2019

Convergence and Conflation in Online Copyright

Christopher A. Cotropia
University of Richmond - School of Law, ccotropi@richmond.edu

James Gibson
University of Richmond - School of Law, jgibson@richmond.edu

Convergence and Conflation in Online Copyright

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

ABSTRACT

The Digital Millennium Copyright Act 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.

At first glance, this convergence 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 caused courts to conflate the two different sets of standards, mixing and matching them in unpredictable and counterproductive ways to 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.

[*] Professor of Law, Director of Intellectual Property Institute, University of Richmond School of Law.

[†] Professor of Law, University of Richmond School of Law.

TABLE OF CONTENTS

Convergence and Conflation in Online Copyright

INTRODUCTION

The Digital Millennium Copyright Act[1] is the most important piece of copyright legislation of the last forty 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 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 today.[3] It is no exaggeration to say that YouTube, Facebook, and the like might not exist today were it not for 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

---

[1] Pub. L. No. 105-304, § 201, 112 Stat. 2877 (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, 1203-04 (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 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, 28 (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 ("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) (defining the substantive requirements for falling within one of the four the safe harbors).

[6] "As provided in subsection (*l*), 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." H.R. REP. NO. 105-796, at 73 (1998), *reprinted*

a safe harbor, a court could still find infringement, because the safe harbor merely limited the available remedies.[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, despite courts' opportunity to develop an independent case law of online copyright infringement, over the past twenty years 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 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 both unsurprising and 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. 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, creating new, unintended, and unwarranted forms of both copyright liability and copyright immunity. In short, convergence has led to conflation, and the result is a DMCA that may now be doing more harm than good.

---

in 1998 U.S.C.C.A.N. 639, 649.

[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").

This article proceeds as follows. In Part I, 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 II shows that over the next two decades, the case law's liability definitions converged with the DMCA's standards, leaving almost no daylight between the statute and the case law. Part III demonstrates that this convergence has decreased the upside of the DMCA safe harbors, increased the downside, and caused 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.

I. CREATION

A. Courts

Back in the early days of the Internet, long before Instagram and 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 subject to the limits of top-down curation. In contrast, Usenet was entirely user-generated. It was the first platform that really 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

[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 NETBOOK ch. 3 (1996), http://www.columbia.edu/~rh120/ch106.x03.

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

owned by Religious Technology Center, 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.

The precedents on this question were few. The previous year, in *Sega Enterprises Ltd. v. MAPHIA*, a judge in the same California district as *Netcom* had issued a preliminary injunction against the operator of an electronic bulletin board on which users had posted unlicensed copies of videogames.[14] 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 games.[15] In contrast, neither Klemesrud nor Netcom had any idea

---

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

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

[13] *Id.* at 1366.

[14] Sega Enterprises Ltd. v. MAPHIA, 857 F. Supp. 679 (N.D. Cal. 1994) (Wilken, J.). 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 (D. Colo. 1995); *see also Religious Tech. Ctr. v. Lerma*, 897 F. Supp. 260 (E.D. Va. 1995) (rejecting preliminary injunction against activist's posting of Scientology materials online).

[15] *Id.* at 683-84. The same was true of a post-*Netcom* case with facts and reasoning quite similar to *MAPHIA*: Sega Enterprises 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.

that Erlich had posted the Scientology material until RTC contacted them.[16]

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*.[17] 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.[18] 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. 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.[19]

In contrast, the *Netcom* court 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.[20] 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. Indeed,

---

913, 930 (2005) ("One infringes contributorily by intentionally inducing or encouraging direct infringement . . . .").

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

[17] Playboy Enterprises, Inc. v. Frena, 839 F. Supp. 1552 (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).

[18] *Frena*, 839 F. Supp. at 1554.

[19] *Id.* at 1559 (stating that "[i]t does not matter that Defendant Frena may have been unaware of the copyright infringement" and noting that intent and knowledge are relevant only to determining the proper remedy for infringement).

[20] *Netcom*, 907 F. Supp. at 1367.

within a few hours of Erlich's initial upload, copies of the Scientology materials had appeared on every Usenet server around the world.[21]

The question was whether Klemesrud and Netcom were liable for those additional unauthorized reproductions. 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.[22] 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. 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."[23] Neither party initiated the copying of the Scientology materials—that was Erlich's doing—and the propagation of copies into Usenet happened mechanically and indiscriminately once Erlich posted, without any further intervention by Klemesrud or Netcom.[24] Like *Frena*, the *Netcom* court acknowledged that copyright infringement is 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."[25] (As we will see, this volitional requirement would prove important later, when Congress took up the issue.)

---

[21] *Id.* at 1367-68.

[22] We focus here, as the *Netcom* court did, on liability for unauthorized reproduction of the Scientology materials, because it's 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 (definition of "copies"), § 106(1) (defining reproduction as the making of "copies"); *Netcom*, 907 F. Supp. at 1368-71, 1381-82 (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 section 106(3) and unauthorized public display right under section 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.

[23] *Netcom*, 907 F. Supp. at 1369.

[24] *Id.*

[25] *Id.* at 1370.

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.[26] The court held that providing the means by which Erlich's Usenet posts were copied and disseminated to the world constituted substantial participation.[27] 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).[28] 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.[29]

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.[30] RTC 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.[31] But the court found no direct financial benefit as a result of Erlich's postings—no causal connection between his infringement and Klemesrud's and Netcom's revenues.[32]

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.[33] The *Netcom* court also opined on secondary liability (which *Frena*

---

[26] *Id.* at 1373.
[27] *Id.* at 1375.
[28] *Id.* at 1374. This enabled the court to distinguish *Sega v. MAPHIA*, in which the defendant knew and even encouraged the uploaded of infringing content. *Id.* at 1371 & n.17.
[29] *Id.* at 1374-75 (Netcom), 1382 (Klemesrud).
[30] *Id.* at 1375.
[31] *Id.* at 1375-76 (Netcom), 1382 (Klemesrud).
[32] *Id.* at 1376-77 (Netcom), 1382 (Klemesrud). This too helped the court distinguish *Sega v. MAPHIA*, where the defendant's business model was built on soliciting uploads of videogames 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.
[33] As mentioned *supra* note 22, *Frena* based direct liability on the distribution and public display

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.[34]

The small scale of the infringements here make it easy to overlook the significance of the issue that these holdings addressed. In the 1990s, Internet connectivity was transforming from a niche market to a ubiquitous utility. A new generation of netizens 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.[35] 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 the users who used their platforms to violate copyright law. 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 had to guide us was two district court cases from opposite sides of the country, and opposite sides of the issue.

---

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*, *see Netcom*, 907 F. Supp. at 1370-72, but it did not seem to convince even itself, *id.* at 1372 (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 Netcom*, 907 F. Supp 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").

[34] The *Netcom* court also split with *Frena* in finding a triable fair use defense. *Compare Netcom*, 907 F. Supp. at 1380, *with Frena*, 839 F. Supp. at 1159. 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.

[35] *See, e.g.*, *Yahoo to Buy GeoCities for $3.9 Billion in Stock*, L.A. TIMES. 1999-01-29 (noting how Geocities was founded in November 1994).

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 proposition. 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 prevail, because who knew what the next court would do?[36] 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 in the end 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*,[37] whereas others favored *Frena*.[38]

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 (the IITF) just a few months before the *Frena* ruling.[39] Comprising representatives from various federal agencies, the IITF was responsible for developing a National Information Infrastructure, "a

[36] 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").

[37] *See, e.g.*, Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distributors, 983 F. Supp. 1167, 1178-79 (N.D. Ill. 1997).

[38] *See, e.g.*, Playboy Enterprises, 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." 168 F.3d at 486.

[39] The National Information Infrastructure: Agenda for Action, 58 Fed. Reg. 49025-01 (Sept. 21, 1993).

seamless web of communications networks, computers, databases, and consumer electronics" that would "change forever the way people live, work, and interact with each other."[40] 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.[41] The idea was to translate the Working Group's findings into federal legislation that would fulfill the need for national standards governing copyright online.

In July 1994, the Working Group released a preliminary draft report, commonly known as the Green Paper.[42] 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.[43] 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.[44] But by the time the Working Group issued its final report (the so-called White Paper), the uncertainty was gone. The report cited *Frena* and *MAPHIA* favorably[45] and firmly concluded that "the best policy is to hold the service provider liable" for its users' copyright infringement.[46] 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,"[47] excused only in the

---

[40] *Id.*

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

[42] 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].

[43] *See* JESSICA LITMAN, DIGITAL COPYRIGHT 91 (2001) (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 42, at 120-39.

[44] GREEN PAPER, *supra* note 42, at 40-42, 76; *see also supra* notes 22-32 and accompanying text (explaining direct and secondary liability issues), note 22 (explaining section 106 issues).

[45] WHITE PAPER, *supra* note 41, 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).

[46] *Id.* at 117.

[47] *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.").

vanishingly rare instance in which a user encrypted the content.[48]

The Clinton Administration then took the White Paper to Congress, expecting that its recommendations would quickly become federal legislation and thereby provide a much-needed national standard governing copyright online.[49] It turned out, however, that Internet service providers and others in the telecommunications industry were not going down without a fight. And just a few months after the White Paper was published, *Netcom* was decided, giving the opposition a blueprint for an approach very different from the White Paper's.[50] 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 Safe Harbors*

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,[51] 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.

We will begin with the third safe harbor, both because it deals with the scenario that *Netcom* and *Frena* presented and because it has proved to be the most consequential of the four. Found in 17 U.SC. § 512(c), this safe harbor

---

[48] WHITE PAPER, *supra* note 41, at 122 (allowing for possibility of exemption from liability "for an on-line service provider who unknowingly transmitted encrypted infringing material").

[49] 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* LITMAN, *supra* note 1, ch. 9. Indeed, her book is an excellent overview of many other aspects of copyright law's development at the end of the millennium.

[50] *Id.* at 127-28.

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

applies to "Information residing on systems or networks at direction of users"—what we will call System Storage.[52] In other words, this is the safe harbor that deals with the fact pattern in which a service provider 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, section 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."[53] To emphasize this choice of *Netcom* over *Frena*, a later subsection—section 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."[54] In essence, then, Congress adopted *Netcom*'s approach to direct infringement, requiring something more volitional on the service provider's part before contemplating 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 is party liable for another party's direct infringement, and it takes two forms: vicarious and contributory.[55] 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

[52] 17 U.S.C. § 512(c).
[53] *Id.* § 512(c)(1).
[54] *Id.* § 512(m)(1).
[55] *See supra* notes 26-32 and accompanying text.

the service provider has the right and ability to control such activity."[56] 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 fails to expeditiously remove them.[57] 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.[58]

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 mean contributory liability. The System Storage safe harbor therefore explains what sort of information such a notice would have to contain (e.g., identification of the infringed work, location of the allegedly infringing material, contact information), and to whom it would be sent. Indeed, the safe harbor required service providers to register an agent for receipt of any notices.[59]

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 the infringing material, it can do something about it—namely, stop hosting it. But as in *Netcom*, the burden was on the copyright owner to provide the specific information that alerted the provider to the ongoing infringement and gave it the information it needed to take it down.

Two of the three other safe harbors were modeled on System Storage and its

---

[56] 17 U.S.C. § 512(c)(1)(B).
[57] *Id.* § 512(c)(1)(A).
[58] *Netcom*, 907 F. Supp. at 1374-75 (Netcom), 1382 (Klemesrud). Of course, knowledge is only one of two elements of contributory infringement. The other element, substantial participation, was satisfied by Netcom's and Klemesrud's providing the digital networks that allowed Erlich to copy and disseminate the Scientology materials, *id.* at 1375, 1382, and section 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).
[59] 17 U.S.C. § 512(c)(2)-(3).

notice-and-takedown regime. The safe harbor in section 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 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.[60] 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.[61]

The safe harbor in section 512(d) likewise borrows from 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 find infringing material posted elsewhere.[62] (Think search engines, or websites with indexed links to infringing materials.) 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, thus creating the knowledge necessary for contributory liability to attach.[63]

The remaining safe harbor is unique. Found in section 512(a), it addresses liability for online service providers who engage in Transitory Communications—i.e., who simply act as conduits for the infringing transmissions of others.[64] Suppose that Netcom had not stored the infringing Scientology material itself, but had merely transmitted it from Erlich's computer

---

[60] *Id.* § 512(b).
[61] *Id.* § 512(b)(2)(E).
[62] *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").
[63] *Id.* § 512(d)(1)-(3).
[64] The term "conduit" is a common shorthand for the kind of conduct section 512(a) addresses. *See, e.g.*, 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., Subpoena Enf't Matter, 393 F.3d 771, 775 (8th Cir. 2005).

to some distant destination elsewhere in the Internet, through a process that Erlich initiated, and retained no lasting copy on its servers. Section 512(a) limits the liability for such conduct; all the service provider must do is demonstrate that it is indeed a mere conduit.[65]

Importantly, Transitory Communications is the only one of the four safe harbors that imposes no notice-and-takedown obligation on the service provider. The reason for this distinction should be clear. The other three safe harbors all deal with situations in which the provider is facilitating access to copyrighted material in an ongoing way, and can therefore do something once it knows about it (e.g., stop hosting the content, or caching it, or providing links to it). In contrast, when the provider is merely a conduit, its involvement with the material is so fleeting that a notice from a copyright owner could not realistically arrive in time to make a difference; the provider might later learn that it had aided in the transmission of infringing material, but that knowledge would come too late to help stop the transmission.

So there we have it: four carefully delineated categories of conduct in which online service providers could engage without fear of liability.[66] Three of the four deal with storage of third-party content, so they also provide for takedown of such content upon notice. The fourth does not. Together, these four safe harbors protect 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

---

[65] 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* § 512(a)(1)-(5). Whether this sort of fleeting transmission would lead to liability absent the safe harbor's protection was an open question over which there was some controversy at the time of the DMCA's passage, *see* LITMAN, *supra* note 2, at 91-96 (discussing whether transmission and storage of copyrighted material in temporary memory constituted infringement), but which since has largely been settled in favor of conduits, *see, e.g.*, Cartoon Network LP v. CSC Holdings, Inc., 536 F.3d 121, 127-29 (2d Cir. 2008) (finding no copyright infringement for temporary storage of copyrighted data in course of transmission).

[66] 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 section 512(j).

established safe harbors, the courts retained the power to define liability whenever the safe harbors didn't apply. Indeed, the statute itself explicitly recognized as much in section 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." 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).

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.[67] 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 section 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 section 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 section 512(j), essentially aimed at shutting down access to specific online material or denying access to specific infringing users.[68] The

[67] 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. Co. v. Tompkins, 304 U.S. 64, 78 (1938) ("There is no federal general common law."), and because "common-law copyright" sometimes refers to the (mostly moribund) state copyright systems, *see, e.g.*, Zvi S. Rosen, *Common-Law Copyright*, 85 U. CIN. L. REV. 1055 (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 Netcom*, 907 F. Supp. at 1373 (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, 719 (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."). Such standards are essentially common law.

[68] *See* 17 U.S.C. § 512(j).

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 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.[69]

The other feature that complicates the DMCA's protection is that in order to qualify for any of the safe harbors, a service provider has to satisfy two threshold conditions.[70] The first requires the service provider to accommodate "standard technical measures,"[71] which refer to industry-wide technological standards designed to protect copyrighted works.[72] We can safely ignore this requirement, as no court has ever recognized the existence of such a measure in the twenty years since the DMCA was enacted.[73] The other threshold requirement, however, has proved to be more consequential: every service provider must adopt and reasonably implement a policy under which it terminates the accounts of any users who repeatedly infringe copyright.[74]

For present purposes, what these threshold requirements mean is that the DMCA limited liability only for those service providers that *both* engaged in the

---

[69] 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.

[70] 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 section 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). Second, as already mentioned, in order to use the System Storage safe harbor a service provider must register an agent with the U.S Copyright Office for receipt of notices from copyright owners. *Id.* § 512(c)(2), (d)(3). Agent registration is seemingly also required for the System Caching and Information Location safe harbors, both of which refer to section 512(c)'s notice-and-takedown system. (We say "seemingly" because those two safe harbors refer to agent *notification* in subsection (c)(3) but not agent *registration* in subsection (c)(2).) *See id.* § 512(b)(2)(E), (d)(3).

[71] *Id.* § 512(i)(1)(B).

[72] *Id.* § 512(i)(2).

[73] *See, e.g.*, Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1115 (9th Cir. 2007) (considering but ultimately remanding issue). One court 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).

[74] 17 U.S.C. § 512(i)(1)(A). Service providers must also ensure that their users are aware of the repeat-infringer policy. *Id.*

kinds of conduct covered by the safe harbors *and* also jumped through the regulatory hoops that the threshold requirements represent. That left 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. For example, 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 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 hand 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."

II. 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.[75]

The reality, however, is the statutory safe harbors exerted a gravitational pull on the common law. Before the DMCA, the common-law infringement standards diverged wildly.[76] After the DMCA, these varying holdings steadily converged toward a more uniform national standard, a standard whose borders look increasingly like the borders of the safe harbors themselves. This

[75] "As provided in subsection (*l*), 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." H.R. REP. NO. 105-796, at 73 (1998), *reprinted in* 1998 U.S.C.C.A.N. 639, 649.

[76] *Compare Netcom*, 907 F. Supp. at 1380, *with Frena*, 839 F. Supp. at 1159.

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 borders of liability, thereby ignoring the statute's invitation to order injunctive relief under section 512(j).[77] 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 twenty 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 III, 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.[78] To better understand these possibilities, consider the following matrix.

[77] 17 U.S.C. § 512(j).

[78] *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

Common-Law Liability Standards	DMCA Safe Harbor Standards: Δ's conduct falls within safe harbor	DMCA Safe Harbor Standards: Δ's conduct falls outside safe harbor
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 section 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 prevented it from escaping liability.[79] 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.[80] 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

[79] *Netcom*, 907 F. Supp. at 1375.
[80] *Frena*, 839 F. Supp. at 1159.

remedy would be a limited injunction under section 512(j); that's the point of the safe harbor.[81] Yet it is the existence of section 512(j) that actually proves that this sort of divergence is possible—that the DMCA contemplates such an outcome.

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, section 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 . . . ."[82] To be sure, even the *Netcom* ruling implies that liability would follow.[83] 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.[84] 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 ground 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 standards, we would see cases that belong in

---

[81] 17 U.S.C. § 512(j).
[82] *Id.* § 512(*l*).
[83] *Netcom*, 907 F. Supp. at 1380.
[84] *See* Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 800 (9th Cir. 2007) (implying that a company providing electricity to an infringer would not be contributorily liable even if done knowingly).

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. (Spoiler alert: they converge.)

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 particular 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 measures, even if the provider is engaging the very kind of automatic, indiscriminate data processing that the DMCA was designed to protect.[85] Unlike the four safe harbors, however, the threshold requirements are not related to any theory of liability; they are simply a regulatory price that providers must pay to get 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 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 section 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.[86]

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

[85] *See supra* notes 70-74 and accompanying text.

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

infringement.[87] As a matter of civil procedure, then, even when the DMCA safe harbors are in play, courts should decide infringement first.[88] 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,[89] 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.[90] 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 the plaintiffs' invitation to view them as one and the same.[91]

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 this opportunity 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 the standards for qualifying for a safe harbor. To establish convergence, we will examine the cases in the first category to see if the defendant's conduct also falls within a safe harbor, and we will examine the cases in the second category to see if it does not.

---

[87] *See* Lee, *supra* note 4, at 244 ("The DMCA safe harbors are affirmative defenses that the defendant must prove . . . .").
[88] *See Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 94 (2d. Cir. 2016) ("A service provider's entitlement to the safe harbor is properly seen as an affirmative defense, and therefore must be raised by the defendant.").
[89] *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.").
[90] See MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12B.04[A][1][d] n.145 (2015).
[91] 239 F.3d 1004, 1025 (9th Cir. 2001).

1. *Findings of No Liability*

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

a. 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 "it does not matter that Defendant Frena may have been unaware of the copyright infringement."[92] The *Netcom* district court came to the opposite conclusion, concluding that automated copying that occurs as a result of standard Internet operations cannot form the basis of a direct infringement liability, due to lack of volition.[93] 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 such automated copying.[94] 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*.[95] As with many early service provider cases, *ALS Scan* involves Usenet and the unauthorized hosting of copyrighted material—here ALS's photographs of female models—by a service provider, RemarQ.[96] RemarQ did not choose the photos at issue, and all of RemarQ's copying was an automatic, inherent function of hosting Usenet newsgroups.[97] In analyzing whether this copying rendered RemarQ directly liable, the court found that the liability analysis and the DMCA safe harbor defense analysis were one

[92] 839 F. Supp. at 1554.
[93] 907 F. Supp. at 1365.
[94] R. Anthony Reese, *The Relationship Between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability*, 32 Colum. J.L. & Arts 427, 438 (2009).
[95] *ALS Scan, Inc. v. RemarQ Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001).
[96] *Id.* at 620-21.
[97] *Id.*

and the same.[98] 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. Accordingly, . . . direct infringement claims [are] controlled by the DMCA."[99] 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.[100] Even Westlaw appears to have accepted this view, using this analysis in *ALS Scan* to conclude that *Frena* is "superseded by statute"—that statute being the DMCA.[101]

The Fourth Circuit went on to completely import the DMCA safe harbors into the direct infringement liability standard in *CoStar Group v. Loopnet*.[102] Like *ALS Scan*, the *CoStar* case presented the typical System Storage scenario—with LoopNet, the service provider, operating a server onto which its users copied CoStar's copyrighted photographs without a license.[103] The twist here was that LoopNet had not met the threshold conditions for the DMCA safe harbor, making this a case purely about the ultimate liability standards.[104]

Because the DMCA was unavailable to LoopNet, CoStar argued that *Netcom* should also be unavailable. In other words, it asserted that Congress intended for the statute "supplanted and preempted *Netcom*," making the safe harbors the sole determinant of liability and thus finding infringement whenever they did not apply.[105] The Fourth Circuit rejected this claim, embraced *Netcom* as the governing standard, and held that "the automatic copying, storage, and transmission of copyrighted materials, when instigated by others, does not render an ISP strictly liable for copyright infringement."[106] The substance of the safe

---

[98] *Id.* at 622-24.

[99] *Id.* at 621-22 (citing H.R. REP. NO. 105-551(I), at 11 (1998).).

[100] *Id.* ("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.").

[101] *See* Keycite for *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993).

[102] *CoStar Group, Inc. v. Loopnet, Inc*., 373 F.3d 544 (4th Cir. 2004).

[103] *Id.* at 546-57.

[104] *Id.* at 548 (CoStar argued that "[b]ecause LoopNet 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."). It was not clear why LoopNet had not satisfied the threshold requirements, or indeed whether the court was merely assuming *arguendo* that such was the case.

[105] Id. at 552-53.

[106] *Id.* at 554. 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

harbors and the direct infringement liability standard were therefore viewed as identical, even when the DMCA defenses were technically unavailable.[107] As Tony Reese observed, under *CoStar* service providers "do not need a safe harbor's protection in order to avoid direct infringement liability."[108] This is textbook convergence.[109]

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 a license.[110] The defendant's conduct was within the System Storage safe harbor, except it had failed to designate an agent for receipt of takedown notices, making the statutory defense unavailable.[111] 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: "every circuit to address this issue has adopted some version of *Netcom*'s reasoning and the volitional-conduct requirement" for determining direct liability.[112] The court also dismissed the argument that without protection from the DMCA, the service provider had to be liable.[113] The court concluded, like the Fourth Circuit in *CoStar*, that even though a service provider does not

provides explicitly that the DMCA is not exclusive." *Id.* (citing 15 U.S.C. 512(*l*)). For our explanation of section 512(*l*), *see supra* notes 82-84 and accompanying text.

[107] *Id.*

[108] Reese, *supra* note 94, at 438.

[109] *CoStar*, 373 F.3d at 555. In contrast to *CoStar*, the Ninth Circuit in *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004), thought it was still an open question was whether this DMCA-view of direct infringement still controls when the DMCA safe harbors are not available. 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.* at 1077. 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. 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. 105-190, at 19). 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.*

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

[111] *Id.* at 443.

[112] *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).)

[113] *Id.* at 443. The defendant had "never designated an agent," and thus did not meet the DMCA threshold requirements for immunity. *Id.*

qualify for the safe harbors, the volitional-conduct requirement still applied.[114] 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.[115] To succeed on a direct infringement claim, the plaintiff must assert "volitional conduct on the part of [the provider]."[116] 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."[117] 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.

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

Recall that contributory infringement requires both knowledge of and

---

[114] *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.* 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.

[115] *Parker v. Google, Inc*., 242 Fed. Appx. 833, 836 (3d Cir. 2007).

[116] *Id.*

[117] *Parker v. Paypal*, 2017 WL 3508759, *5 (E.D. Penn. Aug. 16, 2017).

substantial participation in an act of direct infringement.[118] 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.[119] Nor was there always a specific knowledge requirement. That is, general knowledge that infringing activity was occurring would satisfy this prong of contributory infringement.[120]

In contrast, the DMCA is more forgiving. It excludes a service provider from the Act's coverage only if the provider has acquired more specific knowledge of infringement. The most direct articulation of this heightened knowledge standard is in section 512(c)(1)(A), which sets forth what level of knowledge will exclude the service provider from the System Storage safe harbor's protection.[121] 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 fail to "act[] expeditiously to remove, or disable access to, the material."[122] 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.[123] 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 perjury—that these allegations are

---

[118] *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").

[119] *See, e.g.*, 2 PAUL GOLDSTEIN, GOLDSTEIN ON COPYRIGHT § 8.1, at 8:9 n.1 (3d ed. 2008) ("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.").

[120] *Id.*

[121] 17 U.S.C. § 512(c)(1)(A).

[122] *Id.*

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

true.[124] And this information must be sent directly to a "designated agent" that the service provider tasks with gathering this information.[125] 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.[126]

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 section 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 with the Ninth Circuit's decision in *Perfect 10 v. Amazon*, where the court vacated a finding of secondary liability under facts that would also qualify the service provider for System Storage safe harbor.[127] The court considered, in part, the secondary liability of Amazon for hosting an alleged direct infringer's copies of Perfect 10's photographs.[128] 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."[129] Such a standard aligned the common-law with

---

[124] § 512(c)(1)(A).
[125] *Id.*
[126] *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").
[127] *Perfect 10, Inc. v. Amazon, Inc*., 503 F.3d 1146 (9th Cir. 2007).
[128] *Id.* at 1156-57.
[129] *Id.* at 1172 (quoting *Napster*, 239 F.3d at 1022, and *Netcom*, 907 F. Supp. at 1375). 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

the statute, departing from the earlier case law in favor of a standard that mimics the DMCA requirement that a service provider act only when it has specific knowledge of the infringing material. 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. 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 the convergence in the contributory infringement context.[130] 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.[131] Just as other courts after the DMCA articulated, mere "conclusory allegations" of infringement are not enough—contributory infringement requires specific knowledge.[132] The convergence here is fairly explicit and congruent, with the court using the DMCA notice-and-takedown requirements to evaluate whether the copyright owner provided the wireless carriers with the requisite knowledge to establish secondary liability. The court explained that the copyright holder's notice (a 150-page-long list of titles) does "not identify which of these titles were infringed, who infringed them, and when the infringement occurred."[133] And although the issue was common-law liability, the court pointed out that these notices did not comply with the requirements of the DMCA.[134] The court explained that the DMCA, "by which the notices purport to be governed, clearly precludes notices as vague as the notices here.[135] In short, the court found no secondary liability for the very same legal and factual reason that the wireless carriers would have fallen under the DMCA: the lack of adequate and statutorily compliant takedown notices.

---

provided by title II of the DMCA." *Id.* at 1172-73.

[130] *Luvdarts, LLC v. AT&T Mobility, LLC*, 710 F.3d 1068, 1072-73 (9th Cir. 2013).

[131] *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.

[132] *Id.*

[133] *Id.* at 1072-73.

[134] *Id.* at 1073 (explaining that "[t]hese notices do not identify which of these titles were infringed, who infringed them, or when the infringement occurred.").

[135] *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'").

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., Box D in our framework. The cases under this scenario is not as numerous as under the first, but it still exhibits convergence. Put simply, there is no reported case where the court found safe harbor immunity after deciding the accused is a copyright infringer. 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.[136] A&M argued that "Napster's potential liability for contributory and vicarious infringement renders the Digital Millennium Copyright Act inapplicable per se."[137] 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 safe haven under the DMCA.[138] The Ninth Circuit resisted making such a "blanket conclusion," particularly at a preliminary stage of the litigation.[139] 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.[140] 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

[136] *A&M Records, Inc. v. Napster, Inc*., 239 F.3d 1004 (9th Cir. 2001).
[137] *Id.* at 1025.
[138] *Id.* The argument was also based on an interpretation that the plain language of 512(c)—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.") The court concluded that Napster "has failed to persuade this court that subsection 512(d) shelters contributory infringers." *Id.*
[139] *Id.* (citing S. REP. 105-190, at 40 (1998)).
[140] *Id.* (noting that some of these were procedural).

ten years later, in *Columbia Pictures v. Fung*.[141] The district court found secondary liability by inducement because the defendant invited users to download copyrighted movies from his company's websites.[142] 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.[143] In other words, a DMCA analysis was unnecessary because such the result was a foregone conclusion under the facts that lead to the inducement finding.[144] 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.[145]

On appeal, the Ninth Circuit was more cautious, citing *A&M Records* and concluding, "We think it best to conduct the two inquiries independently." 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."[146] Again, the court was not willing to reach the blanket conclusion that there was complete convergence between finding liability and denying DMCA immunity; it noted that "[i]t is . . . *conceivable* that a service provider liable for inducement could be entitled to protection under the safe harbors."[147] But it recognized that the common-law liability analysis, which occurs first, produces findings that are highly relevant to the DMCA inquiry.[148]

Other courts, while not considering the convergence question so expressly, have found liability and then used much of the same analysis to deny DMCA safe

---

[141] *Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020 (9th Cir. 2013).
[142] *Id.* at 1031.
[143] *Id.* at 1039-40 ("Columbia argues, and the district court agreed, that inducement liability is inherently incompatible with protection under the DMCA safe harbors.").
[144] *Id.*
[145] *Id.*
[146] *Id.* at 1040 ("[I]f Congress had intended § 512(c)(1)(B) to be coextensive with vicarious liability, 'the statute could have accomplished that result in a more direct manner.' ") (quoting *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 667 F.3d 1022, 1045 (9th Cir.2011)).
[147] *Id.* (emphasis original). 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.*
[148] "[A]lthough, as will appear, 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." *Id.*

harbor protection. The court in *Goldstein v. Metropolitan Regional Information Systems* provides an example.[149] 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. (This was yet another System Storage case, in which unauthorized, uploaded photographs "contain[ed] copyright notices within them," making "it is difficult to argue that a defendant did not know that the works were copyrighted."[150]) Citing *Netcom*, the court concluded that the defendant "knew or had reason to know that the use of the [photographs] on the [] site was in violation of that copyright."[151] Accordingly, the copyright holder properly pleaded contributory infringement.[152]

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 under the DMCA safe harbors.[153] The court explained that while the DMCA safe harbors are a defense, the facts relevant to contributory liability's knowledge requirement also negate the defense's availability.[154] 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 defendant had sufficient actual knowledge to exclude it from the protection of the safe harbors.[155] Here we 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 later 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*,[156] from the same district as the hoary *Frena* case. The allegation was that copyrighted fashion photographs appeared on the defendant's website without the copyright holder's permission.[157] The copyright owner failed to provide specific notice of the URL addresses of the 17,035 copyrighted images

[149] *Goldstein v. Metro. Reg. Info. Sys., Inc*., 2016 WL 4257457 (D. Md. Aug. 11, 2016).
[150] *Id.* at *4-5.
[151] *Id.* (citing *Netcom*, 907 F. Supp. at 1374).
[152] *Id.*
[153] *Id.* at *6-*7.
[154] *Id.*
[155] *Id.* at *7.
[156] Venus Fashions, Inc. v. ContextLogic, Inc., 2017 WL 2901695 (M.D. Fla. Jan. 17, 2017).
[157] *Id.* at *6-*7.

on the site.[158] The court nevertheless found that the defendant had "reason to know" that the images were copyrighted and infringing.[159]

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."[160] Here the court borrowed this standard from the safe harbors and relied on it when determining secondary liability under the common law.[161] 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."[162] The court even cites *Netcom* to support this analysis.[163] We therefore 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.

---

[158] *Id.* at *23.

[159] *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.").

[160] *Viacom Int'l, Inc. v YouTube, Inc*., 676 F.3d 19, 41 (2d Cir. 2012) (detailing the "red flags" analysis under the DMCA safe harbors).

[161] *Venus Fashion*, at *23, n.15.

[162] *Id.* (citing *UMG Recordings*, 718 F.3d at 1125-26; 17 U.S.C. § 512(c)(1)(A)(ii)).

[163] *Id.* ("Also instructive is the relatively early and influential decision in Religious Tech. Ctr. v. Netcom On Line Commc'n Servs., Inc., 907 F. Supp. 1361 (N.D. Cal. 1995) ("Netcom")"). The court also relies upon *Perfect 10* and *Luvdarts*, both cases explored above that evidence convergence between the common-law standard for secondary liability and the DMCA. *Id.*

Table 2: Con/Divergence Case Law

Common-Law Liability Standards	DMCA Safe Harbor Standards: Δ's conduct falls within safe harbor	DMCA Safe Harbor Standards: Δ's conduct falls outside safe harbor
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 the safe harbor (Box C). That's because our research revealed no such cases. Divergence simply did not occur, notwithstanding the freedom courts had in the wake of the DMCA's passage to craft whatever liability standards they saw fit.

III. 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 had 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 would 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 convergence has led to conflation as courts have begun to use ancillary DMCA provisions 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 empirical data that 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 I, 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 see a court from the same district as *Frena* deciding an online infringement case without even citing that once-leading precedent.[164] This means that a service provider can enjoy the benefit of the safe harbors without actually invoking them. Convergence has made the benefits of dealing with the DMCA essentially evanescent.

---

[164] *See Venus Fashions*, 2017 WL 2901695 (not even citing *Frena* once). 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).

B. Conflationary Costs

More significant, however, are the changed in the costs to service providers of complying with the DMCA. Some of these costs have been present since 1998, such as the cost of implementing a system of 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.[165]

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 liability 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 have come with it.

1. *BMG v. Cox: New Liability*

No case better exemplifies the transition from helpful convergence to harmful conflation than 2018's *BMG Rights Management v. Cox Communications*.[166] BMG claimed that its investigating agent, Rightcorp Inc., had observed more than two millions 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,

[165] *See, e.g.*, Jennifer M. Urban et al, *Takedown in Two Worlds: An Empirical Analysis*, 64 J. COPYRIGHT SOC'Y 483 (2018); Electronic Frontier Foundation, Takedown Hall of Shame, https://www.eff.org/takedowns (last visited Aug. 15, 2018).

[166] The full case caption is *BMG Rights Management (US) LLC v. Cox Communications, Inc.*, and we will be referring to three different opinions in the case: the district court's summary judgment ruling (149 F. Supp. 3d 634 (E.D. Va. 2015) ("*Cox SJ*")), the district court's disposition on post-trial motions (199 F. Supp. 3d 958 (E.D. Va. 2016) ("*Cox Post-Trial*")), and the Fourth Circuit's decision on appeal (881 F.3d 293 (4th Cir. 2018) ("*Cox Appeal*")).

store copyright-infringing material on its own computer servers, or control what its subscribers store on their personal computers.

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*)[167] 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*.[168] Even *Frena*, the case most unfriendly to service providers, had involved a service provider that hosted infringing material for others to download, rather than merely providing Internet connectivity.[169]

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 section 512(a). It satisfied all five statutory conditions necessary to qualify for the safe harbor's protection. First, Cox's subscribers initiated each transmission.[170] Second, Cox automatically and indiscriminately transmitted the material.[171] Third, the subscriber chose the destination, not Cox.[172] Fourth, Cox made no lasting copy of the material.[173] Finally, the material was not modified along the way.[174]

Conspicuously absent from those conditions is any notice-and-takedown requirement. As mentioned above, Transitory Communications is unique in that respect; the other three safe harbors all require takedown upon receipt of a compliant notice.[175] The reason for this distinction is clear: if the service provider is merely acting as a conduit, there is nothing to take down. In theory, a notice

---

[167] *See supra* notes 95-101 and accompanying text.
[168] *See supra* notes 149-155 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* at 676, (calling the evidence "hardly overwhelming"), and the jury ultimately rejected it, *Cox Post-Trial*, 199 F. Supp. 3d at 963.
[169] 839 F. Supp. at 1554.
[170] 17 U.S.C. § 512(a)(1).
[171] *Id.* § 512(a)(2).
[172] *Id.* § 512(a)(3).
[173] *Id.* § 512(a)(4).
[174] *Id.* § 512(a)(5).
[175] *See supra* notes 64-66 and accompanying text.

could arrive while a transmission was going on, and the service provider could terminate it midstream. But in practice, that would never happen; the timing is such that any notice would occur after the fact, when the infringement was complete. In order to stop the latter kinds of transmission, it would have to know about them in real time. Once the transmission ended, the conduit's ability to do anything about the act of infringement ended as well, as did its role in providing access to the copyright material.

Congress presumably knew all this, in that it gave conduits protection under section 512(a) regardless of whether they receive notices from copyright owners. In contrast, providers who host infringing material were participating in an ongoing way, such that a notice could prompt a meaningful intervention. Thus section 512(c) has a notice-and-takedown system. The same goes for caching infringing material under section 512(b) or providing links to infringing material under section 512(d), which is why those safe harbors too require takedown upon notice.

If the Transitory Communications safe harbor applies, however, why is *BMG v. Cox* a case of conflation, rather than an example of the DMCA working exactly as intended? Well, recall that in order for any safe harbor to apply, the service provider must satisfy certain threshold requirements, including the requirement that it reasonably implement a policy of terminating repeat infringers.[176] And here the evidence against Cox was damning; the company had such a policy, but it did all it could to avoid implementing it.[177] Setting aside the many notices Cox received from copyright owners alleging infringement by its subscribers (more on them in a moment), Cox hesitated to terminate those subscribers who its own employees learned were repeatedly infringing, and even when it did terminate it often reactivated subscribers right away.[178] The court accordingly ruled that Cox had "failed to implement its policy in any consistent or meaningful way—leaving it essentially with no policy."[179] 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 repeat-infringer policy rendered the entire DMCA a non-factor, and the court would determine liability under the common law only.

---

[176] *See supra* notes 76-80 and accompanying text.
[177] *Cox Appeal*, 881 F.3d at 303-05.
[178] *Id.* at 304.
[179] *Id.* at 305.

What we learned in Part II, however, is that this should have made no difference in the ultimate outcome. Convergence means that the standards for qualifying for a safe harbor are essentially the same as the standards for avoiding common-law liability. And there was no question that Cox qualified for the safe harbor; it was unquestionably a conduit, exactly as section 512(a) contemplated. Only a threshold requirement stood in the way of Cox's DMCA defense, and such requirements had never played any role in the ultimate liability determination. Indeed, no court had ever held a service provider liable for acting purely as a conduit. The conduit's 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, the service provider would no longer be participating in any infringement or facilitating access to the material at issue. (This lack of liability is exactly as one would expect from a world in which the common-law infringement standards had converged with the safe harbor standards.)

Nevertheless, the specter of the DMCA—and Cox's inability to use it as a defense—haunted *BMG v. Cox*. The statute should have been irrelevant once it was clear that Cox had not met its threshold requirements, but instead it reared its head again and again. To establish the knowledge element of contributory liability, BMG cited the many notices sent to Cox, notices which provided the IP addresses of users whom Rightscorp had allegedly seen offering copyrighted material for download.[180] The district court agreed, stating that because the notices were "DMCA-compliant," they constituted "powerful evidence of a service provider's knowledge."[181] Yet not only was the court invoking a statute that it had ruled irrelevant, but it was invoking it inaccurately. There is no such thing as a "DMCA-compliant" notice for conduits, because the DMCA imposes no notice-and-takedown regime on conduits.

In contrast, if Cox had been hosting infringing material itself, its receipt of DMCA notices would have been relevant to its ultimate liability. As we have already seen, common-law liability for hosting has converged with the System Storage safe harbor in section 512(c), and rightly so. It is no surprise, then, that every single case *BMG v. Cox* cited in support of the notion that notices could

[180] *Cox SJ*, 149 F. Supp. 3d at 671; *Cox Post-Trial*, 199 F. Supp. 3d at 976; *Cox Appeal*, 881 F.3d at 312.

[181] *Cox SJ*, 149 F. Supp. 3d at 662. 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 of the DMCA notices, which the appeals court acknowledged as the "primary theory" for Cox's liability. *Cox Appeal*, 881 F.3d at 312.

create culpable knowledge involved a service provider that was hosting material, not merely transmitting it.[182]

One might ask why evidence sufficient to establish knowledge on the part of a hosting service provider would not also suffice for a conduit. After all, in both instances a copyright owner is telling a service provider about alleged infringement committed by its users. The answer lies in the safeguards that keep the copyright owner honest. For example, under the three safe harbors that include notice-and-takedown the copyright owner must vouch for each notice's bonafides, under penalty of perjury,[183] and civil liability exists for material misrepresentation in notices.[184] In addition, service providers can create a counter-notification system through which a user can contest the infringement allegation and have the takedown reversed.[185] In contrast, a notice to a conduit is not a DMCA notice at all, and is therefore not subject to these statutory safeguards.

The most important safeguard, however, is that when the service provider is hosting material subject to a takedown notice, it can examine the material and verify that it appears to be infringing. After all, the material is on its own network.[186] In the absence of this safeguard, the provider has no choice but to

---

[182] The summary judgment ruling cited *Capitol Records, LLC v. Escape Media Group., Inc.*, No. 12-CV-6646 AJN, 2015 WL 1402049 (S.D.N.Y. Mar. 25, 2015) (music streaming), *Perfect 10, Inc. v. Giganews, Inc.*, No. CV 11-07098, 2014 WL 8628031 (C.D. Cal. Nov. 14, 2014) (Usenet hosting), *Corbis Corp. v. Amazon.com, Inc.*, 351 F. Supp. 2d 1090 (W.D. Wash. 2004) (photos on websites), and *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004). *See* Cox SJ, 149 F. Supp. 3d at 671-72. The ruling on post-trial motions added *Netcom*, 907 F. Supp. 1361, *Capitol Records, Inc. v. MP3tunes, LLC*, 821 F. Supp. 2d 627 (S.D.N.Y. 2011) (music storage), *Arista Records LLC v. Usenet.com, Inc.*, 633 F.Supp.2d 124 (S.D.N.Y. 2009) (Usenet hosting), and *CoStar Group Inc. v. LoopNet, Inc.*, 164 F.Supp.2d 688, 706 (D. Md. 2001) (photos on website). *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 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. For procedural reasons, the court declined to rule on whether section 512(c) also applied. *Id.* at 1081 & n.12.

[183] 17 U.S.C. § 512(c)(3)(A)(vi). Note that the notices in *BMG v. Cox* were apparently submitted under penalty of perjury. *Cox Appeal*, 881 F.3d at 299.

[184] 17 U.S.C. § 512(f).

[185] *Id.* § 512(g).

[186] 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 examination.

accept the copyright owner's self-interested allegation at face value. This is why it is so odd that the court in *BMG v. Cox* characterized BMG's notices as "DMCA-compliant"; to comply with the DMCA, a notice must include "information reasonably sufficient to permit the service provider to locate the material."[187] With the information in the notice, Cox could not locate any of the allegedly infringing material. It could only locate the allegedly infringing subscriber. Identifying such subscribers was relevant to the repeat-infringer policy issue, and therefore to whether the DMCA was an available defense. But to focus on repeat infringement once the DMCA is rendered irrelevant is to conflate a statutory defense with a common-law liability standard.

BMG v. Cox has accordingly occasioned a subtle but significant shift from focusing on control of the infringe*ment* to control of the infring*er*. Giving a copyright owner the power to compel service providers to block access to its copyrighted material is one thing. Giving a copyright owner the power to compel service providers to deny Internet access to actual people is another—especially when it's too late to stop the alleged infringement, and the only evidence that it ever occurred is the copyright owner's say-so.[188] And the basis for this shift is conflation: the court conflated a statutory threshold requirement with common-law liability standard, and it conflated the three safe harbors that require notice-and-takedown with the one, more relevant safe harbor that does not.

This is not to say that we should shed tears for Cox Communications, whose internal documents demonstrated a contempt for copyright law.[189] But 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.

---

[187] 17 U.S.C. § 512(c)(3)(A)(iii). A similar provision exists as part of the Information Location safe harbor's notice-and-takedown system. *See id.* § 512(d)(3).

[188] Note that the court rejected the only way in which the infringement could be considered ongoing: that subscribers' mere offering of BitTorrent files was itself an infringing distribution. *Cox SJ*, 149 F. Supp. 3d at 666.

[189] *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.

Even the district court seemed to realize the difficulty its ruling presented. After allowing the case to go to a jury, which found willful contributory infringement and returned a verdict of $25 million against Cox,[190] 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?[191]

These questions are, as the court said, "well-founded."[192] 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 it notices? The Fourth Circuit was similarly uncomfortable with BMG's theory, remanding for a new trial under a standard of actual knowledge of specific infringement.[193]

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 enough allegations of infringement (infringement from the past, mind you, about which nothing can

---

[190] *Cox Post-Trial*, 199 F. Supp. 3d at 963.
[191] *Id.* at 995.
[192] *Id.*
[193] *Cox Appeal*, 881 F.3d at 307-312.

now be done) and demanding the termination of the targeted subscribers' accounts. This goes well beyond any theory of liability 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 divergence, 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 mashed together with the notice-and-takedown scheme from an irrelevant and inapplicable safe harbor, emerging from the oven as a new liability standard. Convergence has become conflation.

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*.[194] Joshua Lange is the owner and sole employee of Internet site Motherless.com, the content of which is stored on servers that Lange owns and maintains.[195] The site contains over 12.6 million mostly pornographic pictures and video clips.[196] The content is uploaded by the site's users, and the uploaders may or may not have created the material.[197]

Lange actively screened much of the material posted on the site, removing any child pornography, bestiality, and copyright infringement that he spotted.[198] He screened out child pornography because it is prohibited by law, and he screened out bestiality because some European countries also prohibit bestiality pornography (and because some of Lange's European advertisers voiced concerns about this content).[199]

Traditionally, such screening is relevant to many secondary liability theories.

---

[194] *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597 (9th Cir. 2018).
[195] *Id.* at 601.
[196] *Id.*
[197] *Id.* at 601-02.
[198] *Id.* at 601-02. 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.
[199] *Id.* "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.

Most directly, screening is evidence of the right and ability to control, one of the two elements of vicarious infringement.[200] 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.[201]

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.[202] 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.[203] 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.[204]

So far, so good. But then, in response, Lange cited section 512(m) of the DMCA.[205] 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

---

[200] *See, e.g.*, *Fono*visa, 76 F.3d at 262-63 (noting that defendant "controlled and patrolled" the premises); *see also Mavrix Photographs, LLC v. LiveJournal, Inc.*, 873 F.3d 1045, 1058 (9th Cir. 2017) (quoting *UMG Recordings, Inc. v. Shelter Capital Partners, LLC*, 718 F.3d 1006, 1030 (9th Cir. 2013)).

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

[202] 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.").

[203] *Id.* at 604 (quoting 17 U.S.C. § 512(c)(1)).

[204] *Id.* (citing 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* Parts II.C.1.a.-b.

[205] *Id.* (citing 17 U.S.C. § 512(m)).

> extent consistent with a standard technical measure complying with the provisions of subsection (i); or
> (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.[206]

Lange's argument was that this provision means that the act of screening can never deprive a service provider of DMCA safe harbor protection.[207]

Surprisingly, the Ninth Circuit agreed with Lange.[208] 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."[209] The court "read section 512(m) to say that Congress expressly provided that such screening does not deprive a website of safe harbor protection."[210] Thus, the act of screening could not be used to deny Lange of DMCA safe harbor protection, and, in turn, copyright infringement immunity.

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 section 230 of the Communications Decency Act.[211] But the DMCA is not one of them; section 512(m) merely removes screening as a condition for accessing the safe harbors, without changing their substance.

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

---

[206] 17 U.S.C. § 512(m).
[207] *Ventura*, 885 F.3d at 605.
[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] 47 U.S.C. § 230(c) (immunizing online platforms that block or screen offensive material from liability as publisher or speaker).

liability where it might otherwise be found.

This again is an act of conflation. Section 512(m) was never meant to create a new zone of non-liability—i.e., immunity for screening by service providers—yet in *Ventura* it does. This is likely the result of further reliance on the DMCA to shape the general scope of copyright liability for service providers, as seen in Part II 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

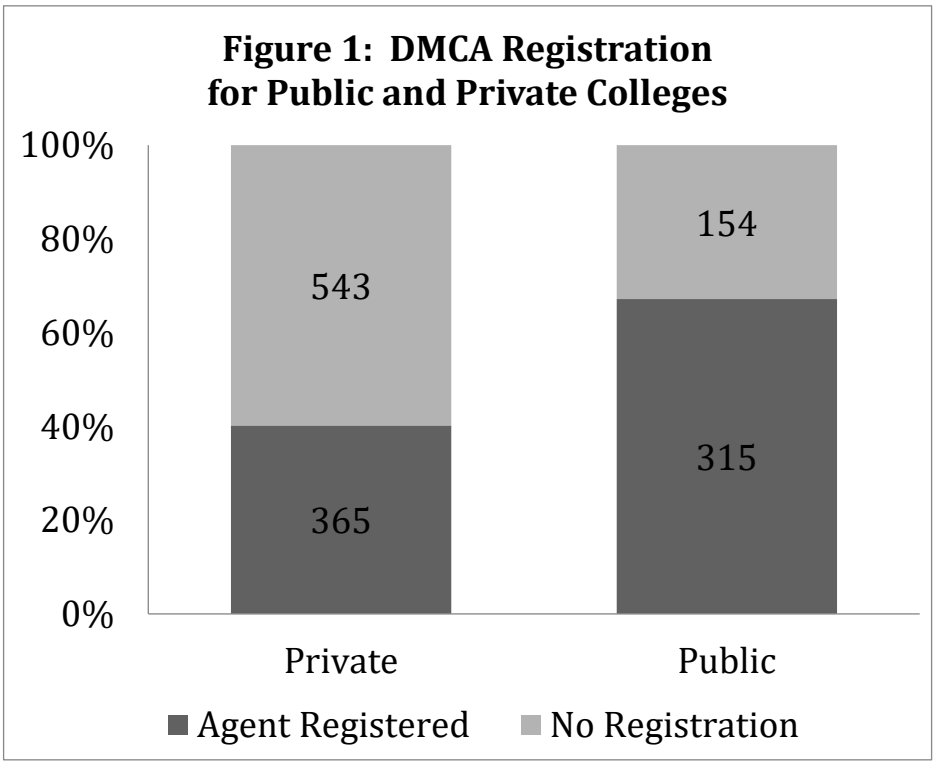
It's no coincidence that we see costly conflation only after convergence was basically complete. That's when the distinction between common-law liability and the safe harbor standards is most difficult to perceive, and where mixing and matching of statutory and common-law standards is most likely to happen. Still, *BMG v. Cox* and *Ventura Content v, Motherless* are only two cases. They may not be a harbinger 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,[212] but of particular importance to the current discussion are two results.

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.[213] What we found, however, is that despite the consequences of not having an agent, over half (50.6%) of all four-year

[212] *See* Christopher Cotropia & Jim Gibson, *Commentary to the U.S. Copyright Office Regarding the Section 512 Study: Higher Education and the DMCA Safe*, IHELG Monograph 17-04 (2016).
[213] *See supra* note 59 and accompanying text.

colleges and universities in the United States had not registered one, and the figure rose to 57.1% if we included those whose contact information was outdated. We considered whether this was because public universities enjoy sovereign immunity from copyright suits,[214] 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[215]—more than half of institutions do not think it worthwhile to comply with the regulations necessary to gain protection from 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 service providers can receive essentially the same protection from courts without the need to create

[214] *See* Coyle v. Univ. of Kentucky, 2 F. Supp. 3d 1014, 1017 (E.D. Ky. 2014).
[215] *See* Cotropia & Gibson, *supra* note 212, at 2-3.

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.[216] 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% answered yes, even though no takedown is necessary under that safe harbor.[217] In contrast, only 76.7% gave an affirmative answer when asked the same question about System Storage, and 62.2% about Information Location—both of which actually require notice-and-takedown to preserve the safe harbor defense.[218]

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.[219] Among the most likely, however, is that those service providers unsophisticated enough to register an agent in the first place apparently 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.[220] 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.

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

[216] The fourth safe harbor, System Caching, is generally not as important, and so for simplicity's sake we left it out.
[217] Note that we conducted the survey before the *BMG v. Cox* case.
[218] *See* Cotropia & Gibson, *supra* note 212, at 6.
[219] *See id.* at 17-19.
[220] *Id.* at 7.

economy would look very different, and not in a good way.

Today, however, we come not to praise the DMCA, but to bury it. The case law has caught up with the statute to the point where the two have converged, eliminating the unique benefit that the Act once conveyed. At the same time, the cost of complying with the DMCA 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. The wisest course for those who provide services online is to resist the Act's temptations and steer clear of its clutches altogether.