A Roadmap to Reform Section 512 of the Copyright Act

Kristian Stout
Geoffrey A. Manne

ICLE White Paper 2022-10-13

ICLE | 1104 NW 15th Avenue Suite 300 | Portland, OR 97209 | 503.770.0076
icle@laweconcenter.org | @laweconcenter | www.laweconcenter.org

Executive Summary

Section 512 of the Copyright Act, passed as part of the Digital Millennium Copyright Act of 1998, was created to preserve "strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment," while also providing "greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities." The idea was to provide a safe harbor to online service providers (OSPs) that would also help to fight piracy.

In practice, Section 512 has reduced OSPs' liability risk and thereby promoted the growth of distribution services. Piracy, however, has grown exponentially. Among the factors driving this growth is that the courts' interpretation of Section 512 has pushed OSPs toward a reactive "file-containment" approach, rather than encouraging them to seek proactive solutions to piracy on their services. Indeed, citing both technological change in the intervening years and the judicial construction of Section 512, the U.S. Copyright Office has concluded that "Congress' original intended balance has been tilted askew." It would therefore be appropriate for Congress to revisit the law, applying lessons learned over the more than two decades since its enactment.

Much of the challenge in combating online piracy stems from the "volume problem." The amount of content that traverses online services makes it unreasonable to expect OSPs to catch every intentional or inadvertent infringement by their users. But the amount of infringement that slips through and harms copyright holders is nonetheless substantial, accelerated by technological innovations like more comprehensive search engines, faster upload and download speeds, and the emergence of peer-to-peer file-sharing services.

One solution would be for OSPs to license content directly from rightsholders. As intermediaries, OSPs can potentially license content more efficiently and cost-effectively than individual copyright holders and users of Internet services could negotiate licenses among themselves. Licensing by OSPs could also remove litigation risk, enable their service's users to benefit from the content, and ensure copyright holders' rights are respected. TikTok, Facebook, Snapchat, Instagram, and YouTube, for example, are increasingly licensing at least some content, so that their users have an authorized way to incorporate that content into posts and streams.

Unfortunately, the current safe-harbor regime gives OSPs little incentive to license content or otherwise proactively deter pirated content on their services, insofar as they can presumptively monetize infringing content until rightsholders issue takedown notices. Under Section 512, to be protected by the safe harbors, OSPs must have neither "actual knowledge" of infringement, nor "red-flag knowledge"—*i.e.*, awareness of facts that make infringement apparent. Judicial interpretations of Section 512, however, have essentially collapsed the red-flag standard into the actual-knowledge standard, while progressively narrowing the scope of the actual-knowledge standard; the bar for legally relevant knowledge of infringing activity is now quite high.

To address this, the standard for when an OSP is considered to have "knowledge" of infringement ought to be changed from what an "ordinary" person might infer from the circumstances to what a reasonable person in the user-generated content business would infer, even absent notification by a rightsholder. This broader knowledge standard would then be used to condition the safe harbors offered by Section 512 on OSPs taking reasonable steps both to prevent infringement and to remove that infringing content that does slip through.

Even where OSPs do not host or display infringing content, they may sometimes facilitate its dissemination by others. To be eligible for the safe harbors, OSPs should be obligated to provide the identity of infringing parties and to prevent further access to the infringing content, even when the OSPs are not at fault for the underlying infringement. Around the world, these sorts of "no-fault injunctions" have been used effectively to combat piracy with no interference with OSPs' normal operations. Indeed, in some cases, private companies have voluntarily partnered with rightsholders to restrict access to content that a court has declared infringing.

Congress originally expected OSPs to collaborate with rightsholders in the development of standard technical anti-piracy measures, such as filtering. In the nearly quarter century since Section 512's enactment, however, no standard technical measures have emerged. Recently proposed legislation—the SMART Copyright Act—endeavors to fix this problem. It would empower the Office of the Librarian of Congress to engage in rulemaking proceedings to develop standard technical measures with the relevant multistakeholder community. Despite some ambiguities and shortcomings in the bill's text, it offers a promising framework to address one of Section 512's longstanding deficiencies.

Finally, Section 512 requires OSPs to have policies to terminate service to repeat infringers and to reasonably implement those policies. Courts, however, have interpreted these requirements loosely. The purpose of the safe harbors is to provide platforms greater certainty regarding litigation risk when they act responsibly and to assure copyright holders that their rights will be reasonably protected in exchange for the liability limitations the platforms receive. That bargain is not achieved unless the platforms and their users know that costly repeat infringement will not be tolerated. To better address this goal, the Copyright Office should be authorized to provide guidance on the minimum requirements necessary to meet the repeat-infringer policy obligation, including by creating a model repeat-infringer policy that will be presumed to comply.

A Roadmap to Reform Section 512 of the Copyright Act

Kristian Stout & Geoffrey A. Manne*

Introduction

The birth of the commercial Internet was among the most important technological developments of the past century and crucial to its success have been the rules governing the Internet's use. These include architectural rules to address such issues as management of the Domain Name System (DNS) and the resolution of disputes over domain names. Other important rules concern the relationships between and among commercial entities and individuals operating online. They include such familiar legal rules as torts, copyright, and antitrust.

In certain respects, these rules of general applicability apply differently on the Internet than they do in other contexts, typically to address the scale, scope, and speed with which information can be shared online via intermediaries (*i.e.*, digital platforms). This leads to the general legal presumption that intermediary liability should be specially tailored online to ensure that business models that rely on user-generated content can thrive, while also suitably protecting broader social interests. Section 230 is one of the most well-known U.S. laws dealing with this subject, and it has received significant attention, aimed at understanding how best to frame policy around intermediary liability online. As we have noted in previous work on that subject, intermediary-liability laws should be focused on balancing the benefits that platforms can provide with the negative externalities they can generate.[1] Any legal policy that requires intermediaries to moderate more than they currently do *will* remove some harmless content; the relevant question, however, is whether the marginal reduction in harmless speech is justified by the marginal increase in the deterrence of illegal content. In essence, crafting intermediary-liability policy is about conducting a cost-benefit analysis that implicitly assumes that the goal is optimally to minimize both the loss of user-generated content and the harms of illegal activity facilitated by platforms.[2]

---

* Kristian Stout is director of innovation policy at the International Center for Law & Economics (ICLE). Geoffrey A. Manne is the president and founder of ICLE.

[1] Geoffrey A. Manne, Kristian Stout, & Ben Sperry, *Who Moderates the Moderators?: A Law & Economics Approach to Holding Online Platforms Accountable Without Destroying the Internet*, at 38-39, INTERNATIONAL CENTER FOR LAW & ECONOMICS, ICLE (2021), *available at* https://laweconcenter.org/resource/who-moderates-the-moderators-a-law-economics-approach-to-holding-online-platforms-accountable-without-destroying-the-internet.

[2] *Id.* at 27 ("The relevant questions [when considering intermediary liability rules] are: To what degree would shifting the legal rules governing platform liability increase litigation costs, increase moderation costs, constrain the provision of products and services, increase 'collateral censorship,' and impede startup formation and competition, all *relative to the status quo*, not to some imaginary ideal state? Assessing the marginal changes in all these aspects entails, first, determining how they are

Given the uncertainties and complexity in locating that middle ground between costs and benefits, erring on the side of granting full immunity from third-party liability to platforms—as Section 230 largely does—may conceivably be the best possible outcome. Without strong evidence to support this position, however, it is highly *improbable* that a legal regime that results in complete immunity for platform operators for the harmful activity that can occur on their services is socially optimal. This is particularly true, given the long history of common-law attempts to parse exactly this kind of liability for offline intermediaries, which suggests that courts and lawmakers can indeed shape regimes to allow both liability and room for firms to operate their services.[3]

In other words, simply claiming that costs would rise if intermediaries were held liable, or that liability itself is a harm to the platforms, is insufficient. Liability has some harmful consequences *everywhere*. The relevant question is whether those harms outweigh the ones avoided by *not* imposing legal accountability.

It is notable that copyright protection was specifically exempted from the liability shield created by Section 230.[4] It is also notable that the subject of this paper—Section 512 of the Copyright Act ("Section 512")—adopted, at least in theory, a different approach than Section 230. But as we discuss below, while Section 512 did not create a complete liability shield, its practical effect, largely through judicial interpretation, has come closer to that end than its drafters likely envisioned.

Section 512 altered key elements of how secondary-liability rules for copyright are applied online. Most notably, Section 512 created a safe harbor for online service providers ("OSPs") for potentially infringing content generated by users of their platforms.[5]

Nearly a quarter-century after its passage, Section 512 is due for reform. When Congress added Section 512 to the Copyright Act, it had two things in mind. First, that copyrighted content merited protection online, just as it did offline. Second, that the then-nascent OSPs would struggle to bear the full weight of direct or secondary liability for all the copyrighted content their users might disseminate without authorization. Thus, Congress intended Section 512 to preserve "strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment," while providing "greater certainty to

---

affected by the current regime. It then requires identifying both the direction and magnitude of change that would result from reform. Next, it requires evaluating the corresponding *benefits* that legal change would bring in increasing accountability for tortious or criminal conduct online. And finally, it necessitates hazarding a best guess of the *net* effect.").

[3] *Id.* at 139-95 and accompanying text.

[4] 47 U.S.C. § 230(c)(1)-(2).

[5] Congress added Section 512 to the Copyright Act through amendments adopted in Section 202 of the Digital Millennium Copyright Act of 1998. *See* Pub. L. No. 105-304, sec. 202, 112 Stat. 2860, 2877.

service providers concerning their legal exposure for infringements that may occur in the course of their activities."[6]

Given the monumental challenges that OSPs would face in trying to prevent any unauthorized dissemination of copyrighted content by their users, they particularly feared the precedent set by 1993's *Frena* decision, which imposed direct copyright liability on a bulletin-board operator for storing infringing images uploaded by users.[7] To address the perceived threat to OSP viability if *Frena* were broadly followed, Section 512 contains safe harbors that essentially codify the precedent in 1995's *Netcom* case, which instead countenanced only secondary liability for OSPs that host infringing content.[8] Broadly speaking, the law grants OSPs conditional immunity for unwittingly disseminating unlicensed copyrighted material without authorization.[9] Importantly, Section 512's immunity is conditioned on OSPs acting to curb infringement once they have actual knowledge of its existence, such as when notified by the copyright owner, or when the infringement is apparent. This latter category of apparent infringement is sometimes referred to as "red flag" knowledge.[10]

The regime Section 512 established has produced mixed results in practice. By enabling OSPs to transmit content across the Internet at greatly reduced risk of liability, Section 512 has, without question, facilitated the rapid growth of distribution services that also benefit content producers and consumers. At the same time, however, the proliferation of pirated content has grown exponentially. The law imposes little obligation on OSPs to mitigate the dissemination of infringing content other than to react *ex post*—at which point, the damage has already been done.

It is therefore not surprising that there have been growing calls for stronger copyright and other forms of content protection, both in the United States and around the world. Australia's Competition and Consumer Commission (ACCC) has moved to impose "neutrality" requirements on tech

---

[6] DIGITAL MILLENNIUM COPYRIGHT ACT, H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.).

[7] *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. 1552, 1554 (M.D. Fla. 1993). *Frena* is discussed, *infra*, at notes 41-45 and accompanying text.

[8] *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1365–66 (N.D. Cal. 1995). Netcom is discussed, *infra*, at notes 46- 51, and accompanying text.

[9] 17 U.S.C. § 512.

[10] *See, e.g.,* 17 U.S.C. § 512(c)(1) (providing safe harbor on the condition that the online service provider "(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material; (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.").

platforms,[11] as well as to curtail platforms' ability to monetize news content without licensing it at what news organizations believe are fair rates.[12] The European Union passed reforms to its Copyright Directive intended to provide greater protection for rightsholders.[13] And following years of public meetings and stakeholder input, the U.S. Copyright Office published its long-anticipated Section 512 report, which concluded that the safe harbors should be adjusted to better address online piracy, as "Congress' original intended balance has been tilted askew."[14]

In this paper, we examine whether Section 512 set the right balance between, on the one hand, mitigating unreasonable copyright-litigation risks that may arise from user-generated content, and on the other, holding online platforms accountable when they unreasonably fail to curb foreseeable infringement risks. We ultimately conclude, as the Copyright Office did, that the law's proper balance has been tilted askew. We therefore recommend adjustments to Section 512.

I. The Development of Section 512

When Congress passed the Digital Millennium Copyright Act ("DMCA") in 1998, only about 30% of the U.S. population used the Internet in any fashion,[15] and only 12% of American adults reported daily online use.[16] Indeed, while the Internet's potential to dramatically alter the way consumers access information and buy all manner of goods and services had become clear by the mid-1990s, much of the technology that would come to shape the Internet as we know it remained either still

---

[11] *See, e.g.*, Dirk Auer et al., *Submission on the Final Report of the Australian Competition and Consumer Commission's Digital Platform Inquiry*, INTERNATIONAL CENTER FOR LAW & ECONOMICS (Sep. 12, 2019), https://laweconcenter.org/resource/submission-on-the-final-report-of-the-australian-competition-and-consumer-commissions-digital-platforms-inquiry.

[12] *Australian News Media to Negotiate Payment with Major Digital Platforms*, AUSTRALIAN COMPETITION AND CONSUMER COMMISSION (Jul. 31, 2020), https://www.accc.gov.au/media-release/australian-news-media-to-negotiate-payment-with-major-digital-platforms; *see also* Journalism Competition and Preservation Act, S. 673, 117th Congress (2021); Dean Miller, *France and Australia to Google and Facebook: Pay for News*, THE SEATTLE TIMES (Apr. 24, 2020), https://www.seattletimes.com/opinion/france-and-australia-to-google-and-facebook-pay-for-news, (France suing Google under the new EU copyright directive for harm to news producers); Inti Landauro & Emma Pinedo, *Alphabet to Reopen Google News in Spain After Govt Amends Rules*, REUTERS (Nov. 3, 2021), https://www.reuters.com/technology/alphabet-reopen-google-news-spain-soon-after-govt-changed-regulation-2021-11-03, (Google required to negotiate with Spanish news producers under EU copyright updates).

[13] *Copyright Reform Clears Final Hurdle: Commission Welcomes Approval of Modernised Rules Fit for Digital Age*, EUROPEAN COMMISSION (Apr. 15, 2019), https://ec.europa.eu/digital-single-market/en/news/copyright-reform-clears-final-hurdle-commission-welcomes-approval-modernised-rules-fit-digital.

[14] U.S. COPYRIGHT OFFICE, SECTION 512 OF TITLE 17: A REPORT OF THE REGISTER OF COPYRIGHTS 1 (May 2020), *available at* https://www.copyright.gov/policy/section512/section-512-full-report.pdf [hereinafter "Section 512 Report"].

[15] *Data Bank: World Development Indicators*, THE WORLD BANK, http://databank.worldbank.org/data/reports.aspx?source=world-development-indicators (last visited Oct. 11, 2022).

[16] *See, e.g.*, *The Internet News Audience Goes Ordinary*, PEW RESEARCH CENTER FOR THE PEOPLE & THE PRESS (January 1999), http://www.people-press.org/1999/01/14/the-internet-news-audience-goes-ordinary.

in its infancy or did not exist at all. Amazon didn't start selling books until 1995,[17] MP3.com wasn't launched until 1997,[18] and Google wasn't founded until 1998.[19] Napster, one of the earliest drivers of massive-scale digital piracy, didn't exist until 1999.[20] Facebook wasn't launched until 2004.[21] YouTube started in 2005 and was bought by Google in 2006.[22] Twitter became a company in 2007.[23]

By contrast, recent estimates find that, today, 81% of Americans have mobile Internet access, while 28% of Americans say they are online "almost constantly."[24] Global Internet access has jumped from 3.14% in 1998 to more than 50% in 2020.[25] This explosion of online access has benefitted consumers and businesses in ways that weren't necessarily obvious in 1998. Amazon's e-commerce revolution, for example, benefitted not just Amazon, but a host of firms that wished to exploit the Internet as a distribution channel. At the same time, service has offered consumers a fast, convenient, and affordable way to shop for nearly every conceivable product. Similar revolutions have been seen in media and the arts, where digital distribution has provided users an outlet for their own creativity, while creating another channel for traditional media entities to reach audiences.

But Internet distribution reduces friction not just for legitimate transactions, but also for unlawful ones.[26] The question becomes how to combat that unlawful activity without hindering the

---

[17] *Amazon Opens for Business*, HISTORY.COM: THIS DAY IN HISTORY (Jul. 27, 2019), https://www.history.com/this-day-in-history/amazon-opens-for-business.

[18] Hope Hamashige, *MP3.com Founder Michael Robertson Discusses His Revolutionary Company*, CNNMONEY (Feb. 20, 2000), https://money.cnn.com/2000/02/28/electronic/q_mp3.

[19] *From the Garage to the Googleplex*, GOOGLE (last visited Oct. 11, 2022), https://about.google/our-story.

[20] Tom Lamont, *Napster: The Day the Music Was Set Free*, THE GUARDIAN (Feb. 23, 2013), https://www.theguardian.com/music/2013/feb/24/napster-music-free-file-sharing.

[21] Anne Sraders, *History of Facebook: Facts and What's Happening*, THESTREET (Feb. 18, 2020), https://www.thestreet.com/technology/history-of-facebook-14740346.

[22] Paige Leskin, *Youtube Is 15 Years Old*, BUSINESSINSIDER (Oct. 11, 2022), https://www.businessinsider.com/history-of-youtube-in-photos-2015-10.

[23] Jack Meyer, *History of Twitter*, THESTREET (Jan. 2, 2020), https://www.thestreet.com/technology/history-of-twitter-facts-what-s-happening-in-2019-14995056.

[24] Monica Anderson, *Mobile Technology and Home Broadband 2019*, PEW RESEARCH CTR. (2019), https://www.pewresearch.org/internet/2019/06/13/mobile-technology-andhome-broadband-2019, (reporting that 81% of American adults owned a smartphone in 2016, up from 35% in 2011); Andrew Perrin & Madhu Kumar, *About Three-in-Ten U.S. Adults Say They Are 'Almost Constantly' Online*, PEW RESEARCH CTR.: FACTTANK (Jul. 25, 2019), https://www.pewresearch.org/fact-tank/2019/07/25/americans-going-onlinealmost-constantly.

[25] *See* ITU TELECOMM. DEV. BUREAU, MEASURING DIGITAL DEVELOPMENT FACTS AND FIGURES 2019, 1 (2019), *available at* https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf; *Internet Usage Statistics: World Internet Users and 2020 Population Stats*, INTERNET WORLD STATS (last visited Oct. 11, 2022), http://www.internetworldstats.com/stats.htm; *Internet Growth Statistics*, INTERNET WORLD STATS (last visited Oct. 11, 2022), https://www.internetworldstats.com/emarketing.htm.

[26] *See* Geoffrey A. Manne & Julian Morris, *Dangerous Exceptions: The Detrimental Effects of Including 'Fair Use' Copyright Exceptions in Free trade Agreements*, INTERNATIONAL CENTER FOR LAW & ECONOMICS, ICLE White Paper 2015-1 (2015)

development of legitimate content and the online platforms that distribute it—either through excessive regulation or unending litigation risk stemming from user-generated content.

It was this question that Congress sought to address in the mid-1990s when it attempted to balance two competing interests regarding copyright policy online. On the one hand, it recognized that the incipient Internet platforms of the day would have great difficulty if they were subject to direct or secondary copyright liability for all their users' posts. On the other hand, rightsholders had a valuable interest in protecting their works. The balance Congress struck is embodied in Section 512, which was added to the Copyright Act through passage of the Digital Millennium Copyright Act of 1998.[27]

Importantly, Section 512 did not create an absolute shield for OSPs against copyright-infringement claims. Rather, Section 512 created a set of "safe harbors" that would grant various types of OSPs protection from copyright claims arising from user-generated content, provided the service providers promptly took down instances of infringement.[28] The safe harbors cover four specific categories of activity. Section 512(a) covers OSPs that merely serve as conduits for material directed at third parties;[29] Section 512(b) covers OSPs that temporarily cache content as it is being transmitted;[30] Section 512(c) covers OSPs that host material for third-party users;[31] and Section 512(d) covers OSPs that "link" to content—for example, search engines or directories.[32] Each of Section 512's safe harbors imposes certain obligations on OSPs before they will merit protection from liability. For example,

("Technologies such as DVRs and MP3 players that predominantly enable users to shift the time, location and/or format of consumption may increase the value of the creative work to the consumer and hence the creator. But there is also a risk that they will be used for illegal distribution of works, reducing income to the creator—since it is almost impossible for the creator to appropriate that value. To the extent that the value added by the technologies may be appropriated by creators, it is in the interests of the creator to permit their use—and to develop technologies that minimize infringing uses. But if the infringing use dominates—as was clearly the case with Napster, for example—then it is in the creators and society's interest for the use to be prohibited."); *See also* Benjamin Klein et al., *The Economics of Copyright "Fair Use" in a Networked World*, 92 AM. ECON. ASS'N PAPERS & PROC. 205, 208 (2002).

[27] *See* H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.) (noting that the purpose of Section 512 was to "preserve[] strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment" while "provid[ing] greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."); *See also* Irina Y. Dmitrieva, *I Know It When I See It: Should Internet Providers Recognize Copyright Violation When They See it?,* 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 233, 235-39 (2000) (discussing debates that emerged in academic circles over the problems faced by both rightsholders and online service providers under the pre-DMCA case law).

[28] 17 U.S.C. § 512.

[29] *Id.* § 512(a).

[30] *Id.* § 512(b).

[31] *Id.* § 512(c).

[32] *Id.* § 512(d).

service providers are required to comply with a notice-and-takedown procedure,[33] as well as to act on both "apparent" and "actual" knowledge of infringement.[34]

As noted above, Section 512 was passed at a relatively immature stage in the development of online technologies. At the time, the web existed largely as a collection of static, primarily text-based pages. Usenet also existed and was then a major conduit for pirated content, although its relative importance has since declined.[35] By today's standards, search technologies were crude[36] and, while there undoubtedly were private servers dedicated to content-sharing, it would have been difficult to find such servers in the relatively disorganized web of the day. High-speed Internet service was also rare and, outside of universities and large corporations, most users connected to the Internet via analog modems and telephone lines.[37] Moreover, the peer-to-peer services that would make file-sharing more efficient effectively did not exist.[38] And yet, even at the time Section 512 was enacted, it was understood that "[d]ue to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy."[39]

---

[33] Intermediaries that qualify on the basis of caching, hosting, or linking must comply with the notice-and-takedown procedures prescribed in Section 512(c)(3). *See also Io Grp., Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132, 1148 (N.D. Cal. 2008).

[34] *See, e.g.*, 17 U.S.C. § 512(c)(1)(A) (providing safe harbor on the condition that the online service provider "(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing [or] (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent"). Courts have progressively made it more difficult for rightsholders to assert claims against OSPs on the basis that they had such knowledge. For example, in *Capitol Records v. Vimeo*, the 2nd U.S. Circuit Court of Appeals construed fair use as a barrier to employees of Vimeo being able to detect potentially illegitimate uses of copyrighted material, even where that employee knew the work was copyrighted. *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 96–97 (2d Cir. 2016), *cert. denied*, 137 S. Ct. 1374 (2017) ("Even assuming awareness that a user posting contains copyrighted music, the service provider's employee cannot be expected to know how to distinguish, for example, between infringements and parodies that may qualify as fair use."). This is particularly striking, because fair use is ostensibly an affirmative defense. *See* Kristian Stout, *A Takedown of Common Sense: The Ninth Circuit Overturns the Supreme Court in a Transparent Effort to Gut the DMCA*, TRUTH ON THE MARKET (Sep. 23, 2015), https://truthonthemarket.com/2015/09/23/a-takedown-of-common-sense-the-9th-circuit-overturns-the-supreme-court-in-a-transparent-effort-to-gut-the-dmca.

[35] Ernie Smith, *How File Sharing Broke the Internet's First Forum*, MOTHERBOARD (Feb. 6, 2018), https://motherboard.vice.com/en_us/article/a34z85/how-file-sharing-broke-the-internets-first-forum-usenet.

[36] As noted above, Google did not exist until 1998 and the then-available search engines were far inferior. *See* Caleb Donaldson, *Beyond the DMCA: How Google Leverages Notice and Takedown at Scale*, 10 LANDSLIDE 2 (2017), *available at* https://www.americanbar.org/content/dam/aba/publications/landslide/2017-nov-dec/beyond-dmca.authcheckdam.pdf.

[37] *See* Howard A. Shelanski, *The Speed Gap: Broadband Infrastructure and Electronic Commerce*, 14 (2) BERKLEY TECH L. J. 721 (1999), *available at* https://lawcat.berkeley.edu/record/1116740/files/fulltext.pdf.

[38] *See* Tom Lamont, *Napster: The Day the Music Was Set Free*, THE GUARDIAN (Feb. 23, 2013), https://www.theguardian.com/music/2013/feb/24/napster-music-free-file-sharing.

[39] THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, S. REP. NO. 105-190, at 8 (1998).

Thus, even in the Internet's infancy, when broadband speeds were a tiny fraction of today's and with only rudimentary file-sharing services available, Congress believed that "[w]ith this… evolution in technology, the law must adapt in order to make digital networks safe places to disseminate and exploit copyrighted materials."[40]

A. The evolving legal backdrop

Section 512 emerged in response to federal case law regarding online copyright infringement. Two cases in particular—*Playboy Enterprises Inc. v. Frena* and *Religious Technology Center v. Netcom On-Line Communication Services Inc.*—represented the dominant poles of jurisprudence.

In *Frena*, Playboy Enterprises sued George Frena, the operator of an online bulletin-board system.[41] The complaint concerned copyrighted photos that were stored on Frena's servers and had been uploaded by users of the bulletin board without Frena's knowledge.[42] As soon as he became aware of the infringing material, Frena removed it.[43] The court, however, framed Frena's activity as one of direct infringement, rather than contributory infringement.[44] After walking through a fairly routine copyright analysis, it found Frena liable.[45]

By contrast, the *Netcom* decision two years later framed the relevant copyright analysis differently. In *Netcom*, an affiliate organization of the Church of Scientology sued the operator of a bulletin board, Thomas Klemesrud, and his Internet-service provider (ISP), Netcom, for hosting portions of copyrighted works that it owned.[46] The works were not posted by either Klemesrud or Netcom, but by a user of Klemesrud's bulletin board named Dennis Erlich.[47] The court dismissed the direct infringement claims, characterizing storage by a bulletin-board operator and transmission by an ISP as "incidentally making temporary copies," and thus insufficiently tangible to support a direct infringement claim.[48]

The court, however, went on to examine the plaintiffs' other claims of contributory infringement, as well as vicarious liability.[49] In this regard, it found that the plaintiffs had raised genuine issues of

---

[40] *Id.* at 2-3.

[41] *Playboy Enterprises, Inc. v. Frena*, 839 F. Supp. at 1554.

[42] *Id.* at 1554.

[43] *Id.*

[44] *Id.* at 1559.

[45] *Id.* at 1555-58. It is noteworthy that the court and litigants did not appear to bring up even the possibility of treating Frena as a secondarily liable party.

[46] *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. at 1365–66.

[47] *Id.* at 1365-66.

[48] *Id.* at 1368–70.

[49] *Id.* at 1373.

fact: whether Netcom and Klemesrud had sufficient knowledge that an infringement was occurring, and whether they were in positions to stop such infringement.[50] Consequently, the court denied the motion for summary judgment, and allowed the case to proceed on the secondary-liability theories.[51]

Thus, under either dominant approach to examining the infringing acts of users of an online service, there was a distinct possibility that providers could be found liable. At the same time, some rightsholders objected that basing service providers' liability on their having sufficient knowledge of infringing activities (however that term would come to be defined) would encourage OSPs to choose to be willfully blind.[52]

In response to these cases, Congress drafted and passed Title II of the Digital Millennium Copyright Act, which was subsequently codified as Section 512 of the Copyright Act:

> There have been several cases relevant to service provider liability for copyright infringement. Most have approached the issue from the standpoint of contributory and vicarious liability. Rather than embarking upon a wholesale clarification of these doctrines, the Committee decided to leave current law in its evolving state and, instead, to create a series of "safe harbors," for certain common activities of service providers. A service provider which qualifies for a safe harbor, receives the benefit of limited liability.[53]

Section 512's explicit goal was to balance the competing interests of rightsholders and service providers in a way that preserved strong incentives for service providers and copyright owners to cooperate in detecting and resolving copyright infringements in the digital networked environment.[54] At the same time, it provided greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.[55]

---

[50] *Id.* at 1376-81.

[51] *Id.* at 1383.

[52] Irina Y. Dmitrieva, *I Know It When I See It: Should Internet Providers Recognize Copyright Violation When They See It?*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 233, 237 (2000).

[53] THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, S. REP. 105-190, at 19.

[54] *Id.* at 20.

[55] *Id. See also* Section 512 Report, *supra* note 14, at 21 ("The legislative history of section 512 thus acknowledges two key components of the balance that Congress sought to achieve: the assurance that good faith actions to address internet piracy by OSPs would qualify for safe harbors, providing 'greater certainty' regarding their liability, and the preservation of 'strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment,' providing creators with viable remedies against online infringement.") *available at* https://www.copyright.gov/policy/section512/section-512-full-report.pdf; *The Digital Millennium Copyright Act at 22: What Is It, Why Was it Enacted, and Where Are We Now: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 116th Cong. (2020) (statement of Senior Judge Edward J. Damich, at 2), *available at* https://www.judiciary.senate.gov/imo/media/doc/Damich%20Testimony.pdf.

II. The Costs and Benefits of Section 512

It is to be expected that a legal regime constructed before the commercial Internet had truly taken shape would require updates as new harms and user behaviors emerged. With the benefit of hindsight that the drafters of Section 512 lacked, this section offers an overview of the positive and negative effects that the law has produced.

A. The positive effects of Section 512

Section 512 has delivered on at least some of its promise. Online-distribution services have grown dramatically: transforming entire industries; significantly altering how we consume books, music, and videos; and increasing the availability of creative works, including user-generated works. Without a doubt, OSPs have generated enormous benefits to society,[56] and a substantial proportion of those benefits have come from legitimate dissemination of high-quality content (*e.g.*, Apple Music, Spotify, Netflix, Amazon Prime Video, etc.).

It would be difficult to quantify the full value that online services carrying user-generated content have offered society, but it is surely quite large. Just seven years after Section 512's passage, YouTube was founded as a platform for individuals to store and stream everything from their own amateur films and home movies to grassroots outreach on important civic and political issues.[57] It now draws 2 billion monthly users.[58] Facebook has 1.9 billion daily users.[59] Google processes at least 2 trillion searches annually.[60] And all of these services are nominally free to users, thanks to the platforms' ability to monetize their services successfully with ad revenue. In the process of hosting and serving ads, the platforms also generate value for advertisers, who are better able to match their offerings to targeted users, and for users, who receive more relevant offers for products and services.

The rise of closed systems like iTunes (now Apple Music) and Spotify also demonstrates the benefits that can flow, in part, from predictable legal liability around digital content. Numerous third-party services allow content creators to feed their music into Apple's and Spotify's ecosystems.[61] It would be virtually impossible to vet rights claims at scale for every piece of content that these services host.

---

[56] *See, e.g.*, Erik Brynjolfsson, Avinash Collis, & Felix Eggers, *Using Massive Online Choice Experiments to Measure Changes in Well-Being*, 116 PROC. NAT'L. ACAD. SCI. 7250 (April 2019) (finding that digital goods and services have "created large gains in well-being that are not reflected in conventional measures of GDP and productivity.").

[57] *See YouTube*, BRITANNICA.COM (last visited Oct. 11, 2022), https://www.britannica.com/topic/YouTube.

[58] *See YouTube for Press* (last visited Oct. 11, 2022), https://blog.youtube/press.

[59] *See Number of Daily Active Facebook Users Worldwide as of 4th Quarter 2021*, STATISTA (last visited Oct. 11, 2022), https://www.statista.com/statistics/346167/facebook-global-dau.

[60] *See* Danny Sullivan, *Google Now Handles at Least 2 Trillion Searches Per Year*, SEARCH ENGINE LAND (May 24, 2016), https://searchengineland.com/google-now-handles-2-999-trillion-searches-per-year-250247.

[61] *See, e.g.*, TuneCore (last visited Oct. 11, 2022), https://www.tunecore.com; *see also* CD Baby (last visited Oct. 11, 2022), https://cdbaby.com.

Platforms like Bandcamp and Soundcloud provide services analogous to YouTube, but for independent musicians. Those sites allow millions of individual artists to release and market their music to a broad array of consumers. And social media like Reddit, Facebook, Instagram, and SnapChat would similarly be unable to offer multimedia-sharing services to millions or billions of users without something like the liability-limiting provisions of Section 512.

Research published in the *Proceedings of the National Academy of Sciences* (PNAS), using willingness-to-accept choice experiments, finds that users assign relatively high values to Internet services.[62] For example, survey respondents in 2017 indicated they would require the following payments to give up each of the following services for one year (95% confidence interval):

Search engines:	$14,000-22,000
Email:	$6,900-10,200
Maps:	$2,700-5,100
Video streaming:	$940-1,490
E-commerce:	$700-1,000
Social media:	$240-430
Messaging:	$115-210
Music:	$130-215

Authors Erik Brynjolfsson, et al., believe that one explanation for the high valuations that users place on Internet services is that many see them as essential to their jobs and would thus be reluctant to give them up, even for significant compensation. Moreover, the authors argue, because most consumers do not pay for these services directly, nearly all of their willingness-to-accept represents consumer surplus.

There are also intangible benefits that flow from Internet platforms and user-generated content. For example, experiments comparing Internet versus non-Internet research have found that searchers are more likely to find an answer to a question using Internet search; that an Internet search takes significantly less time to complete; and that searchers will consult significantly more sources on the Internet.[63] When searching factual questions for which there is a clear correct answer, Internet searches are significantly more likely to find the correct answer.

---

[62] Erik Brynjolfsson, et al., *supra* note 56.

[63] Yan Chen, Grace YoungJoo Jeon & Yong-Mi Kim, *A Day Without a Search Engine: An Experimental Study of Online and Offline Searches*, 17 EXP. ECON. 512 (2014).

B. The negative effects of Section 512

Along with the value created by online platforms, however, has also come the widespread, unauthorized dissemination of copyrighted content. This has almost certainly diminished some of the investment-backed expectations of content creators and rightsholders; raised costs for producers, and, thus, consumers; and reduced the quantity, breadth, and quality of content available to audiences. Early on, for example, YouTube quickly became a major venue for users to upload copyrighted content illegally,[64] while other legitimate social-media platforms similarly have hosted large quantities of unauthorized content.[65] The past quarter-century has, of course, also seen the development of myriad other sites specifically dedicated to the mass, unlawful dissemination of copyrighted content.[66]

At the same time, direct piracy is not the only negative effect suffered by rightsholders. The broad dissemination of pirated content as an alternative to legitimate content, coupled with Section 512, has placed downward pressure on the value of licenses for content. The Phoenix Center's T. Randolph Beard, George S. Ford, and Michael L. Stern conducted an economic analysis examining the distortions that online platforms have had on the market for licensing by examining the relationship between market rates and the rates that YouTube paid for digital music.[67] They concluded that YouTube's use of Section 512, given the widespread piracy on its service, "reduces revenues to artists and labels in the U.S. by at least hundreds of millions and by perhaps more than one billion dollars each year."[68] If YouTube were to pay rates closer to the market level, it would generate between $650 million and $1 billion in additional revenue for content creators.[69]

This is not to suggest that OSPs like YouTube do not attempt to control piracy on their services. Soon after acquiring YouTube, Google developed its innovative ContentID "fingerprint" filtering

---

[64] Kenneth Li, *YouTube Anti-Piracy Software Policy Draws Fire*, REUTERS (Feb. 16, 2007), https://www.reuters.com/article/us-youtube-media/youtube-anti-piracy-software-policy-draws-fire-idUSN1321663620070217, (noting that, in 2007, one copyright holder alone was demanding the removal of 100,000 copyright-protected videos from YouTube).

[65] *See, e.g.*, *Transparency Report 2021*, REDDIT.COM, https://www.redditinc.com/policies/transparency-report-2021-2, (Reddit reports a 104% increase in takedown requests for 2021, amounting to nearly 1 million pieces of content); *see also Notice and Takedown,* Facebook Transparency Report, META, https://transparency.fb.com/data/intellectual-property/notice-and-takedown/facebook, (In the first half of 2021, Facebook reports taking down more than 3 million pieces of content for copyright violations in response to 738,000 notices).

[66] *See, e.g.*, Brett Danaher, et al., *The Effect of Piracy Website Blocking on Consumer Behavior* (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2612063, (discussing the effects of site-blocking on the well-known piracy site The Pirate Bay); *see also* Brett Danaher & Michael D. Smith, *Gone in 60 Seconds: The Impact of the Megaupload Shutdown on Movie Sales* (2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229349.

[67] T. Randolph Beard, George S. Ford & Michael L. Stern, *Safe Harbors and the Evolution of Music Retailing*, PHOENIX CENTER, Phoenix Center Policy Bulletin No. 41 (2017).

[68] *Id.* at 3.

[69] *Id.* at 20.

system.[70] Such systems detect attempts to upload unauthorized content, allowing copyright holders to determine whether to permit dissemination and whether to monetize it.[71] While this is the sort of technological innovation that Congress hoped to encourage with Section 512, filtering systems are available on only a few platforms and they extend primarily to the largest copyright holders, often to the exclusion of smaller content creators.[72] Moreover, such systems do nothing to stem access to infringement on dedicated piracy sites, whose unlawful offerings can be found relatively easily, whether through word of mouth, linking sites, or search services.[73]

Compounding matters, there have been significant changes in the legal and technological landscape over the last two decades that undermine some of the assumptions underlying Section 512. As we discuss at length in the remainder of this paper, judicial interpretations have systematically diminished the effectiveness of many of the provisions of Section 512 that were meant to aid rightsholders in combatting piracy. Although red-flag knowledge of suspicious activity that could be infringement was supposed to constitute grounds on which OSPs were expected to act, judicial interpretation of Section 512's relevant provisions has so narrowed the scope of those grounds as to render them a nullity.[74] Rightsholders have, moreover, largely been unable to seek adequate redress in U.S. courts by seeking the sorts of no-fault injunctions that have been widely successful in other jurisdictions.[75] And the original standard technical measures envisioned by Section 512's drafters, which would have enabled collaborative approaches between platforms and rights holders to control piracy, have not adequately materialized.

---

[70] *See* Paige Leskin, *YouTube Is 15 Years Old. Here's a Timeline of How YouTube Was Founded, Its Rise to Video Behemoth, and Its Biggest Controversies Along Way*, BUSINESS INSIDER (May 30, 2020), https://www.businessinsider.com/history-of-youtube-in-photos-2015-10.

[71] *See, e.g., Overview of Copyright Management Tools*, YOUTUBE HELP (last visited Oct. 11, 2022), https://support.google.com/youtube/answer/9245819. "Monetization" is the process, typically, of permitting YouTube to run ads alongside the content in question and to share the proceeds of that ad sale in different ways (*e.g.*, between YouTube, the video creator, and the copyright holder).

[72] House Section 512 Hearing, 113th Cong. 54 (statement of Maria Schneider, Grammy Award Winning Composer/Conductor/Producer, Member of the Board of Governors, New York Chapter of the Recording Academy); see also Directors Guild of America ("DGA"), Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015, Notice of Inquiry at 8 (Apr. 1, 2016) ("DGA Initial Comments") ("[I]ndividual creators usually do . . . not have any access to, or in many cases awareness of . . . [content-filtering technologies]. That . . . needs to be rectified."); FMC, Additional Comments Submitted in Response to U.S. Copyright Office's Nov. 8, 2016, Notice of Inquiry at 6 (Feb. 21, 2017).

[73] Note, however, that the full picture of enforcement online remains relatively complicated. For example, acknowledging that search results can be a major vector for individuals locating pirated content, Google has begun working with the Motion Picture Association to delist sites in voluntary compliance with no-fault injunctions. *See, e.g.*, Ernesto Van der Sar, *MPA: Google's Delisting of Thousands of Pirate Sites Works*, TORRENTFREAK (Mar. 22, 2022), https://torrentfreak.com/mpa-googles-delisting-of-thousands-of-pirate-sites-works-220322. No-fault injunctions are discussed further, *infra*, at notes 195-205 and accompanying text.

[74] See section notes 100-118, *infra*, and accompanying text.

[75] See section notes 119-130, *infra*, and accompanying text.

III. The Costs and Extent of Piracy

From some perspectives, the balance embodied by Section 512 has largely worked well.[76] As Jennifer Urban, et al., characterized the current enforcement around Section 512:

> Overall, the fundamental compromise in section 512—to manage liability and enforcement costs for OSPs and rightsholders—holds in essence. The basic compromise still underpins negotiations between OSPs and rightsholders over responsibility as Internet services and distribution channels evolve.[77]

For those who take this perspective, where the basic compromise has failed, it has done so in the direction of *over*-enforcement, suggesting that the protections Section 512 offers to rightsholders should be limited further still.[78] More directly, the primary concern of many who support the status quo is the extent to which Section 512 could be used as a tool to stifle free expression, not to facilitate piracy.[79]

Nonetheless, stakeholders on both sides of the Section 512 bargain generally acknowledge that the sheer scale of online piracy has tended to overwhelm the law's notice-and-takedown provisions.[80]

---

[76] Jennifer M. Urban, et al., *Notice and Takedown in Everyday Practice* at 115, BERKLEY PUBLIC LAW RESEARCH PAPER NO. 2755628 (Mar. 17, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628. *See also, e.g.*, Amazon.com, Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015, Notice of Inquiry at 3 (Apr. 1, 2016) ("Amazon Initial Comments") ("A key principle of both federal Internet policy and the DMCA is that online service providers should not be required to police the activities of their users or make difficult legal determinations about the nature of any particular content on the service provider's system. Lawful services like Amazon and other U.S. Internet companies could not have flourished without such a policy. This principle is crucial to the growth of the Internet where today, a single service can facilitate real-time discourse among over three billion worldwide users."); *See The DMCA's Notice-and-Takedown System Working in the 21st Century: Hearing Before the S. Comm. on the Judiciary Subcomm. on Intell. Prop.*, 116th Cong. (2020) (statement of Abigail A. Rives, Intell. Prop. Couns.).

[77] Urban, et al., *id.*

[78] *Id.* at 116-21.

[79] *Id.* at 116-18; *See also* Marc J. Randazza, *Lenz v. Universal: A Call to Reform Section 512(f) of the DMCA and to Strengthen Fair Use*, 18 JETLAW 743 (2020), *available at* https://scholarship.law.vanderbilt.edu/jetlaw/vol18/iss4/3; Rashmi Rangnath, *U.S. Chamber of Commerce Uses the DMCA to Silence Critic*, PUBLIC KNOWLEDGE (Oct. 27, 2019), https://www.publicknowledge.org/blog/u-s-chamber-of-commerce-uses-the-dmca-to-silence-critic.

[80] *See, e.g.*, Computer & Communications Industry Association ("CCIA"), Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015, Notice of Inquiry at 11 (Apr. 1, 2016) ("CCIA Initial Comments"); Microsoft Corporation, Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015, Notice of Inquiry at 9 (Mar. 31, 2016) ("Microsoft Initial Comments") ("In 2012, Microsoft received notices targeting under 1.8 million links to alleged infringing works appearing in Bing's search results. In 2015, that number grew to over 82 million alleged links to infringing works appearing in Bing's search results, with more than 99% of such notices sent using Microsoft's online forms. Processing this volume of notices without the benefit of automated tools and processes, using human review, would not be viable."); Motion Picture Association of America, Inc. ("MPAA"), Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015, Notice of Inquiry at 18 (Apr. 1, 2016) ("MPAA Initial Comments") ("For smaller owners, the phenomenon may well make the notice-and-takedown exercise cost prohibitive. One independent film maker, for example,

Developed in a world that operated at dial-up speeds, Section 512 was targeted at isolating infringing content and preventing its spread. When an infringing file appeared, the relatively slow speeds of dial-up Internet access were a natural barrier that tended to prevent rapid dissemination, giving platforms and rightsholders time to issue a series of notices and counter-notices to stop further infringement. But the underlying assumptions of that bargain have been undermined by the advance of technology. Today, a file-containment approach leads to the well-known game of copyright "Whac-A-Mole" that does little, if anything, to control the spread of massive online piracy.[81]

A core defect of the current Section 512 regime is that it places little onus on platforms to prevent either the initial unlawful dissemination or the repeat posting of files that are known (or easily knowable) to be infringing. While Google faces a gargantuan task in processing millions of takedown notices, rightsholders face an even larger collective challenge in searching across all platforms to discover, investigate, and report on cases of infringement.[82] Many do not have the resources of major movie studios or record labels and must make tough decisions about how to adequately police infringement of their property.

U.S. consumers logged 725 million visits to pirate sites for movies and television programming in April 2020 alone.[83] Close to 90% of those visits were attributable to illegal streaming services.[84] In the United States, there are more than 9 million subscribers to Internet protocol television (IPTV) services specializing in pirated content, which reap more than $1 billion annually in ill-gotten gains.[85] Globally, there are more than 26.6 billion illicit viewings of U.S.-produced movies and 126.7 billion illicit viewings of U.S.-produced television episodes each year, annually costing U.S. rightsholders between $30 and $70 billion, costing the sector between 230,000 and 560,000 jobs, and costing the overall economy between $45 and $115 billion in GDP.[86]

---

had to send 56,000 takedown notices regarding her film, and that volume of notices did not result in the film's permanent removal.")

[81] Section 512 Report, *supra* note 14, at 81.

[82] For just one album ("1989" by Taylor Swift), UMG had to hire full-time staff to issue more than 180,000 takedown requests between October 2014 and March 2016. Nonetheless, that album alone was illegally downloaded more than 1.4 million times. *See* Karen Gwee, *How Artists Are Struggling for Control in an Age of Safe Harbors*, CONSEQUENCE (Jul. 8, 2016), https://consequenceofsound.net/2016/07/how-artists-are-struggling-for-control-in-an-age-of-safe-harbors.

[83] *Now More than Ever*, CREATIVE FUTURE (Jun. 10, 2020), https://creativefuture.org/now-more-than-ever (providing data from research firm MUSO).

[84] *Id.*

[85] *Pirate Subscription Services Now a Billion-Dollar U.S. Industry, Joint Digital Citizens Alliance-NAGRA Report Finds*, DIGITAL CITIZENS ALLIANCE, (Aug. 6, 2020), https://www.digitalcitizensalliance.org/news/press-releases-2020/pirate-subscription-services-now-a-billion-dollar-u.s.-industry-joint-digital-citizens-alliance-nagra-report-finds.

[86] David Blackburn, Jeffrey Eisenach, & David Harrison Jr., *Impacts of Digital Video Piracy on the U.S. Economy*, NERA CONSULTING (June 2019), *available at* https://www.theglobalipcenter.com/wp-content/uploads/2019/06/Digital-Video-Piracy.pdf.

For larger rightsholders, policing this infringement represents a significant cost (albeit one that addresses only a fraction of the online infringement that affects them). For smaller rightsholders, it can be a prohibitive barrier that prevents them from effectively policing unlicensed use of their property and existentially threatens their livelihood.[87] The Copyright Office took note of the explosion of piracy since the mid-1990s in its Section 512 report:

> [B]etween 1998 and 2010, Google received notices for less than three million URLs containing content that allegedly infringed a copyrighted work. The scale of notices grew with time, and in 2013, Google received notices for approximately three million URLs—more than the total received by Google during the previous twelve years. Since then, the volume of infringement notices has rocketed up. In 2017, Google received notices identifying about 882 million URLs, and has processed requests to delist more than 4.6 billion URLs for copyright violations to date.[88]

From January to June 2021, Microsoft reported receiving more than 11 million takedown requests involving 103 million URLs.[89] The company rejected only about 0.33% of these requests.[90]

Because takedowns occur after illicit dissemination, by the time the takedown process is initiated, copyright holders by definition have already suffered significant harm to their exclusive rights to determine whether, how, and under what terms their content may be disseminated. Moreover, the future market for the works likely has been impeded, as at least some portion of the future audience will probably be able to access the content at no cost. Recognizing the smaller addressable market, distributors (whether online or traditional media) will offer copyright holders less to license the content than they would have if the illicit dissemination had never occurred. The volume of takedown notices offers evidence of the massive scope of online piracy, which in turn can have a huge effect on a copyright's value to the rightsholder.

The status quo is also not without cost to the OSPs. Complying with the volume of requests generated pursuant to Section 512's safe-harbor requirements entails significant investment of resources.[91] Just as smaller rightsholders face disproportionately large challenges in policing infringement of their

---

[87] *See, e.g.*, The Internet Association, Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015 Notice of Inquiry at 15 (Apr. 1, 2016) ("Internet Association Initial Comments") ("[T]he problems of scale are true for Internet platform creators: startups and small businesses lack the sophisticated resources of larger, more established businesses in responding to takedown requests.")

[88] Section 512 Report, *supra* note 14, at 32.

[89] *Copyright Content Removal Requests Report*, MICROSOFT (last visited Oct. 11, 2022), https://www.microsoft.com/en-us/corporate-responsibility/copyright-removal-requests-report.

[90] *Id.*

[91] *Id.*

copyrights, it is smaller platforms and new market entrants that are least able to bear the costs of safe-harbor compliance.

There is, moreover, the potential problem of takedown notices that were filed fraudulently. Estimating real costs in this regard is difficult, as the costs of compliance depend on several factors, including internal technology and compliance staff. Some sense of the scale is available, however, from public data. For example, Automattic—the makers of a host of popular web-publishing software, including WordPress and WooCommerce—reports that, generally, between 5% and 10% of the takedown requests they receive are "abusive."[92] In 2021, this accounted for about 530 notices.[93] A larger provider like Google faces substantially more abusive takedown demands. In one study of a single fraudulent effort to force takedowns by misrepresenting ownership of content, a researcher discovered 33,988 illegitimate takedown efforts.[94] Even beyond fraud, erroneous takedowns can be a problem, with another study estimating that up to 30% of the takedown notices in its sample were potentially in error.[95]

IV. Legal Developments in the Section 512 Regime

There are two general trends that can be observed in the evolution of Section 512's legal standards: toward relatively less participation on the part of platforms to deter illegal content on their services and toward greater burdens on rightsholders to police piracy of their content.[96] While the platforms have enjoyed exponential growth and the accompanying financial rewards, the law has not always kept pace with that growth by ensuring that platforms more properly internalize the social costs of their activity.[97]

---

[92] *Intellectual Property 2021: Jul 1-Dec* 31, AUTOMATTIC (last visited Oct. 11, 2022), https://transparency.automattic.com/wordpress-dot-com/intellectual-property/intellectual-property-2021-jul-1-dec-31.

[93] *Id.*

[94] *Over Thirty Thousand DMCA Notices Reveal an Organized Attempt to Abuse Copyright Law*, LUMEN (Apr. 22, 2022), https://www.lumendatabase.org/blog_entries/over-thirty-thousand-dmca-notices-reveal-an-organized-attempt-to-abuse-copyright-law.

[95] Urban, et al., *supra* note 76, at 2.

[96] Section 512 Report, *supra* note 14, at 84 ("Over the decades, the shift in the balance of the benefits and obligations for copyright owners and OSPs under section 512 has resulted in an increasing burden on rightsholders to adequately monitor and enforce their rights online, while providing enhanced protections for OSPs in circumstances beyond those originally anticipated by Congress").

[97] Some rightsholders have claimed that the way DMCA safe harbors have been construed has led to a "culture of free" — expectations by users that content has near-zero cost. *See* U.S. COPYRIGHT OFFICE, DOCKET NO. 2015-7, SECTION 512 STUDY: NOTICE AND REQUEST FOR PUBLIC COMMENT (2015), *available at* https://downloads.regulations.gov/COLC-2015-0013-89806/attachment_1.pdf. According to these commentators, the end result of safe harbors in the presence of a "culture of free" is that the perceived value of licenses themselves goes down, resulting in a vicious circle of devaluation that affects their subsequent bargaining position with the platforms. This is, however, another way of restating the argument here. If the licensing value is diminished because existing safe harbors are improperly biased toward platform owners, then the

For example, courts have consistently interpreted Section 512's grant of immunity as being almost completely undisturbed by red-flag knowledge.[98] Courts have also interpreted a key rightsholder's ability to seek subpoenas and injunctions against actual infringers in so restrictive a manner as to effectively neuter that section of the law.[99] Further, in practice, the ways that OSPs process takedown notices essentially requires copyright holders to proceed URL-by-URL—a linear process doomed to failure and frustration in the face of logarithmic piracy.

A. Knowledge, red-flag knowledge, and the duty to monitor

To receive the benefit of a Section 512 safe harbor, OSPs engaged in hosting or search services must act to address copyright infringement by users of their services when they have either: 1) actual knowledge of infringement, or 2) awareness of facts that make it apparent that infringement is occurring—*i.e.*, red-flag knowledge.[100]

Despite some suggestions to the contrary from the U.S. Supreme Court,[101] courts have not generally imposed a legal obligation on OSPs to proactively mitigate infringement by their users to qualify for the safe harbor; rather, courts have instead only required service providers to curtail infringement after the fact. In this regard, courts have relied upon Section 512(m), which explicitly declines to condition application of a safe harbor on an OSP "monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i)."[102] There is room, however, between actively monitoring to *discover evidence of actual or impending infringement* and taking preventative measures to avoid infringement where such evidence presents itself—either because it has been affirmatively called to the OSP's attention or has otherwise become apparent.

Indeed, the legislative history of Section 512 describes actual and red-flag knowledge as two distinct ways through which OSPs may become aware of infringing material that requires action on their part.

---

devalued license reveals that the costs of piracy are born by rightsholders, instead of being allocated more equitably between platforms and rightsholders.

[98] *See*, *e.g.*, *Capitol Records, Ltd. Liab. Co. v. Vimeo, Ltd. Liab. Co.*, 826 F.3d 78 (2d Cir. 2016); *Viacom Int'l, Inc. v. YouTube, Inc.*, 676 F.3d 19 (2d Cir. 2012); *Mavrix Photographs, Ltd. Liab. Co. v. LiveJournal, Inc.*, 873 F.3d 1045 (9th Cir. 2017).

[99] *See infra* notes at 104-111 and accompanying text.

[100] *See* 17 U.S.C. § 512(c)–(d).

[101] In *Grokster*, the Supreme Court noted that secondary liability for "vicarious" infringement could attach when an OSP directly profits from an infringement, while also declining to exercise its right to stop or limit that infringement. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930 (2005). While not an explicit command to proactively monitor infringement, the Supreme Court recognized some circumstances in which a service provider's obligations are heightened with respect to deterring the presence of infringing material on their services.

[102] 17 U.S.C. § 512(m).

> [A] service provider need not monitor its service or affirmatively seek facts indicating infringing activity... in order to claim this limitation on liability (or, indeed any other limitation provided by the legislation). However, if the service provider becomes aware of a ''red flag'' from which infringing activity is apparent, it will lose the limitation of liability if it takes no action. The ''red flag'' test has both a subjective and an objective element. In determining whether the service provider was aware of a ''red flag,'' the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a ''red flag''—in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances—an objective standard should be used.[103]

To be sure, this can be a complicated standard to adjudicate. A court was expected, first, to determine whether an OSP had subjective red-flag knowledge of infringement. Next, if a court found that the OSP did not have subjective knowledge, it would have to determine if the lack of such knowledge was objectively reasonable. If the OSP's lack of knowledge was objectively unreasonable, the OSP would be required to remove the infringing material or lose the safe harbor. Thus, in the original formulation of Section 512, actual or red-flag knowledge of infringement could theoretically arise from a range of potential situations: rightsholders pointing out a violation, an employee discovering (either through automated functions or plain observation) such material, or from evidence that would lead a reasonable person to recognize that infringement might be occurring.

A series of court decisions, however, have significantly enhanced the requirements to meet these knowledge standards. In the *Viacom* case, the 2nd U.S. Circuit Court of Appeals described actual knowledge as whether the OSP "'subjectively' knew of specific infringement."[104] Other circuits and district courts have largely followed this view of actual knowledge.[105]

As for red-flag knowledge, the *Viacom* court described it as turning "on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."[106] Along these lines, the 9th U.S. Circuit Court of Appeals ruled that "general knowledge" that an entire category of hosted content was likely to contain copyrighted material was

---

[103] DIGITAL MILLENNIUM COPYRIGHT ACT, H.R. REP. NO. 105-551, at 53 (1998) (Conf. Rep.).

[104] *Viacom*, 676 F.3d at 31.

[105] *See, e.g., UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021 (9th Cir. 2013) (noting that "actual knowledge" as being "specific" knowledge of "particular infringing activity"); *BWP Media USA, Inc. v. Clarity Digital Grp., LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016) ("general knowledge of potential infringement could not count as 'actual' knowledge"); *Sony Music Entm't v. Cox Commc'ns, Inc.*, 426 F. Supp. 3d 217, 230–31 (E.D. Va. 2019) (adopting the 9th Circuit's interpretation of actual knowledge of infringement).

[106] *Viacom*, 676 F.3d at 31.

insufficient to create red flag awareness in an OSP.[107] Curiously, the 9th Circuit held that red-flag knowledge didn't exist even when a suspected infringer went so far as to label its files "stolen" or "illegal," as such labels merely increased the "salacious appeal" of the content.[108]

In effect, courts have collapsed the distinction between red-flag knowledge and actual knowledge by disallowing "red flags" to arise from general awareness of infringement on a service. The 9th Circuit's *Veoh* opinion is emblematic:

> Although the parties agree, in retrospect, that at times there was infringing material available on Veoh's services, the DMCA recognizes that service providers who do not locate and remove infringing materials ***they do not specifically know of*** should not suffer the loss of safe harbor protection.[109]

As noted above, the 2nd Circuit's *Viacom* decision essentially agreed with the requirement that subjective knowledge of infringement be "objectively reasonable" to avoid constituting red-flag knowledge.[110] Yet it also followed the 9th Circuit's approach of pinning the knowledge requirement to "specific" acts of infringement. This substantially narrows the circumstances under which an OSP could theoretically be said to form a reasonably subjective view of potential infringement.[111]

It is helpful to unpack the 2nd Circuit's 2016 *Vimeo* decision to understand the scope of the problem. Vimeo is a website that allows users to post videos. Several record labels and music publishers sued Vimeo for direct, contributory, and vicarious copyright infringement, documenting at trial a variety of Vimeo employee messages about incorporating copyrighted songs in uploads. Examples included three members of the Vimeo content-moderation team individually:

- telling a user that Vimeo allowed uploading "lip-synch" videos containing copyrighted music, but would take them down if and when asked by a rightsholder;
- telling a user, "don't ask, don't tell," in response to a question about including copyrighted music in original videos the user created;

---

[107] *Shelter Capital*, 718 F.3d at 1023.

[108] *Perfect 10, Inc. v. CCBill LLC*, 488 F.3d 1102, 1114 (9th Cir. 2007). This case may be a classic instance of bad facts making bad law, with the subject content—pornography—perhaps being viewed negatively by the reviewing court in such a way that users' increasing the "salacious appeal" of the content was seen as expected behavior.

[109] *Shelter Capital*, 718 F.3d at 1023 (emphasis added).

[110] *Viacom*, 676 F.3d at 31.

[111] *Id.* The court felt that the two provisions did not collapse into each other because of the addition of the "objective" standard for red-flag knowledge, even though the set of circumstances in which the knowledge standard could apply would become virtually identical ("The red flag provision, because it incorporates an objective standard, is not swallowed up by the actual knowledge provision under our construction of the § 512(c) safe harbor. Both provisions do independent work, and both apply only to specific instances of infringement.").

- saying to a user "[w]e can't officially tell you that using copyright music is okay. But…" in response to a question about using a song by the band Radiohead;

- telling fellow employees that she was "[i]gnoring, but sharing" internally a user message that included a link to a video and asked what Vimeo did about people using copyrighted music on Vimeo; and

- responding to a user question about including Bobby McFerrin's "Don't Worry, Be Happy" in a home video that "[t]he Official answer I must give you is: While we cannot opine specifically on the situation you are referring to, adding a third party's copyrighted content to a video generally (but not always) constitutes copyright infringement under applicable laws… Off the record answer… Go ahead and post it…."[112]

The company's vice president of product and development also sent a message to two members of the content-moderation team and every employee in the "all@vimeo.com" email group asking: "Who wants to start the felons group, where we just film shitty covers of these [EMI] songs and write 'FUCK EMI' at the end?"[113]

The 2nd Circuit nonetheless ruled that the messages in this case did not constitute red-flag knowledge because they did not relate to the specific infringement claims at issue and because the mere viewing by employees of videos containing recognizable songs would not be sufficient.[114] Citing its prior decision in *Viacom*, the court said that, to possess red-flag knowledge, the service provider must be *subjectively* aware of facts that would make the specific infringements at issue *objectively* obvious to a reasonable person.[115] Moreover, that "reasonable person" is "an ordinary person" without any expertise regarding music or copyright law, and without any obligation to investigate whether the content is copyrighted or the poster is engaged in a licensed or fair use.[116]

According to the court, it would not be sufficient to establish red-flag knowledge that there were facts that would lead a reasonable person to infer that infringement occurred. Rather, the service provider must have actual knowledge of the significance of those facts, and those facts would need to lead an ordinary, reasonable person to infer infringement was occurring.[117]

---

[112] *Vimeo*, 826 F.3d at 85-86.

[113] *Id.* at 86.

[114] *Id.* at 94.

[115] *Id.* at 93-94.

[116] *Id.* at 94.

[117] *Id.*

This appears to be both a poor interpretation of the statute and bad policy. Indeed, the Copyright Office does not appear to believe that Congress intended to erect so high a bar as the *Vimeo* court and others have suggested:

> The Office believes a standard that requires an OSP to have knowledge of a *specific* infringement in order to be charged with red flag knowledge has created outcomes that Congress likely did not anticipate. The Copyright Office reads the current interpretations of red flag knowledge as effectively removing the standard from the statute in some cases, while carving an exceptionally narrow path in others that almost requires a user to "fess up" before the OSP will have a duty to act. OSPs are correct that Congress likely did not intend to adopt a *general* awareness standard for red flag knowledge, since such a standard would consume many OSPs Congress otherwise sought to protect. ***Yet courts have set too high a bar for red flag knowledge, leaving an exceptionally narrow space for facts or circumstances that do not qualify as actual knowledge but will still spur an OSP to act expeditiously to remove infringing content.***[118]

B. Subpoenas and injunctions

Another notable trend in the law, both in the United States and abroad, has been the growing challenges rightsholders' face in seeking to identify suspected infringers. Under the EU's General Data Protection Regulation, for example, it has become significantly more difficult to obtain valid WHOIS contact information for the owners of domains that host infringing content.[119] In a similar vein, the European Commission has been wrestling with so-called "structural infringement"—infringement that occurs as a core component of a provider's business model and is aided by online anonymity.[120] According to a recent report prepared for the Commission, rightsholders in the EU find that such structural infringement is compounded by the paucity of requirements that intermediaries be identifiable to hosting providers.[121] There is little recourse under current EU law to identify anonymous parties, leading to calls to impose "know your customer" requirements on intermediaries.[122]

---

[118] Section 512 Report, *supra* note 14, at 123 (emphasis added).

[119] *See WHOIS Database Under GDPR: Temporary Measures in Place*, EURODNS (Jul. 17, 2018), https://www.eurodns.com/blog/whois-database-gdpr-compliance. The WHOIS information is now considered protected. A third party with a valid interest *can* still obtain this information, but the process has become more cumbersome and may require appeals through the ICANN organization.

[120] Jan Bernd Nordemann, *The Functioning of the Internal Market for Digital Services: Responsibilities and Duties of Care of Providers of Digital Services*, EUROPEAN PARLIAMENT IMCO COMMITTEE at 51 (2020), *available at* https://www.europarl.europa.eu/RegData/etudes/STUD/2020/648802/IPOL_STU(2020)648802_EN.pdf.

[121] *Id.* at 51-54.

[122] *Id.* at 54.

In the United States, Section 512 theoretically grants rightsholders some ability to unmask anonymous infringers through subpoenas.[123] Although it is not explicit on this point, Section 512(h) has been narrowly interpreted by courts to apply only to hosting providers, and not to Internet service providers (ISPs).[124] Technically, there are other means to potentially identify infringers, including relying on FRCP (26)(d)(1) motions to seek the identity of infringers.[125] This process, however, requires additional pleading and litigation expense as compared to Section 512(h), which allows rightsholders to apply for an unmasking order as of right once a takedown request has been filed. Limiting subpoenas solely to storage providers often ignores "the most relevant OSPs for uncovering the identity of individuals using BitTorrent and similar file-sharing protocols."[126]

Another area where Section 512 has failed to evolve is in the use of injunctions. On its face, Section 512(j) appears to provide a broad remedy to rightsholders. It allows courts to grant injunctions: 1) to disable access to infringing content, 2) to limit service to the subscriber who is infringing, or 3) to provide other relief the court deems necessary to limit infringement of copyrighted content at a specific online location.[127] The first two forms of relief, however, only address access to a specific unauthorized copy of the copyrighted content or continued service access by a specific subscriber, rather than preventing unauthorized access more broadly to the copyrighted work. This perpetuates the Whac-A-Mole problem.

The third form of injunctive order might prove more useful, but it is rarely issued. Before granting any injunction under Section 512(j), a court must perform a balancing test to determine whether the burden placed on the OSP outweighs the harm to rightsholders.[128] The Copyright Office has observed that courts have generally found that the burden on OSPs from broader orders would outweigh the benefit to rightsholders.[129] Short of a major reconsideration of how injunctive remedies should work, Section 512(j)'s injunctive remedy is unlikely to be of much use to rightsholders in the foreseeable future:

> The cost and expense of seeking an injunction in federal court against an OSP, particularly one that has previously demonstrated a willingness to litigate subpoenas and other matters relating to claims of online infringement, likely has some deterrent effect on rightsholders' willingness to test the outer boundaries of section 512(j). Thus, while there

---

[123] 17 U.S.C. § 512 (h).

[124] *See, e.g.*, *In re Subpoena to Univ. of N.C. at Chapel Hill*, 367 F. Supp. 2d 945, 955 (M.D.N.C. 2005); *see also Recording Industry Association of America, Inc. v. Verizon Internet Services, Inc.*, 351 F.3d 1229, 1233 (D.C. Cir. 2003).

[125] See, *e.g.*, *Strike 3 Holdings, LLC v. Doe*, 964 F.3d 1203, 1213 (D.C. Cir. 2020).

[126] *Id.*

[127] 17 U.S.C. 512(j)(1).

[128] 17 U.S.C. 512(j)(2).

[129] *See, e.g., Wolk v. Kodak Imaging Network, Inc.*, No. 10 CIV. 4135 RWS, 2011 WL 940056, at *8 (S.D.N.Y. Mar. 17, 2011).

> may be some untapped "potential" in section 512(j) for combating online infringement, it is unlikely that changes to section 512(j) would play a significant role in restoring the balance under section 512. Nonetheless, the Office notes that, even in the absence of legislative change, courts have been overly narrow in their consideration of available injunctive relief under section 512(j).[130]

C. Failure of voluntary, industrywide solutions

One final aspect of the legal development of Section 512 is worth addressing. As noted previously, Section 512 was enacted to create a set of tools for rightsholders and OSPs to work collaboratively to mitigate piracy, while also facilitating the growth of the commercial Internet. Ostensibly, part of this collaboration was to be the voluntary development of standard technical measures ("STMs") that could effectively prevent infringement.[131] Yet, after more than 20 years, no STMs have been adopted.[132] The most effective preventive measures produced to date have been the filtering solutions adopted by YouTube,[133] Facebook,[134] and Audible Magic,[135] but neither filtering nor other solutions have been adopted industrywide. As the Copyright Office has observed:

> While consensus-based fixes would be the ideal approach to improving the U.S. notice-and-takedown system, it has become clear that this is one instance where the perfect should not become the enemy of the good. Throughout the Study, the Office heard from participants that Congress' intent to have multi-stakeholder consensus drive improvements to the system has not been borne out in practice. By way of example, more than twenty years after passage of the DMCA, although some individual OSPs have deployed DMCA+ systems that are primarily open to larger content owners, not a single technology has been designated a "standard technical measure" under section 512(i). While numerous potential reasons were cited for this failure— from a lack of incentives for ISPs to participate in standards to the inappropriateness of one-size-fits-all technologies—the end result is that few widely-available tools have been created and consistently

---

[130] Section 512 Report, *supra* note 14, at 171.

[131] *Id.* at 67.

[132] *See e.g.*, Authors Guild, Inc., Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015, Notice of Inquiry at 27 (Apr. 1, 2016) ("As a result, there has been no impetus to conduct the sort of standards creation process to develop STMs that was contemplated by Congress . . . ."); Comput. & Commc'ns Indus. Ass'n ("CCIA"), Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015, Notice of Inquiry at 24 (Mar. 31, 2016) ("CCIA Initial Comments") ("CCIA is unaware of any successful or emerging inter-industry technological effort that satisfies the requirements of Section 512(i)(2)."); *see also* SMART Copyright Act of 2022, S. 3880, 117th Congress (2022) [hereinafter "SMART Copyright Act"].

[133] *How ContentID Works*, YOUTUBE HELP (last visited Oct. 11, 2022), https://support.google.com/youtube/answer/2797370?hl=en.

[134] *About Rights Manager*, META FOR BUSINESS (last visited Oct. 11, 2022), https://www.facebook.com/business/help/2015218438745640?id=237023724106807.

[135] *Technology*, AUDIBLE MAGIC (last visited Oct. 11, 2022), https://www.audiblemagic.com/technology.

> implemented across the internet ecosystem. Similarly, while various voluntary initiatives have been undertaken by different market participants to address the volume of true piracy within the system, these initiatives, although initially promising, likewise have suffered from various shortcomings, from limited participation to ultimate ineffectiveness.[136]

The Copyright Office sounds a somewhat pessimistic note on this situation, seeing proposed STMs as "likely to encounter opposition from one or several groups of stakeholders."[137] This concern is well-taken. For example, in their analysis of Section 512, Urban, et al., regard YouTube's use of Content ID as a *negative* for the Internet ecosystem, fearing that it may become a standard for effective rights enforcement:

> From the perspective of some other [online service providers], Google's size, its prominence in the politics of notice and takedown, and its role in litigation, combined with its early adoption of DMCA Plus measures like content filtering on YouTube, trusted sender programs, autocomplete restrictions, and search result demotion, make it a dangerous elephant in the room. It is capable of adopting practices that could move collective perceptions of what is required for good practice, or even for safe harbor protection. When Google adopts DMCA Plus measures, these OSPs see their own practices under threat, as they fear the norm-setting potential of these moves.[138]

The ideal solution to control widespread piracy would likely be a set of standards that evolve naturally and that work for both rightsholders and platform operators. In lieu of that, unfortunately, Section 512 likely needs to be reevaluated to discover where incentives can be better aligned.

In that vein, Sens. Patrick Leahy (D-Vt.) and Thom Tillis (R-N.C.)—the chair and ranking member, respectively, of the U.S. Senate Judiciary Committee's Subcommittee on Intellectual Property—recently introduced S. 3880, the SMART Copyright Act. The bill would amend Section 512 to require OSPs to comply with a slightly heightened set of obligations to deter copyright piracy on their platforms.[139] Among other changes, the Leahy-Tillis bill would empower the Office of the Librarian of Congress ("LOC") with broad latitude to recommend STMs for everything from off-the-shelf software to open-source software to general technical strategies that can be applied to a wide variety of systems. This would include the power to initiate public rulemakings in which the LOC could either propose new STMs or revise or rescind existing STMs. The STMs could be as broad or as narrow as

---

[136] Section 512 Report, *supra* note 14, at 67-68.

[137] *Id.* at 68

[138] Urban, et al. *supra* note 76, at 71.

[139] SMART Copyright Act, *supra* note 132.

the LOC deems appropriate, including being tailored to specific types of content and specific types of providers.

Critically, the SMART Copyright Act would not hold OSPs liable for the infringing content itself, but only for failure to make reasonable efforts to accommodate the STM (or for interference with the STM). Courts finding an OSP to have violated their obligation for good-faith compliance could award an injunction, damages, and costs.

Indeed, this approach comports with general principles of intermediary liability. The common law has deployed these principles in analogous situations, where the incentives of private actors are not aligned with the socially optimal outcome. As Doug Lichtman and Eric Posner have observed:

> [R]ules that hold one party liable for wrongs committed by another are the standard legal response in situations where . . . liability will be predictably ineffective if directly applied to a class of bad actors and yet there exists a class of related parties capable of either controlling those bad actors or mitigating the damage they cause. . . . [W]hile indirect liability comes in a wide variety of flavors and forms . . . , it is the norm.[140]

And as we have detailed in work examining nearly this exact concept in the context of Section 230:

> Generally speaking, the law of negligence has evolved a number of theories of liability that apply to situations in which one party obtains a duty of care with respect to the actions of a third party. One legal obligation of every business is to take reasonable steps to curb harm from the use of its goods and services.... If the business has created a situation or environment that puts people at risk, it has an obligation to mitigate the risk it has created.[141]

Services that depend on user-generated content have been a boon to free expression, commerce, and likely much more. With that said, these services are inherently likely to surface illicit content if they are not adequately maintained. It is widely debated today what sort of changes are needed to reform Section 230 in order to prevent some of the harms that have emerged in the last quarter century.[142] Section 512 is due no less for this sort of reform, where OSPs should be obligated to take reasonable steps to ensure that their services are not vulnerable to piracy. Section 512 originally contemplated that voluntary standards would emerge to achieve this end. History has demonstrated that a more positive obligation may be necessary.

---

[140] Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 223 (2006).

[141] Geoffrey A. Manne, Kristian Stout, & Ben Sperry, *Who Moderates the Moderators?: A Law & Economics Approach to Holding Online Platforms Accountable Without Destroying the Internet* at 38-39, INTERNATIONAL CENTER FOR LAW & ECONOMICS, ICLE (2021), *available at* https://laweconcenter.org/resource/who-moderates-the-moderators-a-law-economics-approach-to-holding-online-platforms-accountable-without-destroying-the-internet.

[142] See *id.* at notes 25-100 and accompanying text.

V. Potential Solutions

A range of possible reforms to Section 512 could better mitigate piracy and offer incentives for OSPs and rightsholders to engage in licensing negotiations. Properly applied safe harbors should encourage OSPs to help *prevent* unlawful dissemination of copyrighted content—as the obligation to act in the face of red-flag knowledge would largely do, absent its amelioration by the courts.[143] Ideally, such rules would also encourage OSPs to license content, enabling them and their users to benefit from such content without litigation risk. Indeed, in theory, it should be significantly more efficient for OSPs to negotiate license agreements with rightsholders than for rightsholders to do so with each of the service providers' many users.[144]

But, as noted above, the current safe-harbor regime offers few incentives for OSPs either to curb piracy or to license content at market rates; indeed, they can obtain de facto *unlicensed* access to the content at no cost and with effectively no risk of liability.[145] To help address these misaligned incentives, Section 512's safe harbor should be conditioned on OSPs taking reasonable steps: 1) to prevent infringement proactively, and 2) to stop infringement either a) when they have actual knowledge,

---

[143] *See* T. Randolph Beard, et al., *Fixing Safe Harbor: An Economic Analysis,* PHOENIX CENTER POLICY PAPER NO. 52 (2017) at 23, *available at* https://www.phoenix-center.org/pcpp/PCPP52Final.pdf (stating that "the vetting of upload material prior to its availability for consumption on the UUC platform should be encouraged" and that "the protection of the safe harbors could be limited to UUC platforms with formal vetting policies and systems.").

[144] *See, e.g.*, Reiko Aoki & Aaron Schiff, *Intellectual Property Clearinghouses: The Effects of Reduced Transaction Costs in Licensing*, 22 INFO. ECON. & POL'Y 218 (2010) (noting that third-party clearing houses are "two-sided platforms" that can improve intellectual-property licensing by centralizing information, reducing search friction, solving coordination and externality problems, simplifying contracting, and generally creating economic value by bringing upstream IP owners and downstream IP users together more efficiently); Bruce I. Carlin, *Intermediaries and Trade Efficiency*, at 6-7 (2005), https://ssrn.com/abstract=779485 (stating that intermediaries add value by allowing suppliers and consumers to trade objects of all quality levels, by alleviating the cost of obtaining a counterparty and decreasing search costs, and by decreasing the transaction cost); John E. Dubiansky, *The Licensing Function of Patent Intermediaries*, 15 DUKE LAW & TECH. REV. 269, 269-70 (2017) (arguing that licensing to intermediaries can provide advantages over unilateral licensing because intermediaries can overcome search and valuation costs, avoid litigation costs, drive licensee demand by reducing uncertainty, and create network effects by increasing the number of prospective licensees accessed through the intermediary).

[145] *See* George R. Barker, *The Value Gap in Music Markets in Canada and the Role of Copyright Law*, at 8 (2018), https://ssrn.com/abstract=3320026 (stating that poor copyright law creates a "value gap" by enabling OSPs to commercially exploit copyrighted works at less than market-based rates, if they pay copyright holders anything at all); Daniel Lawrence, *Addressing the Value Gap in the Age of Digital Music Streaming*, 52 VAND. J. TRANSNAT'L L. 511, 518-522 (2019), *available at* https://cdn.vanderbilt.edu/vu-wp0/wp-content/uploads/sites/78/2019/05/25124350/9.20Lawrence.pdf (explaining how flaws in the U.S. Copyright Act have caused a value gap); T. Randolph Beard et al., *Safe Harbors and the Evolution of Music Retailing*, PHOENIX CENTER POLICY BULLETIN NO. 41, at 20 (2017), *available at* https://www.phoenix-center.org/PolicyBulletin/PCPB41Final.pdf (estimating that the flawed safe harbors in the United States create a value gap of between $650 million and more than $1 billion *per year for music, alone*).

such as when notified by a rightsholder, or b) when infringement would be apparent to a reasonable person.[146]

Below, we discuss potential adjustments to the legal standards that lead to application of safe harbors, as well as the practical steps that OSPs would need to take to qualify. We also examine some relatively less dramatic changes that could nonetheless contribute to a healthier online ecosystem that deters piracy and preserves the freedom of OSPs to innovate.

A. Clarification of the knowledge standards

As noted above, judicial interpretations of Section 512 have essentially collapsed the red-flag standard into the actual-knowledge standard, while progressively narrowing the scope of the actual-knowledge standard; the bar for legally relevant knowledge of infringing activity is now quite high.[147]

To remedy this, the statute should be revised to effectively overturn the subjective element of red-flag knowledge applied in *Vimeo*. OSPs that host user-generated content should be attributed more knowledge than an "ordinary" person. Thus, red-flag knowledge would be present when information exists that would *objectively* lead a reasonable person *in the business of facilitating dissemination of user-generated content* (*i.e.*, running a website that hosts such content) to infer infringement is taking place, even if a rightsholder has not alerted the site to a *specific instance* of infringement.

OSPs that host user-generated content seek to monetize that content. The DMCA presumes a significant likelihood that much of that content includes copyrighted material. Just as Congress wanted to ensure that platforms had room to grow and operate, so too did it intend to provide opportunity for rightsholders and platforms to work together to meaningfully control piracy. A service in the business of distributing content, where there is an elevated risk of infringing content, should be expected to act according to a higher standard than that to which we would hold an uninformed lay person.

This obligation to behave reasonably should exist even if that requires some degree of investigation and remediation on the part of the OSP *once they have information that would objectively lead a reasonable platform to infer infringement is taking place*. The obligation should obtain even if that information did not come from the rightsholder and was not related to a specific instance of infringement.

Such a standard would still offer reasonably responsive OSPs a safe harbor, which is appropriate, given that it would be impossible for platforms to catch all instances of infringement. The standard

---

[146] *See* Beard et al., *supra* note 143 at 4-5, 8-10, 20, 21-22, 25-26 (2017) (stating that the United States' flawed copyright safe harbors promote infringing platforms to the detriment of responsible ones, and recommending that the safe harbors be conditioned on platforms doing more to *prevent* piracy in the first place).

[147] *See, e.g.*, *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d at 78; *Viacom v. YouTube*; *Ventura Content, Ltd. v. Motherless, Inc.*, 885 F.3d 597, 610–11 (9th Cir. 2018); *BWP Media USA, Inc. v. Clarity Digital Grp., LLC*, 820 F.3d 1175, 1182 (10th Cir. 2016).

is not and should not be one of perfect content moderation, but one of *reasonable* content moderation. So long as a platform takes objectively reasonable steps to prevent and remediate infringement, the fact that other infringement slips through should not result in loss of the Section 512 safe harbor.

B. Authentication, anonymous users, and subpoena authority

The Internet has long facilitated anonymous or pseudonymous communications. Fully anonymous communication systems obviously make it more difficult for rightsholders to pursue the parties responsible for infringement. Further, they can create a sense of safety (real or imagined) for would-be infringers, who may believe they can infringe with impunity.

Thus, another beneficial reform would require OSPs that host content likely to contain infringing material to reasonably ensure that they know their users' identities. This would both discourage users from engaging in piracy and make it harder for those users to evade enforcement (and to continue infringing) simply by changing account names once caught. It would also help rightsholders to seek redress, including in cases where all they want is to ask users who are infringing unintentionally to cease doing so. Identities could remain confidential, disclosed to third parties only when needed to resolve a case of infringement.

Such disclosure might be provided voluntarily by the service provider, subject to any applicable requirements regarding the user's privacy. The disclosures might also be provided pursuant to subpoenas issued under Section 512(h), which provides that "[a] copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection."[148]

Relatedly, as the Copyright Office has explained, "this provision has proven to be little-used by rightsholders, in part because of how restrictively courts have interpreted it and in part because the information gleaned from such subpoenas is often of little use."[149] Such subpoenas can be costly to obtain and are frequently ineffective; the data are often inaccurate or useless, and the OSPs may have already deleted it.[150] Moreover, courts have held that only OSPs that *host* material that can be removed pursuant to section 512(c)(3)(A) may be the subject of a Section 512(h) subpoena. In practice, this means such subpoenas cannot be used to obtain information from "mere conduit" ISPs.[151]

The Copyright Office is not convinced that Congress intended to exclude ISPs from section 512(h). Only an ISP is likely to be able to determine the identity of a user behind an IP address, information

---

[148] 17 U.S.C. § 512(h)(1).

[149] Section 512 Report, *supra* note 14, at 6.

[150] *Id.* at 164.

[151] Verizon, 351 F.3d at 1234–36.

essential to filing an infringement claim.[152] The Copyright Office has therefore recommended clarifying that Section 512(h) applies to conduit ISPs.[153] OSPs are supposed to help rightsholders combat infringement in exchange for safe-harbor protection. Section 512 should be amended to require all OSPs seeking safe-harbor protection to provide whatever identifying information their service collects pursuant to a Section 512(h) subpoena.

C. Filtering, takedown, and staydown

Section 512 does not require OSPs to proactively filter infringing content.[154] It was, however, expected that private industry would collaborate to develop and implement widespread standards for proactive technological controls to deter piracy. Section 512(i), for example, requires OSPs to accommodate STMs that would deter piracy and that have been developed through a voluntary, consensus process. While there have been piecemeal developments toward that end, the imagined innovations have thus far failed to materialize industrywide.

Congress must consider ways to prevent the initial sharing of pirated works, rather than the prevailing outdated file-containment approach. The latter presumes that post-hoc notice-and-takedown will be sufficient to control the spread of infringing material, which has not proven to be the case. New filtering solutions could empower OSPs to contribute significantly toward fighting piracy.[155]

Were OSPs to adopt reasonably effective filtering technologies, infringing files that are flagged and removed could more reliably be prevented from being reposted in the future. Indeed, as far back as 2007, several media and platform companies developed a set of best practices to control the proliferation of piracy. The proposed principles for user-generated content called on "websites to implement filtering technology that can recognize copyrighted works and notify rightsholders of any matches; rightsholders may then determine how the match should be treated."[156]

---

[152] See discussion, *supra*, at note 125 and accompanying text.

[153] Section 512 Report at 6, 166-67.

[154] But note that the Supreme Court has held that, in some cases, a lack of filtering is a relevant element of an infringement analysis. *See Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 913 (2005) (noting that evidence suggested that Grokster and StreamCast were not "merely passive recipients of information about infringing use" but engaged in inducement, and observing that there was "no evidence that either company made an effort to filter copyrighted material from users' downloads or otherwise impede the sharing of copyrighted files.").

[155] *See* Beard et al., *supra* note 143, at 10 (observing that platforms are now capable of relatively effective filtering and suggesting that such filtering should be a "predicate for safe harbor," with notice and takedown used as a "backstop.").

[156] *Principles For User Generated Content Services*, UGCPRINCIPLES.COM (last visited Oct. 11, 2022), *available at* https://ugcprinciples.com.

Such filtering technologies already exist. Google employs proprietary filtering systems, for example.[157] DropBox has also implemented filtering in the past.[158] Audible Magic makes its filtering technology available for use by others,[159] and even small websites have found ways to employ filtering.[160] Indeed, even more prosaic technologies that have existed for decades—like web crawlers and digital fingerprinting accessible through basic APIs—could be adopted as effective STMs.

As the Copyright Office has noted, however, private firms could do more to advance broader access to these technologies for a wider range of firms.[161] A legal requirement to filter content for copyright infringement would help to foster a market for additional filtering solutions. This, in turn, could drive down costs and help to address the concern that smaller entities lack the resources to either create or obtain filtering solutions.[162]

The Copyright Office could help facilitate this process. Congress could empower the office to work with industry on specifications for STMs and to establish guidelines that ease their implementation. This could include determining minimum levels of functionality that such filters must include, which in turn should take a given platform's size into account.

Indeed, this idea is central to the proposed SMART Copyright Act, discussed at the end of Part IV.[163] In this regard, the bill is directionally correct legislation, with two important caveats: it all depends on the kinds of STMs the LOC recommends and on how a "violation" is determined for the purposes of awarding damages.

The law would magnify the incentive for private firms to work together with rightsholders to develop STMs that more reasonably recruit OSPs into the fight against online piracy. In this sense, the LOC would be best situated as a convener, encouraging STMs to emerge from the broad group of OSPs and rightsholders. The fact that the LOC would be able to adopt STMs with or without stakeholders' participation should provide more incentive for collaboration among the relevant parties.

Short of a voluntary set of STMs, the LOC could nonetheless rely on the technical suggestions and concerns of the multistakeholder community to discern a minimum viable set of practices that

---

[157] *See supra* notes 133 & 134.

[158] Greg Kumparak, *How Dropbox Knows When You're Sharing Copyrighted Stuff (Without Actually Looking At Your Stuff)*, TECHCRUNCH (Mar. 30, 2014), https://techcrunch.com/2014/03/30/how-dropbox-knows-when-youre-sharing-copyrighted-stuff-without-actually-looking-at-your-stuff.

[159] Audible Magic (last visited Oct. 11, 2022), https://www.audiblemagic.com.

[160] *See, e.g., Ventura Content v. Motherless, Inc.*, 885 F.3d 597, 616 (9th Cir. 2018) (indicating a site in the case employed hashing software to police the presence of illicit clips on its service).

[161] Section 512 Report, *supra* note 14, at n. 501.

[162] Urban, et al. *supra* note 76, at 124.

[163] *See* SMART Copyright Act, *supra* note 132 and accompanying text.

constitute best efforts to control piracy. The least desirable outcome—and the one most susceptible to failure—would be for the LOC to examine and select specific technologies.[164]

Among the concerns that surround promulgating new STMs are that they could potentially create cybersecurity vulnerabilities or sources for privacy leaks, or that they could accidentally chill speech.[165] In light of the potential unforeseen harms that can arise from implementation of an STM, the SMART Copyright Act's requirements should be modified. If a firm does, indeed, discover that a particular STM, in practice, leads to unacceptable security or privacy risks, or is systematically biased against lawful content, there should be a legal mechanism that would allow for good-faith compliance, while also mitigating the STM's unforeseen flaws. Ideally, this would involve working with the LOC in an iterative process to refine relevant compliance obligations.

While adopting filtering solutions would represent a new cost for many OSPs, complying with the existing notice-and-takedown system has costs, as well.[166] Using filtering solutions to prevent the unauthorized dissemination of copyrighted material would reduce the number of takedown notices that rightsholders would need to send and that OSPs would need to process. All parties would save time, hassle, and money—very possibly reducing the overall cost of Section 512 compliance.

1. Fears of illegitimate blocking are overstated

Some critics have raised concerns that flaws in filtering technology could lead to mistakenly blocking legitimately disseminated content.[167] Among the faults commonly attributed to filtering solutions are failures to recognize licensed content or content disseminated pursuant to the Fair Use doctrine, or instances in which a rightsholder is mistaken as to the scope of its copyright.[168] The extent to which such faults are common is difficult to assess empirically. The experience of companies that offer content filters is proprietary information, and there are any number of reasons a platform

---

[164] All else equal, firms are more intimately familiar with how their own technology works and how their users interact with that technology than are regulators. As such, regulators are usually best positioned to propose general standards and leave technical implementation details up to actual market participants (so long as such implementation reasonably comports with the requirements of the standard).

[165] *Re:Create Statement on Dangerous Technical Mandate and Filtering Bill, S. 3880*, RE:CREATE (Mar. 18, 2022), https://www.recreatecoalition.org/press_release/recreate-statement-on-dangerous-technical-mandate-and-filtering-bill-s-3880.

[166] *See* Section 512 Report, *supra* note 14, at n. 237 (quoting comments of the Business Software Alliance that "BSA members invest significant resources into developing state of the art systems for processing high volumes of takedown notices."); *In re* Section 512 Study: Notice and Request for Public Comment, Copyright Office Docket No. 2015-7, *Comments of the Information Technology and Innovation Foundation*, at 3, (Mar. 21, 2016), *available at* http://www2.itif.org/2016-section-512-comments.pdf (stating that "[t]he best way to minimize the cost of sending and responding to so many notices of infringement is to use automated techniques. In particular, online service providers can use automated filtering systems that check content as it is uploaded to stop a user from reposting infringing content.").

[167] *See, e.g.*, Ben Depoorter & Robert Kirk Walker, *Copyright False Positives*, 89 NOTRE DAME LAW REV. 319, 322 (2013) ("Second, and even more problematic, are instances where transaction costs and risk aversion inhibit wrongly accused infringers from opposing copyright infringement actions.").

[168] *Id.*

might choose not to contest a takedown request that it or its users believe to be illegitimate. But some inferences may be drawn from available data, which generally suggest that harms stemming from this concern do not outweigh the known costs of piracy.

Actual false positives—instances where a user has an unambiguous right to use a file (*e.g.*, they are the actual creator or have a license)—are likely to be exceedingly rare. A party who is the unambiguous creator of a work understandably has strong incentives to ensure that she can use her work as she sees fit.

What remains are false positives that fall somewhere on the spectrum of fair use—that is to say, they are somewhere between probably authorized under the fair-use factors and probably not authorized. If this reasoning is correct, then looking at the known instances of objections to takedown requests offers some sense of the possible scope of any false-positives problem. Some of the testimony offered during a December 2020 hearing of the U.S. Senate Judiciary Committee is illustrative in this regard.

According to Katherine Oyama, global director of business public policy for Google, uploaders disputed less than 1% of the Content ID claims made from January through June 2020.[169] Thus, in the set of all takedowns, 99% of the uploaders did not feel sufficiently entitled to use as to lodge an objection, or lodging an objection was otherwise not worth their time due to a variety of costs.[170] The remaining 1% captures some significant portion of those who are both definitely entitled (*i.e.*, the original creator or a licensee who was misidentified) and those legitimately entitled to use under the fair-use affirmative defense.[171]

Among that 1% of uploaders, slightly more than half of the disputes were resolved in the uploader's favor.[172] Even if all the remaining disputed uploads were kept down in error—which is unlikely—that would represent an error rate of less than 0.5% of all content flagged by Content ID. It is likely that most, if not all, of the errors were remedied in the slightly more than 0.5% of material flagged by Content ID that was allowed to proceed onto YouTube. Further, according to Noah Becker—president and co-founder of Adrev, a digital-rights-management company that administers Content ID

---

[169] *The Role of Private Agreements and Existing Technology in Curbing Online Piracy: Hearing Before the Subcomm. on Intell. Prop. of the S. Comm. on the Judiciary*, 116TH CONG. (2020) (written testimony of Katherine Oyama, at 9), *available at* https://www.judiciary.senate.gov/imo/media/doc/Oyama%20Testimony.pdf.

[170] Some users undoubtedly lack knowledge of their rights. Others will find the costs in time to outweigh the benefit of pressing a fair use claim. The relevant point here is that the reasons for failing to object are likely diverse. Thus, concerns rooted in a concept that all users who fail to object to a takedown are having their rights improperly ignored is potentially quite misleading.

[171] Admittedly, this is an extrapolation. But it is hard to imagine that a true author would fail to object to a takedown of her content. Similarly, a person who incorporates part of a work into his or her own work and feels entitled under fair use (*e.g.*, a parody or a news commentary) has a relatively strong incentive to object. Whereas a user that incidentally includes a song in the background of a video has a much more ambiguous claim and is much less likely to object.

[172] *Id.*

claims for rightsholders—70% of Content ID disputes are "false claims of fair use, false claims of having procured a license, or false claims that the content is in the public domain. Most of these illegitimate disputes contain perjurious information from the user."[173]

Using a similar set of numbers as those offered by Katherine Oyama, economist Stan Liebowitz estimated the differential between the number of infringing files uploaded to YouTube annually and the number of files taken down as infringing but later restored.[174] By his analysis of publicly available data, in 2016, roughly 2 million takedown disputes were resolved in favor of the uploader, while 600 million files were taken down and stayed down.[175] That is to say, 0.3% of takedowns were in error, which he characterized as a conservative estimate.[176]

It is, of course, possible that the percentage of false takedowns is greater than 1%, given that we can extrapolate only from known takedowns and putbacks. But if some unaccounted-for number of false takedowns are never challenged, it would appear that those users have deemed it not worth the trouble. Given the relative simplicity of the platforms' takedown-challenge process,[177] a reluctance to engage would suggest the uploader does not place much value in the upload (*i.e.*, there is not much benefit to be had and, by implication, limited social value). In such cases, the social cost of the false positive (erroneous takedown) is presumably not very significant compared to the value of enforcing IP rights.

By contrast, a false negative (erroneously leaving content up), even on a small site, can create significant harms to a rightsholder. Even a single unauthorized version of copyrighted content can quickly become available to the world, due to the global nature of the Internet and the availability of search, linking sites, and Internet-protocol-enabled piracy devices. Moreover, a single unauthorized version can multiply quickly. Thus, without more evidence, there is currently no reason to assume that content-filtering solutions like Content ID result in such widespread removal of legitimate uses of copyrighted material as to justify failing to enforce rightsholders' claims rigorously.

---

[173] *Id.*; *The Role of Private Agreements and Existing Technology in Curbing Online Piracy: Hearing Before the Subcomm. on Intell. Prop. of the S. Comm. on the Judiciary*, 116TH CONG. (2020) (written testimony of Noah Becker, at 6), *available at* https://www.judiciary.senate.gov/imo/media/doc/Becker%20Testimony.pdf. And to the extent the illegitimate disputes were inadvertent, the education requirement discussed above would play an ameliorating role.

[174] Stan J. Liebowitz, *Economic Analysis of Safe Harbor Provisions*, CISAC, at 10 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143811.

[175] *Id.* at 11.

[176] *Id.* (Noting that he is selecting numbers on the low side of the potential range of takedowns and putbacks). In another analysis of a study purporting to demonstrate "high" error rates from false takedown notices, George Ford demonstrates that the actual incidence is less than 0.2% of requests. George S. Ford, *Notice and Takedown in Everyday Practice: A Review*, 3 (2017), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2963230.

[177] *See, e.g.*, *Submit a Copyright Counter Notification*, YOUTUBE (last viewed Apr. 7, 2022), https://support.google.com/youtube/answer/2807684.

While an industry standard for proactive filtering would help, the incredible scale of the takedown problem highlights deeper flaws in Section 512. The law should also be extended to place affirmative obligations on OSPs to employ filtering to prevent the recurrence of known infringing material once it has been discovered—a so-called "staydown" obligation, similar to recent experiments in the EU.[178] Expecting a rightsholder to repeatedly notify an OSP each time an infringing file reappears on the service makes little sense: it places rightsholders—especially small rightsholders—at a constant disadvantage.

Indeed, the Copyright Act does not currently require a copyright holder to scour a site for every instance of infringement of a specific work and to itemize every URL. Section 512(c)(3)(A)(ii) specifies that a takedown notice must identify the "copyrighted work claimed to be infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a *representative list* of such works at that site."[179] Section 512(c)(3)(A)(iii) makes clear that the copyright holder need provide only "information *reasonably sufficient* to permit the service provider to locate" the infringing material.[180] Even if a copyright holder fails to "substantially comply" with the notice information requirements, the OSP must take "reasonable steps" to work with the copyright holder to gather the missing information.[181] If reasonably sufficient information remains unavailable, the copyright holder's notice would not be considered the source of actual or red-flag knowledge.[182] The OSP may, however, obtain such knowledge from other sources.

Despite the broad obligations placed on OSPs by the Copyright Act's statutory language, courts have rendered decisions that suggest rightsholders must provide near-exhaustive information, including URLs, for each and every specific infringement before OSPs have essentially any obligation to act.[183] The legislative history makes clear that such detailed information, while certainly helpful, is not required:

> Where multiple works at a single on-line site are covered by a single notification, a representative list of such works at that site is sufficient. Thus, for example, where a party is operating an unauthorized Internet jukebox from a particular site, *it is not necessary that the notification list every musical composition or sound recording that has been, may have*

---

[178] *See* DSM Directive, art. 17(4). To avoid liability for an instance of infringement on its service, an OSP must have "acted expeditiously, upon receiving a sufficiently substantiated notice from the rightholders, to disable access to, or to remove from their websites, the notified works or other subject matter, **and made best efforts to prevent their future uploads**." (emphasis added)

[179] 17 U.S.C. § 512I(3)(A)(ii).

[180] 17 U.S.C. § 512(c)(3)(A)(iii).

[181] 17 U.S.C. § 512(c)(3)(B)(ii).

[182] 17 U.S.C. § 512(c)(3)(B)(i).

[183] *See Perfect 10 v. CCBill*, 488 F.3d 1102 (9th Cir. 2007); *Viacom Int'l v. YouTube, Inc.*, 940 F.Supp. 2d 110, 115 (S.D.N.Y. 2013).

> *been, or could be infringed at that site*. Instead, it is sufficient for the copyright owner to provide the service provider with a *representative list* of those compositions or recordings in order that the service provider can understand the nature and scope of the infringement being claimed.
>
> New subsection (c)(3)(A)(iii) requires that the copyright owner or its authorized agent provide the service provider with information *reasonably sufficient* to permit the service provider to identify and locate the allegedly infringing material. An *example* of such sufficient information would be a copy or description of the allegedly infringing material and the so-called ''uniform resource locator'' (URL) (*i.e.*, web site address) which allegedly contains the infringing material. The goal of this provision is to provide the service provider with *adequate information* to find and examine the allegedly infringing material expeditiously.[184]

Some OSPs impose additional technical requirements for notices, such as creating an account or using an online form, instead of emailing the designated agent registered with the Copyright Office.[185] To mitigate this problem, the Copyright Office should be authorized to create model forms deemed to provide adequate notice, as well as to specify what kind of information is necessary and sufficient to require takedown. This information could be revised in a periodic process to give the office and stakeholders opportunities to properly shape the contours of this set of requirements.

D. Repeat-infringer policies

Section 512 already requires that OSPs have policies to terminate service to repeat infringers, and to reasonably implement those policies. Indeed, Section 512(i) requires that, to be eligible for safe harbor, an OSP must have "adopted and reasonably implemented, and inform[ed] subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers."[186] As the Copyright Office has observed:

> Both the House Commerce and Senate Judiciary Committee Reports explained that "those who repeatedly or flagrantly abuse their access to the Internet through disrespect

---

[184] H.R. Report No. 105–551, at 55 (emphasis added).

[185] *See Copyright and the Internet in 2020–Reactions to the Copyright Office's Report on the Efficacy of 17 U.S.C. § 512 After Two Decades: Hearing Before the H. Comm. on the Judiciary*, 116TH CONG. (Dec. 15, 2020) (statement of Terrica Carrington, at 8), *available at* https://copyrightalliance.org/wp-content/uploads/2020/11/Copyright-Alliance-512-DMCA-HJC-Testimony-for-September-30-FINAL.pdf (stating that "[i]ndividual creators face numerous other significant barriers to the effective use of the notice and takedown process, including the lack of uniformity and consistency from one OSP's web form to the next, and the practice by some OSPs of imposing requirements beyond those prescribed under the law").

[186] 17 U.S.C. § 512(i)(A).

> for the intellectual property rights of others should know that there is a realistic threat of losing that access."[187]

Courts, however, have historically interpreted the repeat-infringer policy requirement rather loosely. In *Ventura Content v. Motherless, Inc.*,[188] a site that allowed users to upload pornographic images and videos was found not to be in violation of the repeat-infringer policy requirement, even though the operator did not have a formal, detailed policy or keep a list of the number of times a user infringed.[189] The operator testified that he instead relied on his memory and terminated some repeat infringers but not others based on his own "gut" judgment, after considering a variety of unwritten factors that were not publicly available.[190] The court nonetheless concluded that this met the obligation to have a policy and to reasonably implement it.[191]

Where violations have been found, such cases have typically involved such egregious fact patterns as to provide little generalizable guidance. In *Capitol Records v. Escape Media Group*, an online-music service was found in violation where it failed to keep adequate records of infringement, prevented copyright owners from collecting information necessary to issue takedown notices, and did not terminate repeat infringers.[192] In *UMG Recordings v. Grande Communications Networks*, an ISP was found in violation where it had "utter[ly] fail[ed] to terminate any customers at all over a six-and-a-half-year period despite receiving over a million infringement notices and tracking thousands of customers as repeat infringers."[193] And in *BMG Rights Management v. Cox Communications*, an ISP was found in violation where it capped the total number of notices a copyright holder could provide in a day; only counted one copyright-holder notice per subscriber per day; only *considered* terminating users after 13 strikes; and, if it did terminate them, reinstated the users after a break and restarted the strike counter so that, as an employee email indicated, the company could "collect a few extra weeks of payments for their account."[194]

The point of the DMCA safe harbor is to provide platforms greater certainty regarding litigation risk *when they act responsibly* and to assure copyright holders that their rights will be reasonably protected in exchange for the liability limitations the platforms receive. That bargain is not achieved unless the platforms (and their users) know that costly repeat infringement will not be tolerated. To better

---

[187] Section 512 Report, *supra* note 14, at 102 (citing H.R. Rep. No. 105-551, pt. 2, at 61 (1998); S. Rep. No. 105-190, at 52 (1998)).

[188] 885 F.3d 597 (9th Cir. 2018).

[189] *Id.* at 607-8.

[190] *Id.* at 616.

[191] *Id.* at 619.

[192] *Capitol Records v. Escape Media Group*, 12-CV-6646 (AJN) (S.D.N.Y. Mar. 25, 2015).

[193] *UMG Recordings v. Grande Communications Networks*, 384 F. Supp. 3d 743 (W.D. Tex. 2019).

[194] *BMG Rights Management v. Cox Communications*, No. 16-1972 (4th Cir. Feb. 1, 2018).

address this goal, the Copyright Office should be authorized to provide guidance on the minimum requirements necessary to meet the repeat-infringer policy obligation, including by creating a model repeat-infringer policy that will be presumed to comply. This would offer platforms, their users, rightsholders, and courts more clarity on what behavior will be sanctioned.

E. No-fault injunctions

Even where U.S. courts have ruled that websites have willfully engaged in infringement, stopping the infringement can be difficult, especially when the parties and their facilities are located outside the United States. One solution would be for a court to direct a non-party to the case, such as a U.S. -based ISP, to cut off access to a website held to be infringing.

Although Section 512 does allow courts to issue injunctions, there is ambiguity as to whether it allows courts to issue injunctions that obligate OSPs not directly party to a case to remove infringing material. Section 512(j) provides for the issuance of injunctions "against a service provider that is not subject to monetary remedies under this section."[195] The "not subject to monetary remedies under this section" language *could* be construed to mean that such injunctions may be obtained even against OSPs that have not been found at fault for the underlying infringement.[196] But, "[i]n more than twenty years … these provisions of the DMCA have never been deployed, presumably because of uncertainty about whether it is necessary to find fault against the service provider before an injunction could issue, unlike the clear no-fault injunctive remedies available in other countries."[197]

Indeed, more than 40 countries—including Denmark, Finland, France, India, England, and Wales—have enacted or are under some obligation to enact no-fault-injunction provisions directing ISPs to disable access to websites that predominantly promote copyright infringement.[198]

---

[195] 17 U.S.C. § 512(j).

[196] *See Copyright Law in Foreign Jurisdictions–How Are Other Countries Handling Digital Piracy?: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 116TH CONG. (Mar. 10, 2020) (statement of Justin Hughes, at 11 & n.65), *available at* https://www.judiciary.senate.gov/imo/media/doc/Hughes%20Testimony.pdf ("§512(j)(1)(B) makes transmission ISPs eligible for injunctive orders to deny access to subscribers engaged in infringing activity 'by terminating the accounts of the subscriber or account holder that are specified in the order' as well as eligible for orders 'restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.' I believe that §512(j)(3) makes it clear that these orders were intended to be "innocent" third party injunctions available without suing the ISP.").

[197] *See Copyright Law in Foreign Jurisdictions–How Are Other Countries Handling Digital Piracy?: Hearing Before the Subcomm. on Intellectual Property of the S. Comm. on the Judiciary*, 116TH CONG. (Mar. 10, 2020) (testimony of Stanford K. McCoy, at 6), *available at* https://www.judiciary.senate.gov/imo/media/doc/McCoy%20Testimony.pdf.

[198] *See* Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, art. 8(3), 2001 O.J. (L 167) (EC); Ellen Marja Wesselingh, *Website Blocking: Evolution or Revolution? 10 Years of Copyright Enforcement by Private Third Parties*, REV. INTERNET DERECHO POLITICA 38–39 (October 2014), https://idp.uoc.edu/articles/10.7238/idp.v0i19.2422/ galley/2482/download; Neil Turkewitz, *Why the Canadian Supreme Court's Equustek Decision Is a Good Thing for Freedom – Even on the Internet*, TRUTH

> [L]egally and factually, these remedies turn on the infringing conduct of the pirate site at issue; they do not entail any finding of fault on the part of the intermediaries. No-fault injunctive remedies have been applied against a wide range of intermediaries, after first giving the intermediary notice of the infringing conduct taking place through its platform, all without entailing any inquiry into whether the intermediary may or may not have behaved in a manner that would incur primary or secondary liability. That question simply is not relevant to this form of relief, which turns on the simple finding that "such intermediaries are best placed to bring such infringing activities to an end."[199]

Relatedly, Google has been working with rightsholders to delist pirate sites in response to "'no fault' orders directed at ISPs."[200] To date, they have delisted nearly 10,000 sites in this manner.[201] The Motion Picture Association claims that its partnership with Google to delist pirate sites results in a "1.5 times larger traffic decline," when compared with no-fault injunctions applied strictly at the ISP level.[202]

Thus, Section 512 should be amended to similarly grant U.S. courts authority to issue no-fault injunctions that require OSPs to block access to sites that courts have ruled are willfully engaged in mass infringement. Comparable authority was included in the Stop Online Piracy Act that was defeated in 2012, amid hyperbolic claims that allowing such orders would "break the Internet." Notably, however, such sky-is-falling predictions have not materialized in the other nations that have authorized no-fault injunctions.[203] In fact, there is evidence that such orders can be quite useful in

---

ON THE MARKET (Jul. 8, 2017), https://truthonthemarket.com/2017/07/08/why-the-canadian-supreme-courts-equustek-decision-is-a-good-thing-for-freedom-even-on-the-internet.

[199] *See* McCoy, *supra* note 175, at 3 (quoting Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, recital 59).

[200] Charles H. Rivkin, *Working Toward a Safer, Stronger Internet*, MOTION PICTURE ASSOCIATION (Mar. 21, 2022), https://www.motionpictures.org/press/working-toward-a-safer-stronger-internet.

[201] *Id.*

[202] *Id.*

[203] *See* Brett Danaher et al., *Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior* at 17 (Apr. 18, 2016) (unpublished article), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2766795; *see also Rettighedsalliancen, Annual Report 2017*, 5 (March 2018), *available at* https://rettighedsalliancen.dk/wpcontent/uploads/2018/08/ENGB_RettighedsAlliancen2018.pdf (noting the average 75% decrease in Danish IP traffic to piracy sites in the wake of DNS blocking orders).

curbing piracy,[204] with one study demonstrating that no fault injunctions led to a more than 90% decrease in piracy.[205]

F. Preservation of rights-management information

Digital copyrighted files often have embedded rights-management information, which indicates who holds the copyright and how the content may be used. OSPs and others who use the work sometimes strip out such information,[206] which is unlawful under Section 1202 of the Copyright Act. But to obtain redress, a rightsholder must demonstrate both that the OSP or other entity: 1) intentionally removed the rights-management information or disseminated the copyrighted work with knowledge that the rights-management information had been removed, and 2) did so with knowledge that its actions would facilitate infringement.[207] In practice, this section has been difficult to enforce, because the second requirement has proven a very high bar.

For example, in *Stevens v. CoreLogic, Inc.*,[208] CoreLogic's software removed rights-management information from the photographs of two professional real-estate photographers when it compressed

---

[204] *See* McCoy, *supra* note 197, at 4 ("Our internal data shows us that site blocking is very effective at cutting traffic to pirate domains – meaning that an order applicable to the main access providers in a given country reduces traffic to a targeted domain by 70% on average and can be as high as 80-90% in some countries. That domain-specific impact is very clear and sustained over time. It becomes even more durable if the remedy specifies the underlying site, rather than just one or a few of the many domain names the site may use at any given time (this is the case in the UK, for example)."); Beard et al., *supra* note 116 (observing that site blocking has helped to curb digital piracy) (citing Brett Danaher, Michael D. Smith, and Raul Telang, *Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior*, WORKING PAPER (Apr. 18, 2016), http://ssrn.com/abstract=2766795; *Site Blocking Efficacy in Portugal: September 2015 to October 2016*, INCOPRO (May 2017), *available at* http://www.incoproip.com/wp- content/uploads/2017/07/Site-Blocking-and-Piracy-Landscape-in-Portugal-FINAL.pdf; *Site Blocking Efficacy Study: United Kingdom*, INCOPRO (Nov. 13, 2014), *available at* http://auscreenassociation.film/uploads/reports/Incopro_Site_Blocking_Efficacy_Study-UK.pdf; *Site Blocking in the World*, MOTION PICTURE ASSOCIATION (October 2015), *available at* http://www.mpa-i.org/wp-content/uploads/2016/02/Site-Blocking-October-2015.pdf; Nigel Cory, *How Website Blocking is Curbing Digital Piracy Without "Breaking the Internet,"* INFORMATION TECHNOLOGY & INNOVATION FOUNDATION (August 2016), *available at* https://www.researchgate.net/publication/333292640_How_Website_Blocking_Is_Curbing_Digital_Piracy_Without_Breaking_the_Internet; T. Randolph Beard, et al., *supra* note 117.

[205] Brett Danaher, Michael D. Smith & Rahul Telang, *Copyright Enforcement in Digital Age: Emprical Evidence and Policy Implications*, 60 COMM'CNS ACM 2, 11 (2017).

[206] A frequent reason for violating this provision appears to be simple error. For example, in *Stevens v. CoreLogic*, No. 16-56089 (9th Cir., Aug. 6, 2018) (Order and Amended Opinion), the defendants employed standard software libraries that did not adequately read and retain embedded metadata in photos, giving rise to a claim under Section 1202.

[207] *See* 17 U.S.C. § 1202(b) (making it unlawful for someone to "intentionally remove or alter any copyright management information" or to distribute or perform a copyrighted work "knowing that copyright management information has been removed or altered," if that person also knows or has reasonable grounds to know that doing so "will induce, enable, facilitate, or conceal an infringement of any right under this title.").

[208] *Stevens v. CoreLogic*, No. 16-56089 (9th Cir. 2018).

them for uploading to the Multiple Listing Service database.[209] The photographers, alleging that this might have led to unauthorized use of their photographs, sued under Section 1202.[210] The court upheld summary judgment for CoreLogic, on grounds that there was no evidence CoreLogic knew or had reason to know its actions would "induce, enable, facilitate, or conceal" infringement.[211] Similarly, in *Philpot v. AlterNet Media Inc.*,[212] photographer Larry Philpot alleged that AlterNet posted on its Facebook page a copyrighted photograph he took of Willie Nelson, and that it did not include the associated rights-management information.[213] The court granted AlterNet's motion to dismiss on grounds that Philpot failed to plead facts showing that AlterNet knew or had reason to know that removal of the rights-management information would induce, enable, facilitate, or conceal an infringement.[214]

The lack of accurate rights-management information makes it harder for copyright holders to enforce their rights, as well as for individuals willing to license content to determine whom to approach to do so. Consequently, anyone disseminating the copyrighted work, including OSPs that may monetize the content through advertising or other means, should have an obligation to ensure that rights-management information included by a copyright holder remains intact and accurate. The concern here is not that the entity may be infringing the copyright or that there has been some intent to cause harm (although both may be true in some cases), but that the entity's carelessness increases the likelihood that someone else will use the work without the copyright holder's authorization. Consequently, Congress should consider amending Section 1202 to make it unlawful to negligently, recklessly, or knowingly remove rights-management information, or to negligently, recklessly, or knowingly disseminate a copyrighted work without that rights-management information, regardless of whether there was an intent to facilitate infringement.

CONCLUSION

Revising the Copyright Act as described above would encourage OSPs both to prevent initial infringement and to more effectively curtail ongoing or repeat infringement. OSPs could decline to implement these content-protection requirements, but the consequence would be losing the safe harbors and becoming subject to the ordinary standards of copyright liability. OSPs also might more widely choose to license copyrighted works that are likely to appear on their platforms. That would

---

[209] *Id.* at 7.

[210] *Id.* at 9.

[211] *Id.* at 16-17.

[212] No. 18-cv-04479-TSH (N.D. Cal., Nov. 30, 2018).

[213] *Id.*

[214] *Id.*

benefit copyright holders and Internet consumers alike. The providers themselves might even find it leads to increased use of their service—as well as increased profits.

Ultimately, however, it is important to advance copyright reforms that take seriously both the constraints on OSPs as well as the real harms that the failures of Section 512 have caused rightsholders for more than two decades. Real reform can be accomplished in a way that preserves both the benefits of a free and open Internet, as well as healthy legal protection for intellectual-property rights.

At the same time, it is important to be cognizant that effective reforms must move through a political process that can be challenging. What is set forth in this paper is a vision of what comprehensive reform would look like. But, short of a full reform, there are select measures proposed above that we believe could, even standing on their own, provide significant benefit. Foremost among these would be the expanded use of no-fault injunctions in the United States. As we note above in Section V(e), no-fault injunctions have been successfully employed around the world in a way that protects both the interests of copyright holders, as well as the interests of OSPs and private citizens. Moreover, we believe that a reform that facilitates a no-fault injunctive regime would go very far in controlling the most egregious forms of organized piracy.