*, BWP Media USA Inc. v. Polyvore, Inc., 922 F.3d 42, 55–57 (2d Cir. 2019) (Walker, J., concurring) (rejecting claim that image metadata qualifies); Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1115 (9th Cir. 2007) (considering but ultimately remanding issue); Obodai v. Demand Media, Inc., No. 11 Civ. 2503(PKC), 2012 WL 2189740, at *5 (S.D.N.Y. June 13, 2012) (rejecting claim that website that "distributed copyrighted texts and entered into some form of a distribution agreement" failed to accommodate standard technical measure), *aff'd sub nom.* Obodai v. Cracked Entm't Inc., 522 F. App'x 41 (2d Cir. 2013). One court found a triable issue as to whether image metadata constituted a standard technical measure. *See* Gardner v. CafePress Inc., No. 3:13-cv-1108-GPC-JMA, 2014 WL 794216, at *5–6 (S.D. Cal. Feb. 26, 2014). Another seemed to accept *arguendo* the existence of a standard technical measure, only to find that the service provider had indeed accommodated it. *See* Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724, 745 (S.D.N.Y. 2012). But no court has actually held that a standard technical measure exists.

100. At least, without fear of the kind of liability that would have attached under a *Frena* standard. As we will soon see, even when a safe harbor applies, a service provider can be subject to a limited injunction under § 512(j).

recognized as much in § 512(l), which noted that a failure to qualify for a safe harbor "shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense."[101] In other words, being outside a safe harbor's protection didn't necessarily mean a service provider was liable; it simply threw the issue back to the courts, which were still free to fashion copyright standards that favored service providers (as *Netcom* had done) or copyright owners (as *Frena* had done).[102]

At first glance, this might appear to be a purely academic point. After all, the four safe harbors covered the most important issues in online copyright, seemingly leaving little common law for the courts to decide.[103] A service provider that merely transmitted data no longer had to worry about whether a court would consider such conduct infringing; even if the data contained copyrighted material, the provider had the Transitory Communications safe harbor in § 512(a) to protect it. A service provider sued for hosting user-generated material no longer had to worry about whether the court would follow *Netcom* or *Frena*; the System Storage safe harbor in § 512(c) clearly sided with the former. And so forth.

All that would be true, were it not for two other features of the DMCA. The first is that even when the safe harbors apply, they do not give service providers total immunity. Instead, they each allow for the possibility of certain forms of injunctive relief under § 512(j), essentially aimed at shutting down access to specific online material or denying access to specific infringing users.[104] The clear implication is that even after passage of the Act, courts remained free to adopt standards of infringement more unfavorable to service providers than the DMCA was; otherwise, the injunction provision would be

101. 17 U.S.C. § 512(l).

102. As the congressional conference report put it, the DMCA "is not intended to imply that a service provider is or is not liable as an infringer either for conduct that qualifies for a limitation of liability or for conduct that fails to so qualify." H.R. REP. NO. 105-796, at 73 (1998).

103. We use the term "common law" with some hesitation, both because it is a loaded term when used in reference to federal law, see *Erie R.R. Co. v. Tompkins*, 304 U.S. 64, 78 (1938) ("There is no federal general common law."), and because "common-law copyright" sometimes refers to (mostly moribund) state copyright systems, see, e.g., Zvi S. Rosen, *Common-Law Copyright*, 85 U. CIN. L. REV. 1055, 1057 (2018). Nevertheless, it is the term that best describes the judicial lawmaking that takes place in federal copyright cases, which is the focus of Part II. The standards for secondary liability, for example, are completely judge-made. *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1373 (N.D. Cal. 1995) (noting that "there is no statutory rule of liability for infringement committed by others"). And even when a federal copyright statute governs, courts retain a lot of discretion in fashioning interpretive standards. *See, e.g.*, Amy B. Cohen, *Masking Copyright Decisionmaking: The Meaninglessness of Substantial Similarity*, 20 U.C. DAVIS L. REV. 719, 720 (1987) ("[N]either the statute nor its legislative history clearly defines the substantive showing a plaintiff must make to establish that a party has infringed the copyright."); James Gibson, *Risk Aversion and Rights Accretion in Intellectual Property Law*, 116 YALE L.J. 882, 888–91 (2007) (discussing the indeterminacy of various judge-made doctrines in copyright law). Such standards are essentially common law.

104. *See* 17 U.S.C. § 512(j).

mere surplusage. For example, in a jurisdiction that followed *Frena*, a service provider could qualify for the System Storage safe harbor yet still be subject to a limited injunction.[105]

The other feature that complicates the DMCA's application is the two threshold requirements. We have seen that these requirements do not impose any affirmative legal obligation on service providers, because failure to comply with them does not lead to liability. But the threshold requirements do matter, because the DMCA's limited liability is available only to those service providers that *both* engage in the kinds of conduct covered by the safe harbors *and* also jump through the regulatory hoops that the threshold requirements represent. That leaves open the possibility that a provider could, for example, unknowingly host infringing content and yet not be within the protection of the System Storage safe harbor—because it neglected to establish a repeat-infringer policy. In such cases, the DMCA would be irrelevant, and the parties would be back in the case-law world, fighting over whether *Netcom* or *Frena* should govern.

In the end, then, the DMCA left significant gaps for the federal judiciary to fill, one case at a time. If a court preferred *Frena* to *Netcom*, it could impose the former's more demanding standards on any service provider that neglected to satisfy one of the DMCA's threshold requirements. Even when those requirements were satisfied, qualifying for a safe harbor still left service providers exposed to certain injunctive relief, under whatever liability standards the judge deigned to apply. And when it came to conduct that did not fall within any safe harbor, both liability and remedy were wholly in the hands of the courts. Despite the promise of national uniformity, the DMCA simply had nothing to say in any of these contexts—except, in essence, "good luck with all that."

III. CONVERGENCE

We have now seen that, in theory, the DMCA had no say in the continuing development of the common-law standards for online infringement. The safe harbors were just statutory defenses to a claim of copyright infringement leveled against a service provider. The common-law liability standards, both direct and secondary, could continue to develop on their own without regard for the DMCA. Indeed, such development was, if not expressly set forth, at least implicitly assumed within the DMCA's structure.

The reality, however, is that the statutory safe harbors exerted a gravitational pull on the common law. Before the DMCA, the common-law

105. In contrast, a court that followed *Netcom* would see qualifying for the System Storage safe harbor as proof that there was no basis for common-law liability, since Congress essentially borrowed *Netcom*'s holding in creating that safe harbor.

infringement standards diverged wildly.[106] After the DMCA, these varying holdings steadily converged toward a more uniform national standard, whose borders look increasingly like the borders of the safe harbors themselves. This convergence took place even when the threshold conditions were not met —i.e., even when the safe harbors played no role at all in the case. And when the safe harbors did play a role, courts have essentially used them to define the extent of liability, thereby ignoring the statute's invitation to order injunctive relief under § 512(j).[107] Put simply, no court has taken the opportunity to develop the common law independently of the contours of the safe harbors. Instead, the DMCA safe harbors and common-law standards, after 20 years, are almost identical.

The following discussion summarizes this process of convergence. We begin by setting forth a framing structure that categorizes the possible paths the common law could have taken after the DMCA was enacted, some of which are convergent and some of which are divergent. We then discuss the circumstances that made each outcome a real possibility, rather than merely a professor's thought experiment; convergence may look inevitable in retrospect, but it was anything but. Finally, we show that despite those circumstances, and despite the two divergent possibilities, the actual case law has moved in a consistently convergent direction, heavily influenced by the statutory standards even when the statute was not at issue. This will set the stage for Part IV, in which we will see that although convergence might appear benign, it has a dark side that is both unexpected and unwelcome.

A. THEORETICAL PATHS OF CON/DIVERGENCE

As discussed above, the DMCA theoretically left open the possibility that common-law standards could develop in any number of directions, some of which would converge with the statutory safe harbor standards, others of which would diverge.[108] To better understand these possibilities, consider the following matrix.

106. *Compare Netcom*, 907 F. Supp. at 1380 (declining to hold service provider directly liable for user activity), *with* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993) (holding service provider directly liable for user activity).

107. 17 U.S.C. § 512(j).

108. *See, e.g.*, *id.* § 512(l) ("OTHER DEFENSES NOT AFFECTED.—The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.").

Table 1. Con/Divergence Scenarios

		DMCA SAFE HARBOR STANDARDS: Δ's conduct falls within safe harbor	DMCA SAFE HARBOR STANDARDS: Δ's conduct falls outside safe harbor
COMMON-LAW LIABILITY STANDARDS	Δ not liable	A Convergence	C Divergence
	Δ liable	B Divergence	D Convergence

As Table 1 illustrates, the common law and the DMCA safe harbors can interact in four different ways. Start with Box A, in the upper left. As the column heading indicates, defendants who fall within this box are engaging in conduct that falls within one of the DMCA safe harbors. For example, suppose a service provider (let's call it Comnet) hosts Usenet content, is told by RTC of a user's infringing posts, and takes them down immediately in response. Comnet's conduct would thereby fall within the System Storage safe harbor in § 512(c). Now consider the row heading for Box A: It indicates that the defendant is not liable under the applicable case law. That would be the case if Comnet were judged by the *Netcom* court's standard, since that court held that it was only the service provider's failure to take down the content upon notice that exposed it to liability.[109] Thus we have convergence of the two sets of standards: The same conduct that qualifies the service provider for the safe harbor rescues it from liability.

It does not have to be so. Turn to Box B in the matrix and consider the same facts: Comnet takes down the infringing content upon notice. We know that that means the System Storage safe harbor is available. Now, however, we are in a jurisdiction that follows *Frena*. As the row heading indicates, Comnet would still be liable, because *Frena* predicated liability on the mere hosting of the content, whether knowing or not.[110] So here we would have a divergence of standards, in that conduct that falls within a safe harbor is nonetheless a basis for liability. Of course, if the safe harbor applied in such a case, the only available remedy would be a limited injunction under § 512(j); that's the point of the safe harbor.[111] Indeed, it is the very existence of § 512(j) that proves that this sort of divergence is possible—that the DMCA contemplates such an outcome.

109. *Netcom*, 907 F. Supp. at 1375.
110. *Frena*, 839 F. Supp. at 1559.
111. 17 U.S.C. § 512(j).

Move now to Box C. Here the column heading indicates that no safe harbor applies. So change the facts of the hypothetical: This time, Comnet does not take down the infringing material, even after it receives sufficient notice. Its conduct therefore falls outside the System Storage safe harbor. Yet that does not necessarily mean that it is liable for infringement. As we have already seen, § 512(l) explicitly states that failure to qualify for a safe harbor "shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title . . . ."[112] To be sure, even the *Netcom* ruling implies that liability would follow.[113] But just as courts remain free to depart from *Netcom* by being more demanding of service providers, as *Frena* did, they also remain free to go the opposite way and apply more relaxed standards. For example, a court might decide that a service provider like Comnet is a mere utility, like the electric company, too far removed from the direct infringement to be liable even when it knows what its customer is doing.[114] A court that went in this direction would be diverging from the safe harbor standards.

Finally, Box D. Again, as the column heading indicates, Comnet's failure to take down the infringing material disqualifies it from the safe harbor's protection. But now the court decides that the same failure is grounds for imposing liability, as the *Netcom* court seemed to contemplate. As with Box A, we have convergence, but in the inverse: The same conduct that puts the provider outside of the safe harbor also renders it liable.

In the end, then, the DMCA left open a variety of possibilities, and courts could develop common-law liability standards as they saw fit. To the extent those standards mirrored the safe harbors, the cases would all end up in Box A or D of the matrix, and we would see convergence. To the extent that they developed more or less demanding common-law standards, we would see cases that belong in Boxes B and C—evidence of divergence. When we begin our exploration of the post-DMCA case law, we will apply this framing device to the holdings.[115]

B. PRACTICAL OPPORTUNITIES FOR COMMON-LAW DEVELOPMENT

Not only did the DMCA theoretically allow for either convergence or divergence, but it also created real opportunities for courts to choose either path. These opportunities were a function of two features of the DMCA.

One feature is the threshold requirements. As explained above, the DMCA denies its protection to service providers who do not reasonably implement a repeat-infringer policy or accommodate standard technical

112. *Id.* § 512(l).

113. *See Netcom*, 907 F. Supp. at 1380.

114. *See* Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 800–01 (9th Cir. 2007) (implying that a company providing electricity to an infringer would not be contributorily liable even if done knowingly).

115. Spoiler alert: They converge.

measures, even if the provider is engaging the very kind of automatic, indiscriminate data processing that the DMCA was designed to protect.[116] Unlike the safe harbors, however, the threshold requirements are not related to any recognized basis for liability; they are simply a regulatory price that providers must pay to receive the Act's benefits. Indeed, when we say that a defendant's conduct falls within one of the DMCA safe harbors—and this is an important point for understanding where cases fall in our matrix—we are not saying that the DMCA actually applies. It's entirely possible for a service provider's conduct to fall within a safe harbor, only to see the DMCA rendered inapplicable because the provider failed to satisfy one or both of the threshold requirements.

What the threshold requirements do, however, is create real potential for development of the common law of infringement. After all, if the DMCA applies, the court might decline to articulate liability standards at all, because the statute mostly settles the question, leaving only the possibility of a § 512(j) injunction (which the copyright owner might not pursue). But when a threshold requirement goes unmet, the court has to deal with the question of common-law liability, even as to defendants whose conduct would otherwise fall within a safe harbor. The potential for lawmaking in the shadow of the DMCA is real.[117]

The other feature of the DMCA that lends itself to common-law development is that the safe harbors are an affirmative defense to a claim of copyright infringement.[118] As a matter of civil procedure, then, even when the DMCA safe harbors are in play, courts should decide infringement first.[119] If the copyright owner cannot carry its burden of proving infringement, then there is no need for a defense. This procedure is sometimes honored in the breach,[120] but we will soon see that there are a number of cases in which courts did indeed determine and apply the common-law standards for infringement, moving to the DMCA only if such infringement was proved. For example, in *A&M Records v. Napster*, an early post-DMCA case, the Ninth Circuit first did a liability analysis and only then turned to the DMCA—resisting both the

116. *See supra* Section II.B.2.iii.

117. As is the potential for private ordering in the shadow of the DMCA. *See generally* Sag, *supra* note 3 (discussing ways in which private agreements and automated systems now mediate relationship between copyright owners and online platforms).

118. *See* Lee, *supra* note 4, at 244 ("The DMCA safe harbors are affirmative defenses that the defendant must prove . . . .").

119. *See* Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1039 (9th Cir. 2013) (considering defendant's assertion of safe harbors only after concluding "that [plaintiff] ha[d] carried its burden of proving" defendant's *prima facie* liability); 4 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.04[A][1][e] (2019) (Matthew Bender, ed.) ("Once [plaintiff] establishes its *prima facie* case . . . the burden shifts to defendant to establish the affirmative defense of a Section 512 safe harbor.").

120. *See* Lee, *supra* note 4, at 244 ("[O]ften, the defense is invoked on summary judgment without any determination of liability because the safe harbor can more easily dispose of the case.").

temptation to reverse the order and the plaintiffs' invitation to view the inquiries as one and the same.[121]

Together, the threshold requirements and procedural posture of the safe harbors mean that there are many cases in which courts have not only the theoretical authority to develop their own liability standards, but also the practical opportunity to do so. We therefore turn to an examination of such cases, in which courts have taken the chance to articulate common-law infringement standards in the shadow of the DMCA.

C. CONVERGENCE IN THE CASE LAW

We divide the case law into two categories: cases in which courts found no liability for copyright infringement and cases in which they did find such liability. Each category contains cases in which the court had an opportunity to opine on the common-law standards for liability, separate and apart from any statutory safe harbor standards. To establish convergence, we will examine the cases in the first category to see if the defendants' conduct also fell within a safe harbor, and we will examine the cases in the second category to see if it did not.

1. Findings of No Liability

The first possible scenario starts with a finding of no copyright infringement, with convergence resulting if this finding also means the defendant falls within a DMCA safe harbor. In other words, this scenario corresponds to Box A in our matrix.

i. Direct Infringement Convergence

Convergence is most striking in decisions finding no direct copyright infringement. As noted above, prior to the DMCA there were two approaches to direct infringement, particularly for service providers. The district court in *Frena* found that automated copying that took place via a service provider's system constituted direct copyright infringement by the provider, noting that "[i]t does not matter that Defendant Frena may have been unaware of the copyright infringement."[122] The *Netcom* district court came to the opposite conclusion, concluding that the lack of volition meant that automated copying occurring as a result of standard network operations cannot form the basis for direct infringement liability.[123] After the DMCA essentially adopted the *Netcom* approach, courts have consistently cited the DMCA and *Netcom*, ignored *Frena*, and moved toward a uniform standard of non-infringement for

121. *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025, 1029 (9th Cir. 2001).

122. Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993).

123. Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1372–73 (N.D. Cal. 1995).

such automated copying.[124] And this is even the case when the threshold requirements for the DMCA safe harbors are not met.

This convergence first presents itself in the Fourth Circuit's decision in *ALS Scan, Inc. v. RemarQ Communities, Inc.*[125] As with many early service provider cases, *ALS Scan* involves Usenet and the unauthorized hosting of copyrighted material—here, ALS's photographs of adult models—by a service provider, RemarQ.[126] RemarQ did not choose the photos at issue, and all of RemarQ's copying was an automatic, inherent function of hosting Usenet newsgroups.[127] In analyzing whether this copying rendered RemarQ directly liable, the court found that the liability analysis and the DMCA safe harbor analysis were one and the same.[128] It explained that the DMCA "provides certainty that *Netcom* and its progeny, so far only a few district court cases, will be the law of the land."[129] Accordingly, direct infringement claims are controlled by the DMCA.[130] In other words, the Fourth Circuit determined that Congress, by creating the safe harbors, pushed the common law in a particular direction, such that passive, automatic copying cannot establish direct copyright infringement.[131] Even Westlaw appears to have accepted this view, using the analysis in *ALS Scan* to conclude that *Frena* is "Superseded by Statute"—that statute being the DMCA.[132]

The Fourth Circuit went on to completely import the DMCA safe harbors into the direct infringement liability standard in *CoStar Group v. LoopNet*.[133] Like *ALS Scan*, the *CoStar* case presented the typical System Storage scenario, with service provider LoopNet operating a server onto which its users copied CoStar's copyrighted photographs without a license.[134] The twist here was that LoopNet had not met the threshold conditions for the DMCA safe harbor (having failed to implement a repeat-infringer policy), which made this a case purely about the ultimate liability standards.[135]

---

124. R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability*, 32 COLUM. J.L. & ARTS 427, 437–38 (2008).

125. ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 620 (4th Cir. 2001).

126. *Id.* at 620–21.

127. *Id.* at 620–22.

128. *Id.* at 622–24.

129. *Id.* at 622 (citing H.R. REP. NO. 105-551, pt. 1, at 11 (1998)).

130. *See id.*

131. *Id.* at 622 ("Although we find the *Netcom* court reasoning more persuasive, the ultimate conclusion on this point is controlled by Congress' codification of the *Netcom* principles in Title II of the DMCA.").

132. *See generally* Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552 (M.D. Fla. 1993) (using yellow-flag KeyCite to alert reader to the superseding statute).

133. CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004).

134. *Id.* at 546–47.

135. *Id.* at 548 (relating CoStar's argument that "[b]ecause Loop–Net [*sic*] could not meet the conditions for immunity under the DMCA as to many of the copyrighted photographs, LoopNet accordingly would be liable under CoStar's terms for direct copyright infringement for hosting web pages containing the infringing photos"); CoStar Grp. Inc. v. LoopNet, Inc., 164 F.

Because the DMCA was unavailable to LoopNet, CoStar argued that *Netcom* should also be unavailable. In other words, it asserted that the statute "supplanted and preempted *Netcom*," making the safe harbors the sole determinant of liability and thus finding infringement whenever they did not apply.[136] The Fourth Circuit rejected this claim, embraced *Netcom* as the governing standard, and "h[e]ld that the automatic copying, storage, and transmission of copyrighted materials, when instigated by others, does not render [a service provider] strictly liable for copyright infringement . . . ."[137] The substance of the safe harbors and the direct infringement liability standard were therefore viewed as identical, even when the DMCA defenses were technically unavailable.[138] As Tony Reese observed, under *CoStar* service providers "do not need a safe harbor's protection in order to avoid direct infringement liability."[139] This is textbook convergence.[140]

This "Box A" convergence—finding no direct liability in the exact situations where the DMCA safe harbors would apply—has also occurred outside the Fourth Circuit. For example, the Fifth Circuit, in *BWP Media v. T&S Software*, considered an online forum where users had posted copyrighted photographs without authorization.[141] The defendant's conduct would have fallen within the System Storage safe harbor, except it had failed to designate an agent for receipt of takedown notices, making the statutory defense unavailable.[142] The court nevertheless came to a similar conclusion as *CoStar*, resolving the question of direct infringement by invoking the same *Netcom* reasoning that the DMCA had codified: "[E]very circuit to address this issue

---

Supp. 2d 688, 703–04, 717 (D. Md. 2001) (denying summary judgment based on adequacy of repeat-infringer policy), *aff'd*, 373 F.3d 544, 546 (4th Cir. 2004).

136. *CoStar*, 373 F.3d at 552–53.

137. *Id.* at 555. As the *CoStar* court explained, "[e]ven though the DMCA was designed to provide ISPs with a safe harbor from copyright liability, nothing in the language of § 512 indicates that the limitation on liability described therein is exclusive. Indeed, another section of the DMCA provides explicitly that the DMCA is *not* exclusive." *Id.* at 552 (citing 17 U.S.C. § 512(l) (2000)). For our explanation of § 512(l), *see supra* notes 101–02 and accompanying text.

138. *CoStar*, 373 F.3d at 554.

139. Reese, *supra* note 124, at 430.

140. *CoStar*, 373 F.3d at 555. In contrast to *CoStar*, the Ninth Circuit in *Ellison v. Robertson* thought it was still an open question whether this DMCA-view of direct infringement still controls when the DMCA safe harbors are not available. Ellison v. Robertson, 357 F.3d 1072, 1077 (9th Cir. 2004). The court explained "that '[t]he DMCA did not simply rewrite copyright law for the on-line world.' Congress would have done so if it so desired." *Id.* (alteration in original) (citation omitted) (quoting Ellison v. Robertson, 189 F. Supp. 2d 1051, 1061 (C.D. Cal. 2002)). Accordingly, "[c]laims against service providers for direct, contributory, or vicarious copyright infringement, therefore, are generally evaluated just as they would be in the non-online world." *Id.* "Congress provided that [the DMCA's] 'limitations of liability apply if the provider is found to be liable *under existing principles of law*.'" *Id.* (quoting S. REP. NO. 105-190, at 19 (1998)). The court did not, however, find divergence between the liability and DMCA—instead it remanded the case back to the district court on the issue of liability. *Id.* at 1082.

141. BWP Media USA, Inc. v. T & S Software Assocs., 852 F.3d 436, 438 (5th Cir. 2017).

142. *Id.* at 443.

has adopted some version of *Netcom*'s reasoning and the volitional-conduct requirement" for determining direct liability.[143] The court also dismissed the argument that without protection from the DMCA, the service provider had to be liable.[144] The court concluded, like the Fourth Circuit in *CoStar*, that even though a service provider does not qualify for the safe harbors, the volitional-conduct requirement still applied.[145] The standard set forth in the DMCA again clearly informed the actual direct infringement analysis, despite the technical irrelevance of the safe harbors.

The Third Circuit has also adopted a common-law standard for direct infringement that mimics the System Storage safe harbor. In *Parker v. Google*, the court held that merely hosting copyrighted material does not constitute direct copyright infringement, citing both *Netcom* and *CoStar* to support this proposition.[146] To succeed on a direct infringement claim, the plaintiff must assert "volitional conduct on the part of the [provider]."[147] And courts within the Third Circuit have used this holding to render the DMCA analysis irrelevant. For example, one district court cited *Parker*, *Netcom*, and *CoStar* in yet another Usenet hosting case; in doing so, it applied DMCA-like standards even as it recognized that its finding of no liability meant that "it need not and does not address whether the DMCA applies."[148] By converging the direct infringement standard with the DMCA safe harbors, the analysis can simply stop at a finding of no liability—a finding increasingly identical to, and presumably informed by, the substance of the safe harbors.

ii. Secondary Infringement Convergence

A similar convergence takes place when looking at the development of secondary infringement after the passage of the DMCA. As with direct infringement, the cases have almost exclusively involved web-hosting scenarios, where contributory infringement is a common theory of liability. And the common-law knowledge standard for contributory infringement has

143. *Id.* at 440 (citing Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 666–67 (9th Cir. 2017); Leonard v. Stemtech Int'l Inc., 834 F.3d 376, 387 (3d Cir. 2016); Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 131 (2d Cir. 2008)).

144. *See id.* at 443. The defendant had "never designated an agent," and thus did not meet § 512(c)'s threshold requirements for immunity. *Id.*

145. *Id.* at 443–44. The copyright holder also argued that adopting the requirement would disincentivize DMCA compliance by benefitting those service providers that choose not to satisfy the threshold requirements. *Id.* at 443. While the court dismisses this argument, the plaintiff does identify a possible problem with convergence and keeping the DMCA: The redundancy makes such procedural hurdles irrelevant, and wasteful, given that the "protection" is the same under the common-law.

146. Parker v. Google, Inc., 242 F. App'x 833, 836–37 (3d Cir. 2007).

147. *Id.* at 836.

148. Parker v. Paypal, Inc., No. 16-4786, 2017 WL 3508759, at *5 n.7 (E.D. Pa. Aug. 16, 2017).

steadily moved toward the specific knowledge element found in the System Storage safe harbor.

Recall that contributory infringement requires both knowledge of and substantial participation in an act of direct infringement.[149] Prior to the DMCA, many courts interpreted the knowledge element to mean mere knowledge that the infringing activity was occurring, rather than knowledge that such activity actually constituted copyright infringement.[150] Nor was there always a specific knowledge requirement. That is, general knowledge that infringing activity was occurring somewhere on the defendant's network would satisfy this prong of contributory infringement.[151]

In contrast, the DMCA is more forgiving. It excludes a service provider from the Act's coverage only if the provider has acquired specific knowledge of infringement. The most direct articulation of this heightened knowledge standard is in § 512(c)(1)(A), which sets forth what level of knowledge will exclude the service provider from the System Storage safe harbor's protection.[152] A service provider falls outside that protection if it has "actual knowledge that the material or an activity using the material on the system or network is infringing" and if "upon obtaining such knowledge or awareness" it fails to "act[] expeditiously to remove, or disable access to, the material."[153] This level of knowledge explicitly requires knowing the specific material that allegedly infringes and that the direct infringer's activity constitutes copyright infringement.

We see a similarly high threshold for culpable knowledge in the notice-and-takedown regime that applies in three of the four safe harbors and that (if followed) protects a service provider from liability.[154] The regime requires the copyright owner to not only specifically inform the service provider of the direct infringer's activity, but also to aver that such activity constitutes copyright infringement. Indeed, to qualify as a compliant takedown notice, the notice must contain particularities such as the identity of the copyrighted work allegedly being infringed, the specific location of the allegedly infringing copy, and an affirmation—made under oath and penalty of

149. *See* Ellison v. Robertson, 357 F.3d 1072, 1076 (9th Cir. 2004) (finding that a defendant is a contributory infringer if it (1) has knowledge of a third party's infringing activity, and (2) "induces, causes or materially contributes to the infringing conduct" (quoting Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159, 1162 (2d Cir. 1971))).

150. *See, e.g.*, PAUL GOLDSTEIN, GOLDSTEIN ON COPYRIGHT § 8.1 (3d ed. 2019-2 Supp.) ("To be liable for contributory infringement, the defendant need only have known of the direct infringer's activities, and need not have reached the legal conclusion that these activities infringed a copyrighted work.").

151. *Id.*

152. 17 U.S.C. § 512(c)(1)(A) (2012).

153. *Id.* § 512.

154. *Id.*; UMG Recording, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1021–22 (9th Cir. 2013).

perjury—that these allegations are true.[155] And these particulars must be sent directly to a "designated agent" that the service provider tasks with gathering such information.[156] In essence, this notice-and-takedown structure creates a heightened knowledge requirement, because only notices that meet these specific, high standards impose a takedown obligation on the service provider. Indeed, the statute explicitly states that providers can ignore deficient notices and still gain the protection of the safe harbors.[157]

In the early days of the DMCA, then, there were significant differences between the common-law knowledge standards for contributory infringement and the statutory knowledge standards for safe harbor protection. And as we learned above, nothing was stopping courts from continuing to apply those common-law standards in cases where the DMCA did not apply—or where it did apply but the copyright owner nevertheless sought a § 512(j) injunction. Yet courts have not taken advantage of their independence. Instead, in the years following the DMCA's passage, courts have revised contributory infringement's knowledge element to fall in line with the heightened standards of the DMCA, providing another point of convergence.

This convergence emerged early on, starting with the Ninth Circuit's decision in *Perfect 10, Inc. v. Amazon.com, Inc.* where the court vacated a finding of secondary liability under facts that would also have qualified the service provider for the System Storage safe harbor.[158] The court considered, in part, the secondary liability of Amazon for hosting an alleged direct infringer's copies of Perfect 10's photographs.[159] When determining whether Amazon was contributing to its user's alleged direct infringement, the court cited *Netcom* and concluded that a service provider "can be held contributorily liable if it 'has *actual* knowledge that *specific* infringing material is available using its system,' and can 'take simple measures to prevent further damage' to copyrighted works, yet continues to provide access to infringing works."[160] Such a standard aligned the common law with the statute, departing from the earlier case law in favor of a standard that mimicked the DMCA requirement that a service provider act only when it has specific knowledge of the

155. 17 U.S.C. § 512(c)(1)(A).

156. *Id.* § 512(c)(2).

157. *Id.* § 512(c)(3)(B)(i) ("[A] notification from a copyright owner . . . that fails to comply substantially with the provisions of subparagraph (A) shall not be considered . . . in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.").

158. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1168–70 (9th Cir. 2007).

159. *Id.* at 1156–57.

160. *Id.* at 1172 (citing A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001); Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995)). The court remanded the case to reconsider the contributory infringement claims and consider "whether Google would likely succeed in showing that it was entitled to the limitations on injunctive relief provided by title II of the DMCA." *Id.* at 1175.

infringing material.[161] General knowledge was no longer sufficient for contributory infringement, just as it did not disqualify a service provider from the safe harbors of the DMCA. In other words, the standards for determining culpable knowledge under both statute and case law converged.

The 2013 decision by the court in *Luvdarts v. AT&T Mobility* provides an example of the tail end of convergence in the contributory infringement context.[162] The court dismissed a claim of secondary liability because the copyright holder "fail[ed] to allege that the [defendants] had the requisite specific knowledge of infringement" regarding the copies that their networks were distributing.[163] Just as other post-DMCA courts articulated, mere "conclusory allegations" of infringement were no longer enough; contributory infringement required specific knowledge.[164] The court explained that the copyright holder's notice (a 150-page-long list of titles) did "not identify which of these titles were infringed, who infringed them, or when the infringement occurred."[165] Indeed, although the issue was common-law liability, the court went so far as to point out that these notices did not comply with the statutory requirements: The DMCA, "by which the notices purport to be governed, clearly precludes notices as vague as the notices here."[166] In short, the court found no secondary liability for the very same legal and factual reason that the wireless carriers would have prevailed under the DMCA: the lack of adequate—and statutorily compliant—takedown notices.

2. Findings of Liability

The second convergence scenario involves facts that warrant imposition of copyright infringement liability, along with a determination that the same facts disqualify the defendant from protection under the safe harbors—i.e.,

---

161. *Perfect 10 v. Amazon.com* was a common law case, and not a DMCA case, for the procedural reasons discussed *supra* Section II.B, the lower court had found no prima facie case of infringement and so never had cause to consider the statutory defense. *Id.* at 1175. The Ninth Circuit, after vacating that finding, implicitly recognized the conflation in which it had engaged when it instructed the district court how to approach the issue on remand: "In revisiting the question of Perfect 10's likelihood of success on its contributory infringement claims, the district court should also consider whether Google would likely succeed in showing that it was entitled to the limitations on injunctive relief provided by . . . the DMCA." *Id.*

162. Luvdarts, LLC v. AT & T Mobility, LLC, 710 F.3d 1068, 1072–73 (9th Cir. 2013).

163. *Id.* at 1072. It's not entirely clear from the opinion whether the defendants were engaging in System Storage or some other service; all were providers of Multimedia Messaging Services.

164. *Id.*

165. *Id.* at 1073.

166. *Id.* (noting that the DMCA takedown process "requires the producer to provide '[i]dentification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material'" (alteration in original) (quoting 17 U.S.C. § 512 (2012))).

Box D in our framework. The cases under this scenario are not as numerous as under the first, but they still exhibit convergence. Put simply, there is no reported case where the court found safe harbor immunity while also holding that the defendant was a copyright infringer, despite the potential for such a holding under the DMCA. Instead, the case law, after finding infringement, always finds no safe harbor immunity, with some courts contemplating short-circuiting the analysis altogether, due to convergence, and concluding that liability negates DMCA defenses *per se*.

In *A&M Records v. Napster,* a decision issued a few short years after the DMCA's passage, the Ninth Circuit directly considered whether finding liability absolutely barred DMCA immunity.[167] Napster was one of the first providers of online file-sharing functionality, and its users had uploaded and downloaded copyrighted music. The copyright owners argued "that Napster's potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable *per se*."[168] The argument was based, in part, on the belief that the DMCA safe harbors so mimic the secondary liability standards that once such liability was found, those findings would always preclude a DMCA defense.[169] The Ninth Circuit resisted making such "a blanket conclusion," particularly at a preliminary stage of the litigation.[170] Yet the court did note that many of Napster's actions that were relevant to the infringement analysis also presented "significant questions under [the DMCA] statute" regarding whether the safe harbors were available.[171] The court stopped short of embracing complete convergence, but its recognition of the congruence of the dual inquiries was nevertheless significant, given that the DMCA's case law was still in its infancy.

The Ninth Circuit went a step further on the broad question of convergence ten years later, in *Columbia Pictures v. Fung*.[172] The district court found secondary liability by inducement because the defendant invited users to download copyrighted movies from his company's websites.[173] The copyright owner argued that this finding practically precluded access to the DMCA safe harbors, because an inducer cannot meet the substantive requirements of § 512.[174] In other words, a DMCA analysis was unnecessary because the result was a foregone conclusion under the facts that lead to the

167. A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1025 (9th Cir. 2001).

168. *Id.* (emphasis added).

169. *Id.* The argument was also based on an interpretation of the plain language of the statute—i.e., that the safe harbors are just not applicable to claims of contributory infringement. *Id.* ("The district court did not give this statutory limitation any weight favoring a denial of temporary injunctive relief.").

170. *Id.* (citing S. REP. NO. 105-190, at 40 (1998)).

171. *See id.* (noting that some of these were procedural).

172. Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1023–24 (9th Cir. 2013).

173. *Id.* at 1031.

174. *Id.* at 1039–40 ("Columbia argues, and the district court agreed, that inducement liability is inherently incompatible with protection under the DMCA safe harbors.").

inducement finding.[175] The district court agreed, stating that the liability determination meant that a safe harbor analysis was unnecessary; the defendant could not, as a matter of law, gain safe harbor protection.[176]

On appeal, the Ninth Circuit was more cautious, citing *A&M Records* and concluding, "[w]e . . . think it best to conduct the two inquiries independently . . . ."[177] But the court admitted that "aspects of the inducing behavior that give rise to liability are relevant to the operation of some of the DMCA safe harbors and can, in some circumstances, preclude their application."[178] Again, the court was not willing to reach the blanket judgment that there was complete convergence between finding liability and denying DMCA immunity; it correctly recognized that Congress had stopped short of that conclusion, making it "*conceivable* that a service provider liable for inducement could be entitled to protection under the safe harbors."[179] But it recognized that the common-law liability analysis produces findings that are highly relevant to the DMCA inquiry—and its vision of a defendant who qualifies for the safe harbors despite being otherwise liable remained purely conjectural.[180]

Other courts, while not considering the convergence question so expressly, have found liability and then used much the same analysis to deny DMCA safe harbor protection. The court in *Goldstein v. Metropolitan Regional Information Systems* provides an example.[181] The court found that the complaint stated a case for contributory infringement, based on allegations that the accused website operator had specific knowledge of its users' infringement.[182] (This was yet another System Storage case, in which unauthorized, uploaded photographs "contain[ed] copyright notices within them," making "it . . . difficult to argue that a defendant did not know that the works were copyrighted.")[183] Following the reasoning in *Netcom*, the court concluded that the defendant "knew or had reason to know that the use of the

175. *Id.*

176. *Id.*

177. *Id.* at 1040.

178. *Id.*

179. *Id.* The court explained that "[i]n light of these considerations, we are 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.*

180. *Id.*

181. Goldstein v. Metro. Reg'l Info. Sys., Inc., No. TDC-15-2400, 2016 WL 4257457, at *7–10 (D. Md. Aug. 11, 2016).

182. *Id.* at *4–5.

183. *Id.* (citing Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1374 (N.D. Cal. 1995)).

[photograph] on [its] site was in violation of that copyright."[184] Accordingly, the copyright holder properly pleaded contributory infringement.[185]

This finding of properly pleaded secondary liability, based in part on specific knowledge, was accompanied by a finding that the website operator did not fall within the DMCA safe harbors.[186] The court explained that, while the DMCA safe harbors are a defense, the facts relevant to the contributory liability knowledge requirement also negate the defense's availability.[187] In particular, a notice from the copyright owner, combined with the fact that the photograph in question "contained a watermark indicating that it was copyrighted," supported an inference that the defendant had sufficient actual knowledge to exclude it from the protection of the safe harbors.[188] Here we see almost complete overlap between the inquiries; the same facts that support a finding of infringement also support the inapplicability of the safe harbors. The two converge, rendering the latter analysis irrelevant.

Courts have even imported the DMCA safe harbor's "red flag" test into the secondary liability analysis. Consider the recent district court decision in *Venus Fashions v. ContextLogic*: The allegation was that copyrighted fashion photographs appeared on the defendant's website without the copyright holder's permission.[189] The copyright holder failed to provide specific notice of the URL addresses of the 17,035 copyrighted images on the site.[190] The court nevertheless found that the defendant had "reason to know" that the images were copyrighted and infringing.[191]

On its face, the *Venus Fashions* analysis appears to run counter to the specific knowledge required by the common law and imported from the DMCA. But the System Storage safe harbor has been interpreted to include a "red flag" test for knowledge, where the inquiry is "whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person," regardless of the propriety of the plaintiff's notices.[192] Here the court borrowed this standard from the safe harbors and relied on it when determining secondary liability under the

184. *Id.* at *4 (citing *Netcom*, 907 F. Supp. at 374).

185. *Id.* at *4–5.

186. *Id.* at *6–7.

187. *Id.*

188. *Id.* at *7.

189. Venus Fashions, Inc. v. ContextLogic, Inc., No. 3:16-cv-907-J-39MCR, 2017 WL 2901695, at *6–7 (M.D. Fla. Jan. 17, 2017).

190. *Id.* at *23.

191. *Id.* ("ContextLogic nonetheless has 'reason to know' of the continued Images which have appeared and no doubt will appear on the Wish Website in the future, as well as the indeterminate number of slightly altered but readily identifiable substantially similar Images to those noticed that remain.").

192. Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012) (detailing the "red flags" analysis under the DMCA safe harbors).

common law.[193] As the court explained, "[t]he objective knowledge required for contributory infringement is consistent with the DMCA's knowledge requirement which measures apparent or 'red flag' knowledge by the objective hypothetical 'reasonable person' standard."[194] The court even cites *Netcom* to support this analysis and makes no mention of *Frena*—the ultimate indignity, given that *Frena* and *Venus Fashions* are from the same district.[195] In short, we have yet another instance of a liability finding based on facts that also suffice to deny protection under the DMCA.

* * *

What the foregoing cases reveal is that courts have consistently tailored the common-law liability standards to reflect the DMCA safe harbor standards—particularly in System Storage cases, which dominate the case law. To place these findings in our conceptual framework, consider Table 2.

Table 2. Con/Divergence Case Law

		DMCA SAFE HARBOR STANDARDS	
		Δ's conduct falls within safe harbor	Δ's conduct falls outside safe harbor
COMMON-LAW LIABILITY STANDARDS	Δ not liable	A Convergence: *ALS Scan*; *CoStar*; *BWP Media*; *Parker*; *Luvdarts*	C Divergence: [No cases]
	Δ liable	B Divergence: [No cases]	D Convergence: *A&M Records*; *Fung*; *Goldstein*; *Venue Fashion*

Noticeably absent from our matrix are any instances in which a court found infringement under the common law but immunity via the DMCA safe harbors (Box B) or no liability for conduct that fell outside a safe harbor (Box C). That's because our research revealed no such cases. Divergence simply has not occurred, notwithstanding the freedom courts had in the wake of the DMCA's passage to craft whatever liability standards they saw fit.

193. *See Venus Fashions*, 2017 WL 2901695, at *23 n.15.

194. *Id.* (citing 17 U.S.C. § 512(c)(1)(A)(ii) (2012); UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1125–26 (9th Cir. 2013)).

195. *Id.* at *24 ("Also instructive is the relatively early and influential decision in *Religious Tech. Ctr. v. Netcom* . . . ."). The court also relies upon *Perfect 10* and *Luvdarts*, explored above, which demonstrate convergence between the common-law standard for secondary liability and the DMCA. *Id.*

To be clear, we are not saying that convergence is surprising, or that courts converged because they failed to appreciate that they were free to do otherwise. Indeed, the reasons for convergence are irrelevant to our argument; for our purposes, it is enough to demonstrate that it happened. Nevertheless, let us offer a pair of comments about the dynamics of aligning judicial standards and statutory standards more generally—one comment on those doing the regulating (i.e., courts) and one on those who are regulated.

For courts, efficiency is a likely motivation for the convergence we observed. After all, evaluating the same set of facts under two distinct standards seems redundant. Faced with such a task, one can understand why a court would want the standards to converge. Indeed, one sees the same tendency in trademark law, where courts sometimes use the same set of elements under infringement theories which seem to call for different inquiries.[196] Unless the statutory standard is particularly objectionable, the time savings to be had from using it in common-law cases would naturally lead the courts toward convergence.

For those regulated by a safe harbor regime, judicial efficiency is not much of a concern, but the existence of two sets of standards has an effect nonetheless—a gravitational effect. If a safe harbor offers complete or near-complete immunity, those who might have pushed the envelope by testing the fuzzy borders of a common-law standard will instead likely conform their behavior to the safe harbor, so as to ensure their freedom from liability. And those who might otherwise have been overly conservative in their conduct will feel comfortable going farther (right up to the border of the safe harbor).[197] This dynamic explains why we found so few cases in which the DMCA did not apply; once it was passed, § 512 pulled service provider operations into its orbit, and the courts then dutifully followed with their common-law

196. *See, e.g.*, David S. Welkowitz, *State of the State: Is There a Future for State Dilution Laws?*, 24 SANTA CLARA COMPUTER & HIGH TECH. L.J. 681, 683 (2008) (noting that "federal courts hearing . . . [both federal confusion-based claims and supplemental state dilution-based claims] . . . often inserted a requirement of confusion into [state anti-dilution] statutes that expressly disclaimed the need for it."); *see also* Jada Toys, Inc. v. Mattel, Inc., 496 F.3d 974, 980 & n.3 (9th Cir. 2007) (holding that analysis of dilution claims under federal and California law is the same despite absence of certain federal elements in state counterpart), *overruled on other grounds by* Jada Toys, Inc. v. Mattel, Inc., 518 F.3d 628 (9th Cir. 2008). In fact, some have argued in the trademark context that the presence of legislation has "short-circuited the common law's traditional method of dealing with new problems" and "instant legislative solutions" should therefore be avoided. *See* Suzanna Sherry, *Haste Makes Waste: Congress and the Common Law in Cyberspace*, 55 VAND. L. REV. 309, 311, 317, 349–57 (2002) (making this argument with regard to cybersquatting on domain names and the Anticybersquatting Consumer Protection Act). Our thanks to Rebecca Tushnet for pointing out some of these parallels.

197. For an excellent general discussion of the gravitational effect of safe harbors, see generally Susan C. Morse, *Safe Harbors, Sure Shipwrecks*, 49 U.C. DAVIS L. REV. 1385 (2016) (discussing the gravitational effect of safe harbors). *See also* Gibson, *supra* note 103, at 938 (noting that attempts to introduce bright-line rules into copyright law "often end up compromising flexibility and adaptability without providing much clarity or protection for users, as courts convert safe harbors into the only harbors, floors into ceilings, and minimums into maximums").

convergence. We now turn to whether that convergence was a good thing or bad.

IV. CONFLATION

In some ways, convergence is a good thing. First, *Netcom* was the better case on the merits, so its takeover of the case law was a welcome development. Second, as cases from the different jurisdictions converge around the statutory standards, they also naturally converge around each other too, creating more-or-less consistent liability standards nationwide even when the DMCA does not apply. Even those that might dislike those standards have to admit that certainty and consistency are good things.

But convergence also means that the DMCA's inherent cost/benefit calculus is now very different from how it was in 1998. In essence, the DMCA offered service providers a deal. On the cost side, all they had to do was comply with certain easy-to-satisfy conditions: adopt standard technical measures, implement a repeat infringer policy, and (for three of the four safe harbors) register an agent to receive takedown notices. The benefit they would receive in return would be legal protection for vital parts of their network operations—protection that was especially valuable in light of the possibility that courts might adopt more demanding standards, as *Frena* had done.

What we will demonstrate in this final part of the Article is that both sides of this calculus have changed. On the one hand, the benefits of the DMCA's safe harbors have decreased, now that the otherwise applicable case law provides essentially the same protection. On the other hand, the costs of the DMCA have increased, because now that courts look to the DMCA to define liability, convergence has led to conflation; the statute's ancillary provisions have begun to be used as substantive law, which creates unwarranted forms of liability and immunity alike. Our evidence on the latter point is a set of troublesome cases, but we buttress our argument with some empirics, including data that shows that many online service providers are not even taking the minimal steps necessary to avail themselves of three of the four safe harbors. This suggests that the recalibration of costs and benefits is having a deleterious effect not just on the minds of judges, but also on the behavior of the very service providers whom the statute is supposed to benefit.

A. REDUCED BENEFITS

On the benefits side, the argument should not take long now that we have reviewed the case law. Convergence means that the case law standards and the safe harbor standards are essentially the same. That was not always the case. As we saw in Part II, courts used to be all over the place on what constituted infringement by service providers, creating great uncertainty as to what the liability standards actually were. Convergence only occurred over time.

Now that convergence has occurred, however, courts are providing the same certainty (and applying the same standards) without any need to resort to the statute. And the utter lack of any divergent cases is ample evidence that the liability standards have not only converged, but stabilized. No one thinks *Frena* is going to make a comeback. Indeed, we have recently seen a court from the same district as *Frena* decide an online infringement case without even citing that once-leading precedent.[198] This means that a service provider can enjoy the benefit of the safe harbors without actually invoking them. Convergence has made the benefits of invoking the DMCA essentially evanescent.

This is not to say that removing the statute from the books would be a good idea. Repealing the Act would mean removing its gravitational effect, which could destabilize the common law, give rise to circuit splits, and impose unneeded uncertainty in the online environment. But a service provider that wants to take advantage of the DMCA's standards can now comfortably rely on the case law alone, essentially availing itself of the statutory benefits without paying the statutory costs. And, as we will now see, those costs can be significant.

B. CONFLATIONARY COSTS

Some costs to service providers of complying with the DMCA have been present since 1998, such as the cost of implementing a system for tracking repeat infringers. And as the amount of user-generated content on the Internet has increased, so has the potential for costly abuse of the DMCA process, including "notices" that purport to invoke the statute but in fact are not compliant with it—or, worse yet, have nothing to do with copyright at all.[199]

Other costs, however, are the more recent result of convergence turning into conflation. By conflation, we mean a mixing and matching of common-law standards and statutory provisions irrelevant to infringement to create new, unintended, and unhelpful forms of liability and immunity. The following discussion identifies some forms that this conflation has taken and the costs that it imposes.

1. *BMG v. Cox*: New Liability

No case better exemplifies the transition from helpful convergence to harmful conflation than 2018's *BMG Rights Management (US) LLC v. Cox*

198. *See Venus Fashions*, 2017 WL 2901695, at *1. The court did, however, get on the convergence bandwagon by citing the DMCA in its discussion of common-law issues. *E.g.*, *id.* at *23 (citing DMCA cases when discussing liability standards for contributory infringement).

199. *See, e.g.*, Jennifer M. Urban et al., *Takedown in Two Worlds: An Empirical Analysis*, 64 J. COPYRIGHT SOC'Y U.S.A. 483, 486–87 (2017); *Takedown Hall of Shame*, ELEC. FRONTIER FOUND., https://www.eff.org/takedowns [https://perma.cc/C9RN-XBQ8].

Communications, Inc.[200] BMG claimed that its investigating agent, Rightscorp Inc., had observed more than two million instances in which a Cox subscriber had made one of BMG's copyrighted songs available for download via BitTorrent, the popular file-sharing program. Unlike almost every other service provider we have discussed so far, however, Cox itself did not host any infringing content or help its subscribers find it. This was not a case of System Storage. As the Fourth Circuit noted:

> As a conduit ISP, Cox only provides Internet access to its subscribers. Cox does not create or sell software that operates using the BitTorrent protocol, store copyright-infringing material on its own computer servers, or control what its subscribers store on their personal computers.[201]

The obvious question, then, is what theory of liability BMG proposed to apply. Cox's servers may have played a role in the upload and download of copyrighted materials, but *Netcom*'s volitional requirement (which the Fourth Circuit had adopted in *ALS Scan*)[202] lays the responsibility for that conduct at the feet of the subscribers, not the provider. As for contributory infringement, one can understand imposing liability on a service provider that knows it is hosting infringing content and fails to do anything about it, as in cases like *Goldstein*.[203] Even *Frena*, the case most unfriendly to service providers, had involved a service provider that hosted infringing material for others to download, rather than only providing Internet connectivity.[204]

But Cox hosted nothing. It merely transmitted data, some of which was innocuous, like email and web surfing, and some of which was infringing, like torrents of BMG music. In other words, Cox was the poster child for immunity under the Transitory Communications Safe Harbor in § 512(a). And it satisfied all five statutory conditions necessary to qualify for that safe harbor's protection. First, Cox's subscribers initiated each transmission.[205] Second, Cox automatically and indiscriminately transmitted the material.[206] Third, the

200. BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc., 149 F. Supp. 3d 634, 638–76 (E.D. Va. 2015). We will be referring to three different opinions in the case: the district court's summary judgment ruling, *BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc. (Cox SJ)*, 149 F. Supp. 3d 634 (E.D. Va. 2015), the district court's disposition on post-trial motions, *BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc. (Cox Post-Trial)*, 199 F. Supp. 3d 958 (E.D. Va. 2016), and the Fourth Circuit's decision on appeal, *BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc. (Cox Appeal)*, 881 F.3d 293 (4th Cir. 2018).

201. *Cox Appeal*, 881 F.3d at 299.

202. *See supra* notes 125–32 and accompanying text.

203. *See supra* notes 181–88 and accompanying text. We leave vicarious infringement out of the discussion here; BMG made such a claim, but the district court did not seem impressed by it, *Cox SJ*, 149 F. Supp. 3d at 676 (calling the evidence "hardly overwhelming"), and the jury ultimately rejected it, *Cox Post-Trial*, 199 F. Supp. 3d at 963.

204. Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993).

205. 17 U.S.C. § 512(a)(1) (2012).

206. *Id.* § 512(a)(2).

subscriber chose the destination, not Cox.[207] Fourth, Cox made no lasting copy of the material.[208] Finally, the material was not modified along the way.[209]

In the world of convergence described above, Cox would have escaped liability by squarely falling within the borders of § 512(a). What actually transpired, however, is that a jury found Cox liable for $25 million in damages for willful contributory infringement[210]—the first time in the history of copyright law that a mere conduit had been held liable. What happened?

One possibility is that the case is, at long last, an example of court taking advantage of the freedom that Congress gave it to forge a new standard for copyright liability, rather than conform them to the DMCA's safe harbors. In other words, *BMG v. Cox* could be an example of the kind of divergence contemplated by Box B in our matrix, where the defendant's conduct falls within a safe harbor but a court nevertheless finds liability. If that were the case, the ruling would be unprecedented, but it would be well within the structure that Congress contemplated when it opted to create safe harbors and leave the question of ultimate liability to the courts. One could argue with the merits of the new standard, but one could neither blame the DMCA for it nor view its creation as *ultra vires*.

Unfortunately, that is not what *BMG v. Cox* represents. The case offers no new common-law theory of liability that would explain how and why the law would impose liability on a defendant whose involvement with the copyrighted works is so fleeting. Instead, it simply recites the long-established elements familiar to us from earlier cases, namely knowledge of infringing activity and material contribution thereto.[211] How then did the court arrive at a judgment of infringement? The answer lies in the conflation of a DMCA threshold requirement with substantive liability standards.

Recall that one of the threshold requirements for safe harbor eligibility is that a service provider must implement a policy of terminating the accounts of repeat infringers.[212] And here the evidence against Cox was damning; the company had such a policy, but it did all it could to avoid implementing it.[213] Cox hesitated to terminate those subscribers who its own employees learned were repeatedly infringing, let alone those whose infringement was alleged by copyright owners, and even when it did terminate it often reactivated

207. *Id.* § 512(a)(3).

208. *Id.* § 512(a)(4).

209. *Id.* § 512(a)(5).

210. Verdict Form at 1–2, BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc., No. 1:14-cv-1611, 2015 WL 9999710 (E.D. Va. Dec. 16, 2015).

211. *See* Judge's Instructions/Charge to the Jury at 31–32, BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc., No. 1:14-cv-1611, 2015 WL 13132290 (E.D. Va. Dec. 16, 2015).

212. *See supra* Section II.B.2.iii.

213. BMG Rights Mgmt. (US) v. Cox Commc'ns, Inc. (*Cox Appeal*), 881 F.3d 293, 303–05 (4th Cir. 2018).

subscribers right away.[214] The court accordingly ruled that Cox had "failed to implement its policy in any consistent or meaningful way—leaving it essentially with no policy."[215] What this meant was that, although Cox fit perfectly within the Transitory Communications Safe Harbor, it could not take advantage of its protection. The absence of a meaningful repeat-infringer policy rendered the entire DMCA a non-factor, and the court would determine liability under the common law only.[216]

What should be apparent by now, however, is that unless the court was prepared to articulate a novel and unprecedented theory of conduit liability, the DMCA's unavailability should have made no difference in the ultimate outcome. After all, in contrast to the safe harbors, the repeat-infringer provision was not rooted in any recognized basis for service provider liability; it was merely an encouraged best practice, and the consequence of disregarding it was not a judgment of infringement but merely the loss of DMCA protection and relegation to a common-law determination.[217] And under the common law, Cox would be fine. Its lack of volition would preserve it from direct infringement claims. And only one element of contributory infringement would ever be present at any one time; by the time a notice created the requisite knowledge, Cox would no longer be substantially participating in any infringement or facilitating access to the material at issue. This lack of liability for conduits is exactly as one would expect from a world in which the common-law infringement standards had converged with the safe harbor standards.

Instead of ignoring the DCMA and focusing on the common law, however, the district court conflated the repeat-infringer requirement with the ultimate liability standard. For evidence of Cox's knowledge of infringement, the court cited the many notices BMG had sent to Cox, notices which provided the IP addresses of users whom Rightscorp had allegedly seen offering copyrighted material for download.[218] Characterizing those notices as "DMCA-compliant," the court found that they constituted "powerful evidence of a service provider's knowledge."[219]

---

214. *Id.* at 304.

215. *Id.* at 305.

216. *See id.* at 313. This is what opened Cox up to a damage award. Had it properly implemented a repeat-infringer policy, it could still have been held liable—the court could still have diverged from § 512(a)'s safe harbor principles and used a broader liability standard—but BMG would have been limited to narrow injunctive relief under § 512(j)(1)(B).

217. *See supra* Section II.B.2.iii.

218. BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc. (*Cox SJ*), 149 F. Supp. 3d 634, 671 (E.D. Va. 2015); BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc. (*Cox Post-Trial*), 199 F. Supp. 3d 958, 976 (E.D. Va. 2016); *see also Cox Appeal*, 881 F.3d at 312 (characterizing Cox's treatment of the BMG notices as "the primary theory for liability advanced by BMG").

219. *Cox SJ*, 149 F. Supp. 3d at 662 (citing UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1020 (9th Cir. 2013). The Fourth Circuit later pushed back against some aspects of the district court's handling of the knowledge element, but it left intact the part about

At first glance, this seems sensible. After all, notices are the usual way to establish knowledge on the part of those who host copyrighted works. Indeed, every single case *BMG v. Cox* cited in support of the notion that notices could create culpable knowledge involved a service provider that was hosting material.[220] But on further inspection, it becomes clear that not only was the court invoking a statute that it had ruled irrelevant, but it was invoking it inaccurately. Cox was not a host. It was a conduit. And there is no such thing as a "DMCA-compliant" notice for conduits, because (as we have seen) the DMCA imposes no notice-and-takedown regime on conduits. As the case law has consistently recognized, Congress gave conduits protection under § 512(a) regardless of whether they register an agent, regardless of whether they receive notices from copyright owners, and regardless of whether they take action upon learning of an alleged infringement.[221]

Moreover, notices sent to a conduit not only arrive too late for anything to be done, but they also lack the many statutory safeguards that protect against overreaching by copyright owners. The sender of a truly DMCA-compliant notice must vouch for its bonafides under penalty of perjury, and civil liability exists for material misrepresentation.[222] In addition, service providers can create a counter-notification system through which a user can contest the infringement allegation and have the takedown reversed.[223] The

---

the DMCA notices, which the appeals court acknowledged as "the primary theory for [Cox's] liability." *Cox Appeal*, 881 F.3d at 312.

220. The summary judgment ruling cited *Capitol Records, LLC v. Escape Media Grp., Inc.*, No. 12-CV-6646 (AJN), 2015 WL 1402049, at *43 (S.D.N.Y. Mar. 25, 2015) (music streaming); *Perfect 10, Inc. v. Giganews, Inc.*, No. CV 11-07098-AB (SHx), 2014 WL 8628031, at *7 (C.D. Cal. Nov. 14, 2014) (Usenet hosting); *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090, 1107 (W.D. Wash. 2004) (photos on websites); and *Ellison v. Robertson*, 357 F.3d 1072, 1077 (9th Cir. 2004) (Usenet hosting). *See Cox SJ*, 149 F. Supp. 3d at 671–72. The ruling on post-trial motions added *Netcom*, *Capitol Records, Inc. v. MP3tunes, LLC*, *Arista Records LLC v. Usenet.com, Inc.*, and *CoStar Grp. Inc. v. LoopNet, Inc. See Cox Post-Trial*, 199 F. Supp. 3d at 976. And the Fourth Circuit cited nothing but BMG's brief. *Cox Appeal*, 881 F.3d at 312. All of the cited cases involved the hosting of material by the defendant, not its mere transmission. Only *Ellison* was at all ambiguous on this point, because the court included some mystifying dicta saying that a service provider that hosted Usenet material for two weeks (and therefore could have examined and taken the material down upon receiving notice) could still somehow be considered a conduit. *See Ellison*, 357 F.3d at 1081. For procedural reasons, the court declined to rule on whether § 512(c) also applied. *See id.* at 1081 n.12.

221. *See* 17 U.S.C. § 512(a) (2012); *accord In re* Charter Commc'ns, Inc., Subpoena Enf't Matter, 393 F.3d 771, 776 (8th Cir. 2005) ("The absence of the remove-or-disable-access provision (and the concomitant notification provision) makes sense where an ISP merely acts as a conduit for infringing material—rather than directly storing, caching, or linking to infringing material—because the ISP has no ability to remove the infringing material from its system or disable access to the infringing material."); Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc., 351 F.3d 1229, 1235 (D.C. Cir. 2003) ("No matter what information the copyright owner may provide, the ISP can neither 'remove' nor 'disable access to' the infringing material because that material is not stored on the ISP's servers.").

222. *See* 17 U.S.C. § 512(c)(3)(A)(vi) (mentioning penalty of perjury); *see also id.* § 512(f) (mentioning civil liability).

223. *Id.* § 512(g).

most important safeguard, however, is that because true DMCA notices concern hosted material, the service provider can examine the material firsthand and verify that it appears to be infringing. After all, the material is on its own network.[224] In contrast, a notice to a conduit is not a DMCA notice at all, which means it lacks these safeguards and leaves the service provider no choice but to accept the copyright owner's self-interested allegation at face value; it cannot locate the allegedly infringing material at all, only the alleged infringer.[225] For these reasons, in a related context—requests for subpoenas under § 512(h)—several courts have pointed out that sending a DMCA-style notice to a conduit replaces the statutory safeguards with a mere "conclusory allegation."[226]

In short, notices to a conduit may or may not be relevant to whether a repeat-infringer policy has been reasonably implemented.[227] But by dint of timing and unverifiability, they have no relevance to whether a conduit has the requisite knowledge to be a contributory infringer. To focus on such notices once the DMCA is rendered irrelevant is to conflate a statutory safe-harbor threshold requirement with a common-law liability standard.

This is not to say that we should shed tears for Cox Communications, whose internal documents demonstrated a contempt for copyright law.[228] But

224. This is also true in System Caching situations. Likewise, Information Location service providers can follow their own links or search results to the material in question and subject it to firsthand examination. This is why it is so odd that the court in *Cox SJ* characterized BMG's notices as "DMCA-compliant." *Cox SJ*, 149 F. Supp. 3d at 662. To comply with the DMCA, a notice must include "information reasonably sufficient to permit the service provider to locate the material." 17 U.S.C. § 512(c)(3)(A)(iii).

225. Even this overstates the utility of the information provided in the BMG notices; in reality, Cox could use the information only to identify the *account* used in the alleged infringement. Identifying what individual was using a particular account would be impossible no matter what BMG provided.

226. *See In re* Subpoena to Univ. of N.C. at Chapel Hill, 367 F. Supp. 2d 945, 952 (M.D.N.C. 2005) ("Without the contents of the notification, there would not be a basis for the subpoena, except for a conclusory allegation that the subpoena is sought to obtain the identity of an alleged infringer."); *accord In re* Charter Commc'ns, Inc., 393 F.3d at 776–77 (agreeing with service provider's argument that "the text and structure of the DMCA require the ISP to be able both to locate and remove the allegedly infringing material before a subpoena can be issued against it"); *Recording Indus.*, 351 F.3d at 1237 ("[A]n ISP performing a function described in § 512(a), such as transmitting e-mails, instant messages, or files sent by an internet user from his computer to that of another internet user, cannot be sent an effective § 512(c)(3)(A) notification.").

227. The Fourth Circuit was careful not to rely solely on the notices from BMG when affirming the repeat-infringer ruling; there was plenty of evidence that Cox ignored repeat infringers that it had identified itself, without BMG's help. *See* BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc. (*Cox Appeal*), 881 F.3d 293, 304–05 (4th Cir. 2018); *cf.* David Nimmer, *Repeat Infringers*, 52 J. COPYRIGHT SOC'Y U.S.A. 167, 182 (2005) (arguing both that one can be an infringer for "repeat infringer" purposes without a corresponding notice and that a notice does not necessarily make one an infringer).

228. *See, e.g.*, *Cox Appeal*, 881 F.3d at 303–05. Those emails must have made for some gleeful reading when BMG's attorneys got their hands on them; one of them summarized Cox's so-called termination policy as: "DMCA = reactivate." *Id.* at 303.

contempt is not culpability. The company's blameworthy behavior made it an easy defendant to rule against, yet those rulings have left other service providers bereft of direction. What exactly are conduits to do if they want to avoid liability for the infringement of their subscribers? Terminate after the first (unverified) allegation of infringement arrives? After the second? The fifth? The hundredth? What must the notice contain? The reason the answers are so unclear is that the liability derives from a mishmash of statutory provisions that were never meant to be determinative of liability in the first place.

Even the district court seemed to realize the difficulty its ruling presented. After accepting the jury's $25 million verdict, the court nonetheless denied BMG's request for a permanent injunction. In doing so, it cited a long list of questions that Cox would have to answer to avoid violating the injunction:

> Is Cox required to suspend accused infringers, or simply terminate them upon one notice, or after the second notice? What if BMG sends ten notices for one IP address in one hour, or one minute? If the injunction requires termination of "repeat" infringing subscribers in appropriate circumstances, when is a subscriber a "repeat" infringer, and what are the "appropriate circumstances" for termination? Does the order permit or require suspension before termination? Can Cox warn the account holder first? Is Cox permitted to give customers an opportunity to respond to the accusations against them, or is it required to terminate accused infringers and provide them no redress? If the subscriber denies the accusation, what process will exist to adjudicate the accusation by BMG? Can Cox implement a counter-notice process such as the DMCA provides for storage providers? What if, for example, the subscriber's computer was infected with malware, the user's network password was stolen, or a neighbor or guest accessed the user's account?[229]

These questions are, as the court said, "well-founded."[230] But if they are too hard for Cox to answer now, when it has several detailed judicial opinions to guide it, how could it have known how to answer them back in 2011 when Rightscorp started sending notices?

Despite these reservations, however, neither the district court nor the appeals court pushed back against the central conceit of the case: that a copyright owner can impose liability on a conduit merely by sending it a torrent of unverifiable allegations of infringement (infringement from the

229. BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc. (*Cox Post-Trial*), 199 F. Supp. 3d 958, 995 (E.D. Va. 2016) (quoting Cox's memorandum in opposition to BMG's motion for permanent injunction).

230. *Id.*

past, mind you, about which nothing can now be done) and demanding the termination of the targeted subscribers' accounts.[231] This goes well beyond any basis for infringement ever articulated in the common law. Of course, had the court affirmatively claimed to be articulating a new form of liability—one that would apply even though the defendant's conduct fell within the Transitory Communications safe harbor—then this would simply be an example of deliberate divergence, a permissible (albeit singular) lawmaking of the Box B variety. But liability's ingredients here were explicitly rooted in the DMCA's repeat-infringer provision, which was carelessly conflated with the notice-and-takedown scheme from irrelevant and inapplicable safe harbors, emerging from the oven as a new liability standard. As the legislative history of the DMCA warns us, "[s]ection 512 does not create any new liabilities for service providers . . . ."[232] Except, apparently, when it does.

2. *Ventura Content v. Motherless*: New Immunity

Conflation can go the other direction as well, creating immunity that neither the common law nor the four DMCA safe harbors contemplated. Consider the recent Ninth Circuit decision in *Ventura Content v. Motherless*.[233] Joshua Lange is the owner and sole employee of Internet site Motherless.com, the content of which is stored on servers that Lange personally owns and maintains.[234] The site contains "over 12.6 million mostly pornographic pictures and video clips."[235] The content is "uploaded by the site's users, and the uploaders may or may not have created the material."[236]

Lange actively screens much of the material posted on the site.[237] He removes any child pornography that he finds, because it is unlawful, and he also removes bestiality materials because they are illegal in some European countries and because some of his European advertisers voiced concerns about the presence of such content on his site.[238]

---

231. The Fourth Circuit did remand the case, because the district court had failed to use a standard of actual knowledge of specific infringement. *Cox Appeal*, 881 F.3d at 307–12. But it doubled down on what it called "the primary theory for liability advanced by BMG"—namely, that BMG's many notices to Cox were "powerful evidence from which a reasonable jury could find [liability]." *Id.* at 312.

232. H.R. REP. NO. 105-551, pt. 2, at 64 (1998).

233. Ventura Content, Ltd. v. Motherless, Inc., 885 F.3d 597, 603–19 (9th Cir. 2018).

234. *Id.* at 600.

235. *Id.*

236. *Id.*

237. *Id.* at 605. In addition, "[e]ach time that a user uploads a file, he receives a warning on his computer screen that says 'Anyone uploading illegal images/videos will be reported to the authorities. Your IP address . . . has been recorded. Any images/videos violating our Terms of Use will be deleted.'" *Id.* at 601.

238. *Id.* at 605. "We have been directed to nothing in the record that establishes a factual dispute about whether Lange actually exercises judgment about what to host beyond his screening out child pornography, bestiality, and infringing material." *Id.* at 607.

Traditionally, such screening is relevant to many secondary liability theories. Most directly, screening is evidence of the right and ability to control, one of the two elements of vicarious infringement.[239] Active screening can also create specific knowledge of infringement, or at least the circumstances that can establish such a level of knowledge, which is relevant to contributory infringement.[240]

In a world of convergence, however, the same considerations would bear on the availability of the System Storage safe harbor to immunize Lange. And not surprisingly, the copyright holders of the uploaded pictures and clips pointed to Lange's screening as a basis for excluding him from the protection of the safe harbor—and for imposing liability as well.[241] They argued that the statutory language grants immunity only if the posting of the copyrighted materials was "at the direction of a user," which was arguably not the case when Lange screened each submission.[242] And even if one views the postings as done by users, Lange's screening would seem to create the actual or red-flag knowledge of specific infringement that would place him outside the statutory protection.[243]

So far, so good. But then, in response, Lange cited § 512(m) of the DMCA.[244] That section reads:

> (m) PROTECTION OF PRIVACY.—Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on—
>
> > (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

239. *See, e.g.*, Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262–63 (9th Cir. 1996) (noting that defendant "controlled and patrolled" the premises); *see also* Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1058 (9th Cir. 2017) ("The service provider exerts 'high levels of control,' for example, when it . . . provides 'detailed instructions regard[ing] issues of layout, appearance, and content.'" (alteration in original) (quoting UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1030 (9th Cir. 2013))).

240. *See, e.g.*, Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 31 (2d Cir. 2012) (discussing "red flag" based knowledge).

241. As one would expect in a world of convergence, the court considered the safe harbor question and the liability question to be one and the same. *See, e.g.*, *Ventura*, 885 F.3d at 608 (stating as part of DMCA analysis that "[i]f the website provider actually knows that the material for which relief is sought is infringing, or if the infringement is 'apparent,' he remains liable if he does not expeditiously remove the material upon gaining knowledge").

242. *Id.* at 604 (quoting 17 U.S.C. § 512(c)(1) (2012)).

243. *Id.* at 604–05 (interpreting 17 U.S.C. § 512(c)(1)(a)(i)–(ii)). As we have already seen, these safe harbor standards map precisely onto the common-law standards for direct and contributory infringement. *See supra* Section II.B.2.

244. *Id.* at 605 (citing 17 U.S.C. § 512(m)).

> (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.[245]

Lange's argument was that this provision means that the act of screening can never deprive a service provider of DMCA safe harbor protection.[246]

Surprisingly, the Ninth Circuit agreed with Lange.[247] The court 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."[248] The court "read [§] 512(m) to say that Congress expressly provided that such screening does not deprive a website of safe harbor protection."[249] Thus, the act of screening could not be used to deny Lange of DMCA safe harbor protection, and, in turn, copyright infringement immunity.

We are not saying that this interpretation of § 512(m) was the key to Ventura's victory in the case; there were other reasons the court found the plaintiff not liable.[250] But, as in *BMG v. Cox*, this reading of the statute takes a provision irrelevant to immunity—here, a provision that merely clarifies that service providers have no affirmative screening obligation—and conflates it with the substantive standards of the safe harbors themselves. Some fields of law have statutory safe harbors that explicitly immunize screening from liability, such as § 230 of the Communications Decency Act.[251] But the DMCA is not one of them; § 512(m) merely removes screening as a condition for accessing the safe harbors, without changing their substance. As the title to the section ("Protection of Privacy") suggests, the provision frees service providers from any obligation to spy on their users.[252] If they choose to do so anyway, they must accept the consequences.

Under *Ventura*, however, a service provider's screening becomes a new substantive defense, a new category of conduct for which the statute grants immunity. Screening activity would normally be relevant to the specific knowledge element, which under both the common law and the DMCA would inform the liability determination. Instead, the Act mutates to expand the safe harbors beyond the enumerated four and shield individuals like Lange from liability where it might otherwise be found.

---

245. 17 U.S.C. § 512(m).

246. *Ventura*, 885 F.3d at 605.

247. *Id.* at 604–05.

248. *Id.* at 605.

249. *Id.*

250. *Id.* at 605–06 (noting, for example, that the posting of material was initiated by the users, not Motherless).

251. 47 U.S.C. § 230(c) (immunizing online platforms that block or screen offensive material from liability as publisher or speaker).

252. *See* 17 U.S.C. § 512(m).

This again is an act of conflation. Section 512(m) was never supposed to create a new zone of non-liability (i.e., immunity for screening by service providers), yet that is exactly how *Ventura* interprets it. This is the result of further reliance on the DMCA to shape the general scope of copyright liability for service providers, as seen in Part III above. If the common law and the statute were not so closely aligned, courts would not so blithely invoke statutory provisions to render liability judgments. And just as this conflation can create new liability, it can also work in the other direction—providing immunity where it does not belong, and where a court not distracted by the statute would never grant it.

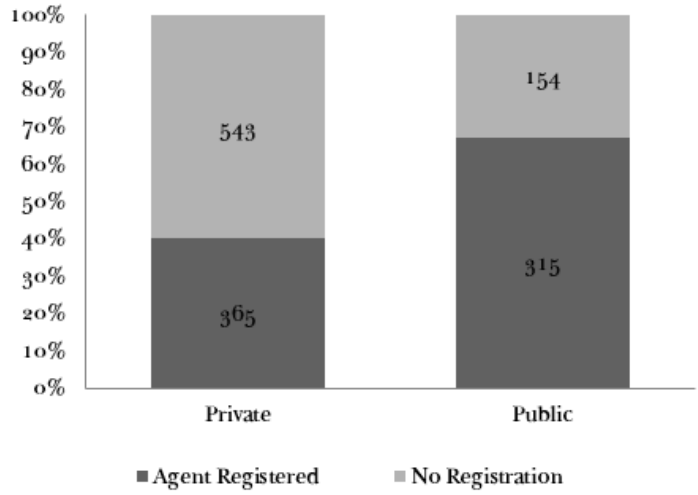
C. *REAL-WORLD EFFECTS OF CONFLATION*

It's no coincidence that we see costly conflation emerge only after convergence was basically complete. That's when the distinction between common-law liability and the safe harbor standards is most difficult to perceive, and where mixing and matching of statutory and common-law standards is therefore most likely to happen. Still, *BMG v. Cox* and *Ventura Content v. Motherless* are only two cases. Maybe they are not harbingers of more conflation to come. After all, hard cases make bad law (as do bad defendants, much to Cox's dismay).

We do have, however, two additional data points relevant to the conflation we have observed in the case law—namely, the documented behavior of those who have to manage DMCA compliance at the service provider level. The data comes from a survey we conducted of DMCA agents at colleges and universities. These institutions act as service providers for their students and employees in a number of ways, and the survey tested them all. The full study is published elsewhere,[253] but of particular importance to the current discussion are two results.

253. *See generally* Christopher A. Cotropia & James Gibson, *Higher Education and the DMCA*, 25 RICH. J.L. & TECH., no. 2, 2018 (publishing the results of a survey of colleges and universities regarding DMCA and copyright policies).

Figure 1. DMCA Registration for Public and Private Colleges



First, in order to send the survey to DMCA agents in higher education, we needed their contact information. Fortunately, the DMCA requires agents to be registered with the U.S. Copyright Office; failure to register means that three of the four safe harbors are unavailable.[254] What we found, however, is that despite the consequences of not having an agent, over half (50.6 percent) of all four-year colleges and universities in the United States had not registered one, and the figure rose to 57.1 percent if we included those whose contact information was outdated. We considered whether this was because public universities enjoy sovereign immunity from copyright suits,[255] but in fact the registration rate is actually higher among public institutions, as shown in Figure 1.

What this means is that in the world of higher education—an industry that for years has been very much in the crosshairs of copyright owners[256] —more than half of institutions do not think it worthwhile to comply with the regulations necessary to gain the protection of three of the four safe harbors. Back when the DMCA was first passed, this failure to register an agent would represent copyright malpractice. But in these days of convergence, when

254. *See supra* note 63 and accompanying text.

255. *See* Coyle v. Univ. of Ky., 2 F. Supp. 3d 1014, 1017 (E.D. Ky. 2014). Another possibility is that automation and private agreements between service providers and copyright owners have displaced legal compliance—but so far it appears that only the most successful commercial platforms are using such alternatives, such that they have not penetrated the service-provider industry in sufficient numbers to explain the overall lack of agent registration. *See* Sag, *supra* note 3, at 506, 539 (noting that providers "with substantial resources" are using such methods by citing "typically large-scale commercial enterprises" such as YouTube and Facebook as examples).

256. *See* Cotropia & Gibson, *supra* note 253, at 3–4.

service providers can receive essentially the same protection from courts without the need to create a DMCA infrastructure, it has become par for the course.

Now consider the second data point. The survey presented respondents with three factual scenarios, intended to mimic the conduct captured in three of the four safe harbors: Transitory Communications, System Storage, and Information Location.[257] The Transitory Communications scenario asked them if they would feel "a legal obligation to take action" if they received a notice from a copyright owner alleging that they provided Transitory Communications for a copyright infringement. Astonishingly, 91.9 percent answered yes, even though no takedown is necessary under that safe harbor.[258] In contrast, only 76.7 percent gave an affirmative answer when asked the same question about System Storage, and 62.2 percent about Information Location —both of which require notice-and-takedown to preserve the safe harbor defense.[259]

What does this second data point tell us about convergence and conflation? There are a number of possible explanations for this seemingly strange result, and we discuss them in our previous study.[260] Among the most likely, however, is that those service providers unsophisticated enough to register an agent in the first place maintain that unsophistication when receiving notices from copyright owners. Like the judges in *BMG v. Cox*, they fail to distinguish between the need to track infring*ers*, for repeat-infringer purposes, and the need to respond to a particular allegation of infringe*ment*, for immunity purposes. After all, most DMCA agents in our survey were housed in information technology departments, not general counsels' offices.[261] They can therefore be forgiven for thinking that a notice is a notice is a notice, and that every notice has the same legal significance. In short, conflation is occurring not just in the courts, but in the trenches.

V. CONCLUSION

When the Digital Millennium Copyright Act became law in 1998, it provided badly needed certainty in a world of inconsistent common-law standards. Its enactment freed up entrepreneurs to harness the power of user-generated content without fear of crippling copyright liability. Without it, our culture and our economy would look very different, and not in a good way.

257. The fourth safe harbor, System Caching, is generally not as important, so for simplicity's sake we left it out.

258. Note that we conducted the survey before the *BMG v. Cox* case.

259. *See* Cotropia & Gibson, *supra* note 253, at 19.

260. *See id.* at 26–29. Note that the most important motivation for respondents' handling of the three scenarios was to limit their institution's exposure to legal liability, *see id.* at 21–22, which suggests that they did indeed misunderstand the DMCA itself.

261. *Id.* at 12.

Today, however, we come not to resurrect the DMCA, but to bury it. We are not calling for a repeal; given the statute's proven gravitational effect, keeping it on the books is worthwhile, if only to ensure stability in the common law. But that common law has caught up with the statute to the point where the two have converged, eliminating the unique benefit that the Act once conveyed and thus diminishing its importance. At the same time, the cost of complying with the Act has risen; convergence has begotten conflation, making it more difficult for courts and practitioners alike to distinguish between substantive legal standards and ancillary, regulatory rules. Going forward, then, service providers would be well advised to rely exclusively on copyright's case law. Despite the DMCA's two decades of faithful service, the time has come to resist its temptations and steer clear of its clutches altogether.