U.S. Copyright Office

Section 512 Study
[Docket No. 2015–7]

Comments of Annemarie Bridy and Daphne Keller

March 30, 2016

These comments are responsive to the following questions in the Notice of Inquiry: 1–5, 9, 10, 12, 15, 16, 17, 19, 20, 23, and 29. They include two Appendices: A (submitted in partial response to Question 15) and B (submitted in partial response to Questions 16 and 29).

General Effectiveness of the Safe Harbors

1. Are the section 512 safe harbors working as Congress intended?

Section 512 of the Copyright Act has been a successful and durable legislative achievement, one that has helped to promote unprecedented economic growth and diversity in user expression on the Internet while simultaneously providing copyright owners with efficient and effective procedures for remedying infringements of their protected content. In the "Online Copyright Infringement Liability Limitation Act" (Title II of the Digital Millennium Copyright Act (the "DMCA"), now codified at 17 U.S.C. § 512), Congress attempted to strike a balance among the rights and obligations of three separate constituencies, each holding substantial, and often conflicting, interests in regard to the distribution of copyright-protected works on the Internet: (1) copyright owners, fearing massive infringement of their protected works;[1] (2) online service providers, concerned with uncertain and potentially astronomical liability under ordinary principles of direct and secondary copyright liability;[2] and (3) Internet users, seeking to partake of and participate in a growing Internet filled with content "as diverse as human thought."[3]

The third group, Internet users, often falls out of the public DMCA discussion. But of course, the DMCA does not affect only the YouTubes, Viacoms, and isoHunts of the world. It

[1] *See* S. REP. NO. 105–190, at 8 (1998).

[2] *See id.* at 7 ("[W]ithout clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet.").

[3] Reno v. Am. Civil Liberties Union, 521 U.S. 844, 870 (1997) (internal quotation marks and citations omitted).

affects ordinary Internet users, too. The operator of a small business that customers find through Google or Yelp search results, the professional artist who promotes her paintings through Facebook, and the student looking for affordable books on eBay or Amazon suffer real harms when legal content is removed.

Small intermediaries are an important part of the picture as well. DMCA processing burdens that are tolerable for prosperous companies may pose a greater challenge for more modest ones, and may meaningfully affect their economic viability. DMCA processing by smaller or less well-funded OSPs can be different in ways that affect users, as well. Providing effective checks against groundless removal requests costs time and money. For a local news site that hosts a user forum, a small ISP, or a social media startup, meaningful legal review of removal requests to provide these checks may simply not be affordable.

Since the DMCA was enacted, the scale of online piracy has increased, and with it the number of legitimate DMCA requests—the bulk of them going from large copyright owners to large OSPs. It is important to bear in mind, however, that legions of ordinary people sharing their own original content online have always been the lifeblood of the Internet. The same is true of the small online businesses trying to respect copyright law while protecting their users. The DMCA was drafted to protect these people and small businesses, and it should continue to do so, even in the current era of entertainment conglomerates and social media juggernauts.

The legislative history of the DMCA frames the statute as a means of ensuring the continued global growth of the Internet.[4] To facilitate that goal, the statute was crafted to minimize obstacles to growth for both content providers, who would not expand the digital distribution of their works without assurances that they would be protected from "massive piracy," and service providers,[5] who would not expand their sites and networks without assurances that they would be protected from massive liability for copyright infringement.[6] In

[4] *See* S. REP. NO.105-190, at 1–2 (1998) ("The 'Digital Millennium Copyright Act of 1998' is designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education in the digital age.").

[5] In the statute, the term "service provider" is defined broadly to include both providers of Internet access (ISPs) and providers of online services. *See* 17 U.S.C. § 512(k).

[6] *See id.* at 8 ("Due 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. . . . At the same time, without clarification

light of the legislative history's focus on promoting growth in both content and services, the DMCA can be understood as a mechanism for simultaneously scaling up online copyright enforcement and scaling back online copyright liability—a unified solution designed to give rights owners the security necessary to expand content distribution and service providers the security necessary to expand online applications and network infrastructure.[7] Website operators and other providers of innovative online services have a clear and straightforward set of ground rules to follow, allowing them to conform their operations to the law and, thereby, avoid the specter of potentially crushing liability. At the same time, copyright owners, through the notice-and-takedown process spelled out in section 512(c), have simple and cost-effective means to curtail large numbers of unauthorized and infringing uses of their protected expression.

Measured against the Congressional goal of promoting the global growth of the Internet, section 512 has been dramatically successful. In 1998, the year of the DMCA's enactment, there were just 147 million Internet users worldwide.[8] In the United States, fewer than half of adults (41%) were online.[9] In 2015, after 17 years of unabated growth and infrastructure investment, there were over 3.2 billion users worldwide, of whom 2 billion were from developing countries.[10] Between 2000 and 2015, the number of people using the Internet globally grew by over 800%.[11] In 2014, the number of American adults online was 87%—more than double what it had been in 1998.[12] These impressive statistics are attributable to an innovation-promoting regulatory environment of which the DMCA safe harbors have been and remain a critical foundation.

As the Internet has grown and thrived, so, too, have the copyright industries, which have successfully adapted their business models to meet robust consumer demand for music and films distributed online in digital formats. According to the International Federation for the Phonographic Industry (IFPI), global revenue from digital music sales was $6.85 billion in 2015,

---

of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet.").

[7] Annemarie Bridy, *Is Online Copyright Enforcement Scalable*, 13 VAND. J. ENT. & TECH. L. 695 (2011).

[8] Miniwatts Marketing Group, Internet World Stats: Usage and Population Statistics, Feb. 15, 2016.

[9] Susannah Fox, *The Internet Circa 1998*, Pew Research Center, June 21, 2007.

[10] International Telecommunications Union (ITU), ICT Facts & Figures, May 2015.

[11] Miniwatts Marketing Group, *supra* note 8.

[12] Susannah Fox and Lee Rainie, *The Web at 25 in the U.S.*, Pew Research Center, Feb. 27, 2014.

which represented growth of 6.9% over the previous year.[13] For the first time, digital sales and sales in physical formats contributed equal shares of revenue.[14] If the music industry stumbled in its initial transition to online distribution, it has since returned to a very sure footing. According to Sony Music's Chairman Edgar Berger, "the industry is performing remarkably well," ably managing simultaneous transitions from physical to digital, download to streaming, and PC to mobile.[15] Metrics from the movie industry suggest a parallel evolution and growth, with business models shifting to satisfy the public's increasing preference for on-demand, over-the-top (OTT) video. The MPAA reported $35.6 billion in online video views around the world during the first quarter of 2014.[16] A market study it commissioned in 2014 projected that electronic home video revenues would double between 2014 and 2018, from $8.5 billion to $17 billion.[17] Across these two major copyright industries, the numbers are healthy, and the future—by their own reports—looks very bright.

Almost twenty years after its enactment, section 512 has proven to be resilient in the face of the Internet's evolving culture and technology. On the whole, it has done what Congress intended, encouraging growth in authorized online distribution of copyrighted works and in technologies that make such distribution both possible and profitable. The cooperative copyright enforcement that section 512 facilitates is not perfect, but its balance between the interests of copyright holders and OSPs is fair and workable. The outcome of the DMCA's balancing for Internet users is a more complicated story. Overall, however, the pragmatic balancing of interests accomplished by section 512 has allowed copyright owners, OSPs, and the American public all to share in the fruits of the Internet's cultural and commercial flourishing.

2. Have the courts properly construed the entities and activities covered by the section 512 safe harbors?

The entities covered by the section 512 safe harbors are determined by the activities they undertake to provide services to Internet users. The safe harbors cover four categories of network activity: transmission and routing; system caching; storage and activities incidental to storage;

---

[13] IFPI, Digital Music Report 2015, at 5.

[14] *Id.* at 6.

[15] *Id.* at 7.

[16] Howard Gantman, *A Remarkable Story of Digital Home Entertainment Growth*, MPAA POLICY FOCUS, June 16, 2014.

[17] *Id.*

and linking.[18] These covered activities are necessary for the Internet to function as a global, digital "network of networks;" all are mission-critical for public access to the Internet and for public participation in the diverse, vibrant culture of peer production and communication that the Internet has enabled.

As the Internet has evolved, the range of services and platforms available to users has greatly expanded, requiring courts to interpret the scope of the safe harbors in light of new technological developments. The covered activities in section 512 have remained, however, the essential technical foundation for all Internet services and platforms—from the news groups and BBSs of the Internet's early days, to the social media/sharing services of Web 2.0, to today's fast-developing Internet of Things. Courts deciding cases involving new Internet technologies and the scope of the safe harbors have for the most part done so with careful regard for the statutory text, the overall architecture of the safe harbor framework, and the policy goals underlying the DMCA.

One of the more controversial questions of scope with respect to the safe harbors relates to the range of activities encompassed by section 512(c)'s limitation of liability for infringements occurring "by reason of" a user's storage of material on an OSP's system.[19] This issue was exhaustively briefed by parties and amici in two significant cases—*Universal Music Group v. Shelter Capital Partners*[20] in the Ninth Circuit and *Viacom International, Inc. v. YouTube, Inc.*[21] in the Second Circuit. The plaintiffs in these cases argued for a narrow interpretation of the scope of the section 512(c) safe harbor, essentially drawing a distinction extrinsic to the statutory text between "passive" and "active" hosting services. Under their reasoning, passive hosts (e.g., cyberlockers) that do nothing more than store material for users should be covered by the safe harbor, while active hosts (e.g., video-sharing services like YouTube and Vimeo) whose systems enable users to view the material they and other users have stored should fall outside the

[18] 17 U.S.C. §§ 512 (a)–(d).

[19] *See* 17 U.S.C. § 512(c) (providing that "[a] service provider shall not be liable…for infringement of copyright *by reason of* the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider") (emphasis added).

[20] 718 F.3d 1006 (9th Cir. 2013).

[21] 676 F.3d 19 (2d Cir. 2012).

DMCA's protections.[22] European courts following reasoning similar to this have generated great uncertainty, risk, and reduced investment in Internet platforms.[23] For sound reasons grounded in statutory text, statutory architecture, and public policy, courts in the United States have univocally rejected this reasoning.[24]

The Ninth Circuit in *UMG Recordings* provided a thorough and well-reasoned analysis of the storage safe harbor's proper scope. Among several other justifications for adopting a broader interpretation of the safe harbor than UMG wanted, the court pointed out that the statute presupposes that storage providers will give users access to the materials that they and other users store.[25] The statute, after all, contemplates that providers will "remove, *or disable access to*" infringing material when they learn about it.[26] The court also noted that even the most passive providers, web hosts—which UMG argued *should* fall within the ambit of the safe harbor—operate by making the websites they store accessible to and viewable by the public.[27] To make websites viewable, web hosts routinely copy their content and transmit it to the browsers of Internet users.[28] Other types of storage providers, for example, those that operate video-sharing platforms, engage in similar automated technical processes that facilitate user access to stored material. These processes include transcoding user-uploaded files into different

---

[22] *See* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1015-16 (9th Cir. 2013) (summarizing UMG's argument that the automatic processes undertaken to facilitate public access to user-uploaded videos do not fall within the statute's definition of "storage").

[23] For example, an Estonian ruling later approved by the European Court of Human Rights held a news portal liable for hosted user comments, and ineligible for intermediary safe harbors, because it encouraged user comments, drew additional traffic and advertising revenue from hosting comments, permitted anonymous speech, and had the ability and right to delete comments. Delfi v. Estonia, (2015) Eur. Ct. H.R. 64659/09. An Italian court—in a ruling recently reversed—denied safe harbors for Yahoo's video-sharing platform because the site indexed user-generated videos, offered a reporting mechanism for inappropriate content, and was indemnified and granted display rights by users in its Terms of Service. Yahoo v. RTI, Corte app., 2015, n.3821/2011; *see also* Sara Balice, *Yahoo! Wins against RTI: Limited Liability for Hosting Providers*, IPT Italy Blog, Feb. 17, 2015, http://blogs.dlapiper.com/iptitaly/?p=56364. For a comparison of technical investment and legal regimes in the United States and other countries, see Anupam Chander, *How Law Made Silicon Valley*, 63 Emory L.J. 638 (2014).

[24] *See id.* at 1016 ("We agree that the phrase 'by reason of the storage at the direction of the user' is broader causal language than UMG contends….We hold that the language and structure of the statute, as well as the legislative intent that motivated its enactment, clarify that § 512(c) encompasses the access-facilitating processes that automatically occur when a user uploads a video to Veoh."); Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 39 (2d Cir. 2012) (holding that it "would eviscerate the protection afforded to service providers by § 512(c)" to exclude YouTube's transcoding, playback, and 'related video' functions, given that the functions are "performed for the purpose of facilitating access to user-stored material").

[25] *UMG Recordings, Inc.*, 718 F.3d at 1017.

[26] *See id.* at 1018 (citing 17 U.S.C. § 512(c)(1)(A)(iii), (c)(1)(C) & (c)(3)(A)(iii)).

[27] *Id.*

[28] *Id.*

formats, extracting metadata from those files, streaming the transcoded files to users, and making suggestions to users about additional files to view.[29] Such automated, access-facilitating functions, which go beyond mere storage, implicate the rights of copyright owners and are therefore, as Congress contemplated, a potential source of infringement that occurs "by reason of" a user's storage of materials on a provider's system. Because they give rise to storage-related liability, these storage-related activities are covered by the safe harbor in section 512(c).

Moreover, the court in *UMG Recordings* said, the only way a copyright owner can know of infringing material stored on a provider's system, and thus initiate the notice and takedown protocol at the heart of section 512(c), is if the copyright owner is able to view (i.e., access) that stored material.[30] Taking these and other considerations into account, including the DMCA's inclusive definition of "service provider" in section 512(k)(1)(B), the Ninth Circuit in *UMG Recordings* readily concluded that the only reasonable reading of section 512(c) is one that includes in the scope of the safe harbor not only storage but all of the access-facilitating functions that are incidental to storage.[31] The Second Circuit in *Viacom* agreed.[32]

If the safe harbor in section 512(c) had been limited as the plaintiffs in *Viacom* and *UMG Recordings* sought, providers would not be protected for performing the basic technical functions that allow users to access and view the materials they store. Without protection of functions ancillary to storage, the storage safe harbor would be so narrow in scope as to be effectively useless to any provider that does more than provide the most basic back-up storage service to users. As the courts have recognized, that cannot be what Congress intended when it enacted the DMCA with the goal of increasing the diversity and number of online services.[33] If not for the inclusion of access-facilitating processes in the storage safe harbor, popular video sharing

---

[29] *See id.* at 1012 (describing the various steps in Veoh's system for processing user-uploaded videos to make them available for viewing); *Viacom*, 676 F.3d at 39-40 (same).

[30] *See id.* ("Indeed, it is not clear how copyright holders could even discover infringing materials on service providers' sites to notify them as the protocol dictates if § 512(c) did not contemplate that there would be access to the materials.").

[31] *See id.* at 1016 ("[T]he language and structure of the statute, as well as the legislative intent that motivated its enactment, clarify that § 512(c) encompasses the access-facilitating processes that automatically occur when a user uploads a video.").

[32] *See Viacom*, 676 F.3d at 39 ("[T]he structure and language of OCILLA indicate that service providers seeking safe harbor under [§] 512(c) are not limited to merely storing material.").

[33] *See* Flava Works, Inc. v. Gunter, 689 F.3d 754, 758 (7th Cir. 2012) (stating that "Congress wanted to make the safe harbor as capacious as possible").

platforms like YouTube and Vimeo, and photo sharing services like Flickr and Photobucket would be exposed to such profound copyright liability that they simply could not afford to operate. That outcome would be antithetical to the policies underlying the safe harbors.

3. How have section 512's limitations on liability for online service providers impacted the growth and development of online services?

Along with its companion provision in federal law, 47 U.S.C. § 230,[34] which provides service providers with a similar safe harbor from claims arising from their users' activities, the DMCA has fueled extraordinary and unprecedented growth in innovative Internet services based entirely on user expression. This explosion of participatory online services and applications has, in turn, fueled the growth of the Internet itself as a truly global communications platform and a powerful tool for grassroots democratic movements around the world.[35]

Thousands of Internet businesses, including both household names (e.g., Wikipedia, Facebook, Twitter, YouTube, Blogger, Reddit, WordPress, Tumblr, Flickr) and newer entrants (e.g., Instagram, Twitch, Vine, Periscope, Meerkat) have emerged over the past fifteen years sharing one common characteristic: they provide virtually no content of their own (copyrightable or otherwise), but rely instead entirely on their users to make the sites valuable, engaging, and attractive for other users. Members of the public have responded to the expressive opportunities these services provide in truly breathtaking numbers.[36]

It is difficult, if not impossible, to imagine this development in the absence of strong DMCA safe harbors. It is no coincidence that all of the service providers listed in the preceding paragraph are based here in the United States, where Congress had the foresight in the early days of the Internet to understand that unlimited or uncertain service provider liability for third-party

---

[34] 47 U.S.C. § 230(c)(1) protects "provider[s] . . . [of] interactive computer service(s)" against claims arising from "any information provided by another information content provider," and has been applied to immunize service providers against a wide range of federal and state law claims. See, e.g., Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008); Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997). By its express terms, however, § 230 does not encompass any intellectual property claims, *see* 47 U.S.C. § 230(e)(2)—precisely the gap that Congress filled in 1998 with Title II of the DMCA.

[35] *See, e.g.*, Clay Shirky, *The Political Power of Social Media: Technology, the Public Sphere, and Political Change*, FOREIGN AFFAIRS, Jan./Feb. 2011.

[36] For example, YouTube and Facebook each have over 1 billion users. YouTube, Statistics, https://www.youtube.com/yt/press/statistics.html (last visited Mar. 3, 2016); Facebook, Stats, http://newsroom.fb.com/company-info/ (last visited Mar. 3, 2016). Reddit has 231 million. Reddit, By the Numbers: 60+ Amazing Reddit Statistics, http://expandedramblings.com/index.php/reddit-stats/ (last visited Mar. 3, 2016). Twitter has 320 million. Twitter, Company Facts, https://about.twitter.com/company (last visited Mar. 3, 2016).

conduct would have drastic, negative consequences for the realization of the Internet's full economic and cultural potential.[37] Without the limitations on liability provided by the DMCA's safe harbors, the legal exposure for a service provider relying upon vast numbers of users freely exchanging content with one another would be entirely unmanageable; a business built on such a foundation could not attract financing in any rational marketplace—or provide the new distribution channels that are now a significant revenue source for copyright owners.[38]

4. How have section 512's limitations on liability for online service providers impacted the protection and value of copyrighted works, including licensing markets for such works?

The DMCA's limitations on liability have made it possible for technology companies to invest in Internet platforms that have revolutionized content distribution. The evolution of these platforms has been challenging but ultimately lucrative for copyright owners, who are now effectively channeling content-hungry consumers to an increasing array of licensed services for online music and video. As copyright owners have created attractive and affordably priced legal options that respond to consumers' desire for large catalogs of on-demand content, piracy levels are decreasing; over the last dozen or so years, the percentage of North American fixed Internet traffic attributable to file sharing has dropped sharply from 60% to 5%.[39]

Professional content creators and copyright owners are rapidly growing their licensing markets through subscription streaming services on new and existing distribution platforms. Amateur creators and performers are also finding monetization opportunities online, through revenue-sharing programs with DMCA-enabled, user-driven platforms like YouTube and

---

[37] *See* S. REP. NO. 105–190, *supra* note 1, at 36 (noting that the "liability of online service providers and Internet access providers for copyright infringements that take place in the online environment has been a controversial issue," and that Title II of the DMCA was designed to "provide[ ] greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities").

[38] A copyright holder is entitled to "an award of statutory damages for all infringements . . . [of] any one work, . . . in a sum of not less than $750 or more than $30,000 as the court considers just," which can be increased at the court's discretion to $150,000 in cases involving "willful infringement." *See* 17 U.S.C. § 504(c)(1), (2). At the scale and volume at which many other user-generated content websites are operating, the potential infringement liability for even a day's worth of activity can mount into the millions or billions of dollars.

[39] According to the global broadband analytics firm Sandvine, "[f]ile sharing continues to disappear from many fixed access networks across the globe as Real-Time Entertainment options that are providing subscribers a wealth of content at reasonable prices launch in new countries." Sandvine, Global Internet Phenomena Report (2H 2013), at 5. When Sandvine published its first Global Internet Phenomena Report, file sharing accounted for over 60% of total fixed daily Internet traffic in North America. *Id.* In 2013, file sharing accounted for less than 10% of total daily traffic in North America. *Id.* Between the second half of 2013 and December 2015, file-sharing in North America dropped over 50%—from around 10% of peak, fixed access traffic to around 5%. Sandvine, Global Internet Phenomena: Africa, Middle East & North America (December 2015), at 2.

Vimeo. These partnership programs, some of which generate revenue by running ads against content and some of which charge viewers per stream or per channel, represent a form of content licensing that provides significant income to creators of all sizes.

According to the IFPI, subscription streaming services like Spotify are the music industry's fastest growing revenue source, increasing by 39% in 2014.[40] In 2014, the number of paying subscribers worldwide increased over 45% to a total of 41 million—five times the total in 2010.[41] For the five-year period ending in 2014, revenue to the major labels from subscriptions grew more than six-fold to $1.6 billion.[42] Major players like YouTube and Apple, which recently launched subscription services, will drive those numbers even higher over the coming years, with the market shifting from less valuable "freemium" models to fully paid subscriptions.

The growth of subscription streaming services in the music industry is mirrored in the film and television industries, where Netflix, Hulu, Amazon Prime and iTunes continue to grow, in addition to standalone offerings from cable networks like Showtime and HBO. The MPAA reports that there are now more than 450 online services available globally, offering legitimate, licensed full-length movies and television shows.[43] Over a hundred of these paid, legal services are available to U.S. viewers.[44]

At the same time as large copyright owners are rapidly expanding their licensing programs to capture new markets and market segments, smaller-scale creators have found on DMCA-protected platforms like YouTube and Vimeo a lucrative outlet for *their* creative, copyrighted output. Some of these "DIY" creators are earning substantial incomes from paid or ad-supported streaming videos. For example, the number of YouTube channels earning six figures grew 50% last year.[45] And the most-followed "game casters" on Amazon's wildly popular Twitch.tv are also drawing six-figure incomes.[46]

---

[40] IFPI, Digital Music Report 2015, at 15.

[41] *Id.*

[42] *Id.*

[43] Howard Gantman, *The Number of Legal Online Services for Movies and TV Shows Around the Globe Keeps Climbing*, MPAA POLICY FOCUS, July 30, 2015.

[44] *Id.*

[45] YouTube, Statistics, https://www.youtube.com/yt/press/statistics.html (last visited Mar. 8, 2016).

[46] *See* Cameron Keng, *Online Streaming and Professional Gaming Is a $300,000 Career Choice*, FORBES, Apr. 21, 2014.

In 2015, *Forbes* published a list of YouTube's top-earners, including Swedish vlogger Felix Kjellberg (a.k.a. Pew Die Pie), who earned $12 million that year.[47] While YouTube's top earners are only a small minority of the platform's billion users, they represent a cross-section of the enormous variety of creative content available on the platform. The list includes a dancing violinist, comedians, singers, pranksters, a beauty entrepreneur, and a pastry chef, many of whom are branching out into traditional media, securing deals for movies, television shows, and books.[48] The content-sharing platforms that allow these diverse, smaller creators to monetize their expression online, alongside the professional content offered by corporate copyright owners, could not exist without the DMCA safe harbors.

5. Do the section 512 safe harbors strike the correct balance between copyright owners and online service providers?

This question is closely related to Question 1, given that Congress designed and intended the safe harbors to "work" by balancing the interests of copyright owners, online service providers, and users. It is important to remember when assessing the success of the safe harbors that user interests are a vital part of the balancing the safe harbors were intended to accomplish. Please refer to our responses to Questions 12, 16, and 17 below for a full discussion of the DMCA's impacts on users, their creativity, and their freedom of expression. Our response to this question will focus at a higher level on the architecture of the safe harbors and their overall success in balancing the competing interests of the three stakeholder groups that Congress intended them to benefit.

Section 512 balances the competing interests of copyright owners, OSPs, and users in a nuanced enforcement regime that requires each group to invest time and resources to ensure that unlawful content is removed from circulation and lawful content remains available online. While section 512 does not guarantee perfect enforcement, it has successfully protected the interests of copyright owners through their difficult transition from brick-and-mortar to online distribution, and it has successfully protected user-generated content platforms in the early stages of their development, when success is uncertain and resources are scarce.

[47] *See* Madeline Berg, *The World's Highest-Paid YouTube Stars 2015*, FORBES, Oct. 14, 2015.

[48] *See id.*

The DMCA safe harbors provide copyright owners with a direct and efficient remedy against infringing conduct on the massive scale made possible by participatory media platforms. Through the notice-and-takedown procedures set forth in section 512(c), billions of infringing works have been removed from circulation over the Internet through a process that avoids costly and time-consuming adjudication while simultaneously providing due consideration of the interests of all parties involved.[49]

Despite initial resistance from both OSPs and copyright owners, the two groups have adapted quite well over the last 18 years to doing business within the parameters defined by the DMCA's notice-and-takedown system.[50] "Trusted submitter" programs on larger platforms (including online search) have allowed the system to automate and scale for corporate copyright owners whose works account for the greatest share of infringing activity online.[51] For smaller copyright owners, the section 512(c) notice process can be initiated on the most popular content-sharing platforms with the click of a mouse following completion of a simple, fillable online form. YouTube, Facebook, Scribd, and Pinterest all offer standardized online notice forms that can be submitted electronically.[52] The forms are structured to comply with the requirements of section 512(c)(3)(A), so that even copyright owners lacking counsel or legal sophistication can easily seek redress. On the Internet's most popular content-sharing sites, the notice-and-takedown system has come to operate as a well-oiled, always-on copyright enforcement machine.

In addition to protecting copyright owners and OSPs, the DMCA also protects Internet users. It is important to remember that they, too, are part of the balance that Congress intended to strike in the DMCA safe harbors. Sections 512(f) and (g) indicate deep Congressional concern

---

[49] *See* Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 524 (S.D.N.Y. 2010) (noting that "the present case shows that the DMCA notification regime works efficiently: when Viacom over a period of months accumulated some 100,000 videos and then sent one mass takedown notice on February 2, 2007, by the next business day YouTube had removed virtually all of them"), *aff'd in part and vacated in part*, 676 F.3d 19 (2d Cir. 2012).

[50] *See* Jerome H. Reichman, Graeme B. Dinwoodie, & Pamela Samuelson, *A Reverse Notice and Takedown Regime to Enable Public Interest Uses of Technically Protected Copyrighted Works*, 22 BERKELEY TECH. L.J. 981, 994 (2007) (concluding that "the past decade of experience with the DMCA notice and takedown regime suggests that a relatively balanced and workable solution to this particular dual-use technology problem has been found.").

[51] *See, e.g.*, Fred von Lohmann, Google's DMCA Notice-and-Takedown Tools, PTO Multistakeholder Meeting, May 2014, http://www.uspto.gov/ip/global/copyrights/Google.pdf (describing the trusted submitter program for Google products—Search, Picasa, Blogger, and YouTube)

[52] *See, e.g.*, Pinterest Copyright Infringement Notification, http://www.pinterest.com/about/copyright/dmca/.

with the implications of the notice-and-takedown system for ordinary Internet users, who could easily find themselves caught between overly-assertive copyright owners on the one hand and overly-risk-averse OSPs on the other.[53]

Section 512(g) protects OSPs against claims arising from their "good faith disabling of access to, or removal of, material or activity claimed to be infringing."[54] In the case of removals pursuant to the notice-and-takedown procedures, this protection applies *only* if the OSP has both provided notice of the removal to the users responsible for posting the material[55] and afforded those users an opportunity to provide a "counter notification" stating their "good faith belief that the material was removed or disabled as a result of mistake or misidentification."[56] If the OSP receives such a counter notification, it can invoke the safe harbor only if it (a) "promptly provides . . . a copy of the counter notification" to "the person who provided the [takedown] notification"[57] (*i.e.*, the copyright holder who initiated the takedown), and (b) "replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice,"[58] unless, in that intervening period, the copyright holder has informed the OSP that it has "filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network."[59] Finally, section 512(g) provides that OSPs that *replace* infringing material in compliance with the counter-notice, like those that *remove* infringing material in compliance with the original takedown notice, are not liable for any claims arising from that action.[60]

Section 512(f), for its part, is intended to ensure that all of the information being provided in this complex notice-and-counter-notice scheme is accurate and reliable. It imposes liability on anyone who "knowingly materially misrepresents… that material or activity is infringing" (in the

---

[53] *See* S. REP. NO.105–190, *supra* note 1, at 50 ("The put back procedures were added . . . to address . . . concerns . . . that other provisions of this title established strong incentives for service providers to take down material, but insufficient protections for third parties whose material would be taken down.").

[54] 17 U.S.C. § 512(g)(1).

[55] 17 U.S.C. § 512(g)(2)(A).

[56] 17 U.S.C. § 512(g)(3)(C).

[57] 17 U.S.C. § 512(g)(2)(B).

[58] 17 U.S.C. § 512(g)(2)(C).

[59] *Id.*

[60] *See* 17 U.S.C. § 512(g)(4) ("A service provider's compliance with the notification and counter-notification procedures set forth in § 512(g)(2) "shall not subject the service provider to liability for copyright infringement with respect to the material identified in the [takedown] notice provided under [§ 512(c)(1)(C)].").

copyright holder's takedown notice) or that "material or activity was removed or disabled by mistake or misidentification" (in the user's counter-notice).[61]

The overall scheme is carefully wrought and finely balanced. It contemplates a world in which copyright owners initiate infringement remediation through section 512(c) takedown notices, knowing that they will be responsible for any material misrepresentations contained therein.[62] OSPs, relying on the information provided in the takedown notice, may remove the material so identified and inform the users responsible for uploading the material that they have done so. If the OSP receives a counter-notice from a user (who is likewise subject to the section 512(f) prohibition on material misrepresentations) informing the OSP that the user has a good faith belief that the material is *not* infringing, the OSP informs the copyright holder of the counter-notice and restores the material in question, unless the copyright holder chooses to file suit to protect its rights. In that case, the OSP leaves the disputed material offline.

The goal Congress was pursuing in sections 512(f) and (g) is clear: Infringing material should be rapidly and permanently removed, but *non*-infringing material should remain available and accessible. Users and copyright owners are charged with acting in good faith in declaring works to be in one category or the other. If OSPs respond to notices and counter-notices within the parameters laid out by the statute, they are effectively insulated from having to adjudicate what are, in the end, disputes between copyright owners and users. By carrying out their duties, OSPs can be assured of protection against claims that they are infringing copyright (when they replace material that has been removed) and against claims that they are violating the contractual rights of their users (when they remove material at the direction of copyright owners).

It is virtually impossible for any law, no matter how well crafted, to keep pace with rapid changes in computer and telecommunications technology. The growth of the Internet has disrupted the copyright system in ways that are still being revealed. Time has shown, however, that the equitable balancing of interests established in section 512 remains viable. Copyright owners, OSPs, and users continue to evolve in their attitudes and practices with respect to online copyrighted content. Online piracy is waning[63] with the expansion of innovative service

---

[61] 17 U.S.C. § 512(f).

[62] *See* Lenz v. Universal Music Group, 801 F.3d 1126 (9th Cir. 2015), *opinion amended and superseded on denial of reh'g*, ___ F.3d ___ (9th Cir. 2016).

[63] *See supra* note 39 and accompanying text.

offerings from copyright owners, who have come to embrace online distribution as a revenue opportunity instead of fearing it as an existential threat. Section 512 has provided a crucial foundation for the growth of the Internet and the development of innovative services for Internet users. It has allowed Web 2.0 startups to flourish, and it has spurred incumbent corporate copyright owners to imagine new ways of reaching audiences that are willing to pay in ever-increasing numbers for lawful, professionally developed content.

Notice-and-Takedown Process

9. Please address the role of both ''human'' and automated notice-and-takedown processes under section 512, including their respective feasibility, benefits, and limitations.

The DMCA moves literally billions of disputes about online speech out of courts and into the hands of private parties. Congress had good reason to create this privatized system of adjudication, given the sheer scale of online copyright infringement. Other effective choices are hard to imagine given current numbers. As discussed above in response to Question 5, the DMCA strikes a wise balance of rights and obligations between copyright owners and intermediaries. But it has meaningful and often underappreciated costs to Internet users. Malicious or erroneous over-removal silences legitimate speech. As discussed below in response to Question 12, this is no speculative harm; it happens all the time. And the due process rights that courts provide to an accused party are lost when private companies effectively adjudicate infringement accusations without that party's involvement.[64]

The DMCA's correctives for these problems were supposed to come from its procedural protections.[65] As discussed below in response to Questions 16 and 29, those protections have had mixed success. But one meaningful protection, historically, has come from the seriousness of lodging a DMCA complaint. A person signing a DMCA notice must state a good faith belief that

[64] Thoughtful assessments of Constitutional harms from this privatization of judicial function appear in several articles. *See, e.g.*, Jack Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296 (2014); Derek Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863 (2012); Seth Kreimer, *Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link*, 155 U. PENN. L. REV. 11 (2006).

[65] 17 U.S.C. 512(g); S. REP. NO. 105–190, *supra* note 1, at 50 ("The put back procedures were added as an amendment to this title in order to address the concerns of several members of the Committee that other provisions of this title established strong incentives for service providers to take down material, but insufficient protections for third parties whose material would be taken down.").

the use is not authorized, declare her authority to act under penalty of perjury, and risk damages for misrepresentation under section 512(f).[66]

That source of protection has not technically disappeared, but its value is largely lost when notices are generated not by a person, but by a machine. The rise of "robo-notices" moves the DMCA one step further away from "real" adjudication. This shift is happening for a compelling reason: Copyright owners' works are massively reproduced across the Internet, so they need a way to identify infringement and submit notices at scale. But taking a human accuser out of the equation comes at an obvious cost. Automated notices are notoriously flawed, often targeting content that has nothing to do with the copyrighted work. In a famous example, an agent of Columbia Pictures sent takedown notices for numerous Vimeo uploads—including the short film that originally inspired Columbia's *Pixels* movie—simply for having the word "pixels" in their names.[67] The rights of wrongly accused Internet users, and of those who would read or watch their work, suffer as a result.

The rise of automated notices without a corresponding fortification of users' rights and protections is troubling. Proposals to require intermediaries themselves to institute similar automated review, discussed in response to the next question, are even more so.

10. Does the notice-and-takedown process sufficiently address the reappearance of infringing material previously removed by a service provider in response to a notice? If not, what should be done to address this concern?

Although some copyright owners advocate interpretations of the DMCA that would require OSPs to be more proactive in their efforts to enforce third-party copyrights, the DMCA is quite clear that active monitoring for infringing content is not a burden that Congress saw fit to allocate to service providers when it balanced the need to make the Internet safe for copyright owners against the need to promote growth and innovation in online services. That allocative choice was reasonable in 1998, and it remains reasonable in 2016. The Internet has grown exponentially in size since the DMCA was enacted, but we should not forget that the problem of large-scale infringement was an expected development—and one that the safe harbors were specifically designed to manage.

[66] 17 U.S.C. 512(c)(3)(A) (detailing requirements for a DMCA notice).

[67] Michelle Starr, *Videos Taken Down From Vimeo For Using the Word 'Pixels,'* CNET, Aug. 9, 2015, http://www.cnet.com/news/videos-taken-down-from-vimeo-for-using-the-word-pixels/.

A "notice and staydown"—a.k.a. monitoring—requirement would radically alter the existing balance in the safe harbors. It would repeal section 512(m) and effectively impose a 24-7-365 monitoring obligation on all OSPs, no matter their size or available resources. Remaking the DMCA in such a way would shift almost the entire burden and cost of enforcement from copyright holders to OSPs. Such a change would be no mere adjustment to the DMCA's balance of burdens; it would be closer to a demolition of the DMCA's existing structure. Once a copyright owner identified a single appearance of a work on a platform, it would never again need to engage with DMCA processes for that work, except in the rare cases of counter-notice. From that point forward, the OSP would no longer just cooperate with the copyright owner, but effectively subsidize and replace it in the ongoing enforcement of its rights.

Whatever one thinks of this drastic shift in burden between intermediaries and copyright owners (often meaning between two large companies), the impact on Internet users could only be bad. Their expressive rights would be predictably compromised by both "human" and "automated" monitoring. Because of the clear prohibition in section 512(m), courts in the United States have not had reason to assess what intermediary monitoring would mean for the rights of Internet users. In other countries, however, high courts have expressed great concern. The European Court of Human Rights recently ruled that Hungary violated the European Convention's Article 10—the analog of the First Amendment—by requiring a host to monitor its users' comments for defamation.[68] The highest court of the EU has never accepted monitoring obligations for intermediaries, and cited concerns about users' rights to seek and impart information in overturning two injunctions that would have required automated filtering.[69] The highest courts of both Argentina and India reached similar conclusions in opinions that drew extensively on US law.[70]

[68] MTE v. Hungary, ECtHR 22947/13 (2016). The case distinguished defamatory content, for which monitoring was not permitted, from more damaging hate speech and threats of violence, for which an earlier case permitted monitoring obligations to be imposed on a news platform's comments forum.

[69] Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) [2011] ECR 2011:771 (Para. 52); Case C-360/10 SABAM v. Netlog [2012] ECHR 2012:85.

[70] Corte Suprema [Supreme Court of Argentina], Civil, Rodriguez M. Belen c/Google y Otro s/ daños y perjuicios, R.522.XLIX., Oct. 29, 2014; Supreme Court of India, Criminal, Shreya Singhal v. Union of India, No. 167/2012, Mar. 24, 2015.

The threat of over-removal under a monitoring regime would not arise solely from intermediaries' fear of liability. It would also stem from the near elimination of an important participant in the DMCA's well-choreographed dance: the copyright owner. Copyright owners are the people best able to identify infringement, and their judgment is key to the DMCA's balanced process. Without the copyright owner, an OSP that has once been notified of an infringement would thereafter act as prosecutor, judge, and executioner for all uses of the same work. Given that the copyright fair use analysis is highly contextual, treating all uses of a given work as presumptively unfair is problematic. Even complete copies of files can be fair use in some cases.[71] The task of making judgments in individual cases would at best fall to the OSP's employees, whose knowledge—for example, of authorization or of how much of a work has been borrowed—can only be poorer than the copyright owner's. At worst, and most plausible for large companies, even this inexpert human judgment would be replaced by a less discriminating filtering algorithm. With automated filtering, every step in assessing and deleting Americans' online speech would be handed off to software. Even when weighed against the substantial need for efficient copyright enforcement, the risk of algorithmically implemented over-removals is too great.

The sections below explore specific issues with "human" and "automated" monitoring regimes.

"Human" Monitoring

Content monitoring by OSP employees would inevitably be inaccurate. It is simply unrealistic to expect rank and file employees to identify infringing content without a significant error rate. This includes both false positives—removing lawful content—and false negatives—leaving infringing content up. Of course, liability concerns would give OSPs great economic incentive to err on the side of false positives and remove legal online speech. Studies show this problem exists already under notice and takedown, and it would only grow worse under a monitoring system.[72]

[71] *See, e.g.,* Online Policy Group v. Diebold, 337 F. Supp. 2d 1195 (N.D. Cal. 2004) (holding that it was fair use to post entire copies of company email messages).

[72] *See* response to Question 29 *infra.*

One obvious problem with OSP employee review is the difficulty identifying fair use—a task with which lawyers and judges struggle. Another is that employees who grew up in other countries may not recognize older movies or TV shows known to many Americans. But perhaps the most significant and under-recognized problem is that tech employees simply don't know about copyright owners' licensing and marketing operations. As the chief IP counsel of Etsy explained, she has no way to know "who's using licensed material in an appropriate way, and who has a license. . . . That's why the DMCA exists."[73]

The problem is vividly illustrated by DMCA notices made public in the course of *Viacom International, Inc. v. YouTube, Inc.*, in which Viacom identified numerous videos uploaded by its own marketing department as infringing.[74] As YouTube's chief counsel stated:

> For years, Viacom continuously and secretly uploaded its content to YouTube, even while publicly complaining about its presence there. It hired no fewer than 18 different marketing agencies to upload its content to the site. It deliberately "roughed up" the videos to make them look stolen or leaked. It opened YouTube accounts using phony email addresses. It even sent employees to Kinko's to upload clips from computers that couldn't be traced to Viacom. And in an effort to promote its own shows, as a matter of company policy Viacom routinely left up clips from shows that had been uploaded to YouTube by ordinary users.[75]

If a large copyright owner itself cannot identify which uses of its works are authorized, it makes little sense to expect those outside the company to know. Uncertainty about the licensing status of movie clips and other commercial content goes far beyond Viacom; it is a pervasive issue for platforms operating under the DMCA. But it is easy to predict what would happen if intermediaries bore the burden of finding infringing content, under threat of liability and

---

[73] Sarah Lai Stirland, *Etsy's Sarah Feingold on Small Business and Copyright Compliance*, PROJECT DISCO BLOG, July 23, 2014, *http://www.project-disco.org/intellectual-property/072314-etsys-sarah-feingold-small-business-copyright-compliance/#.VvbKNRIrJmA*.

[74] *See, e.g.*, Notice of Dismiss. of Specified Clips With Prejudice, *Viacom International, Inc., et al. v. YouTube, Inc., et al.*, 2010 WL 2532404 (S.D.N.Y 2010) (referring to the hundreds of video clips that Viacom had initially identified as "infringing" but which were subsequently withdrawn from the list of works in suit); Mem. in Supp. of Def.'s Mot. for Summ. J., Viacom Intern. Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, S.D.N.Y (Mar. 11 2010), *http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en/us/press/pdf/20100318_google_viacom_youtube_memorandum.pdf*.

[75] Zahavah Levine, *Broadcast Yourself*, YOUTUBE OFFICIAL BLOG, Mar. 18, 2010, *https://youtube.googleblog.com/2010/03/broadcast-yourself.html*.

statutory damages. Few would take the risk of leaving up potentially licensed, fair use, or public domain content. Erring on the side of removal would be the order of the day, and Americans' ability to share legal content online would suffer.

"Automated" Monitoring

Algorithmic monitoring poses similar risks of suppressing legal speech. Part of the problem comes from inevitable failures and inaccuracies of filtering technologies themselves. Such failures arise because algorithms lack human judgment and cannot adequately assess context. A content filter intended to find copyrighted images would not know when those images appear in a critical essay, for example, or be capable of assessing the four fair use factors.[76] An algorithm that could replace expert fair use analysis would be a marvel of technology.

Accidental filtering of legal information can also arise from purely technical errors, when algorithms misjudge whether one file is a copy of another. Developing monitoring tools that do not over-filter (remove more information than intended) or under-filter (remove less) is a significant, perhaps asymptotic technical challenge. Even YouTube's Content ID, the product of over 50,000 hours of engineering work and some 60 million dollars' investment by Google,[77] is routinely faulted by Internet users for misidentifying and removing lawful content.[78]

Requiring similarly Herculean monitoring efforts from smaller Internet intermediaries would have foreseeable consequences. Some would go out of business. Some would never attract investment and be able to launch in the first place. Both of these results would serve to entrench incumbent companies with existing, expensive (yet still-flawed) filtering tools. Some small companies would build whatever filters their skill and budget permitted—meaning significantly less accurate ones, with significantly more false positives. And some would move

---

[76] *See* 17 U.S.C. § 107 (setting forth the factors that must be considered when assessing fair use).

[77] *See Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intellectual Prop., & the Internet of the H. Comm on the Judiciary*, 113th Cong. 2 (2014) (statement of Katherine Oyama) (noting that "[w]hen YouTube became a part of Google, we really injected a huge amount of effort, so more than $60 million, more than 50,000 engineering hours went into building this system.")

[78] *See, e.g.*, Glen Hoban, *YouTube ContentID Fails*, MEDIUM, Jan. 7, 2015, https://medium.com/@glenhoban/youtube-content-id-fails-volume-i-6ae2c9ca570b#.57kvzho2v (reporting hundreds or thousands of erroneous ContentID matches for classical sound recordings); Mike Masnick, *How Google's ContentID System Fails at Fair Use & the Public Domain*, TECHDIRT, Aug. 8, 2012, https://www.techdirt.com/articles/20120808/12301619967/how-googles-contentid-system-fails-fair-use-public-domain.shtml.

back to the 1990s "walled garden" version of the Internet, accepting only monitored and curated content. The Internet's current array of open platforms for free expression, commerce, and public participation would look very different if monitoring users for copyright infringement were a condition for launch.

Proponents of monitoring requirements sometimes argue that voluntarily-developed tools such as YouTube's ContentID show that OSP's are capable of effective monitoring—and that this in turn is a reason the law should *require* them to monitor.[79] This reasoning is unsound on both pragmatic and policy grounds. As a reason to repeal section 512(m) and require all OSPs to monitor as best they can, it runs into the problems discussed above: decreased investment in new OSPs, clumsy monitoring efforts, and removal of users' lawful content. As a reason to impose monitoring requirements on individual companies that build duplicate-detection tools, it is equally problematic, because it would deter competitors from developing similar technologies. A platform would think long and hard before investing in the next ContentID if it knew that doing so would only lead to additional legal liabilities and obligations.

This is exactly the issue that Congress recognized in enacting the United States' other core intermediary liability law, the Communications Decency Act ("CDA").[80] That law responded to a 1990s case holding an OSP liable for user-generated defamation, on the basis of its failed undertaking to monitor for such content.[81] To preclude further rulings of this sort, Congress in CDA section 230 immunized OSPs' "private blocking and screening of offensive material."[82] As the CDA's Policy section states, the legislation served "to remove disincentives for the development and utilization of blocking and filtering technologies" by ensuring that such efforts would not increase an OSP's liability or subsequent obligations.[83] The same reasoning

---

[79] For example, one European plaintiff successfully argued that courts should compel Google to detect and suppress images in his case, because the company had already built a "filter [that] works very well when it comes to child pornography." *See, e.g.*, Susanne Amann and Isabell Hülsen, *Max Mosley: Google Is So 'Arrogant They Do Whatever They Like,'* SPIEGEL ONLINE, Jan. 29, 2014, http://www.spiegel.de/international/zeitgeist/max-mosley-discusses-his-fight-against-google-a-946180.html. That case, which later settled, involved a privacy claim—which in the E.U. falls under the same notice-and-takedown laws as copyright. *See also* IFPI Denmark et al. v. Tele 2, Copenhagen Dist. Ct. F1-15124/2006 (2006) (ordering ISP to block www.piratebay.org based in part on existence of blocking mechanism for child pornography).

[80] 47 U.S.C. § 230.

[81] Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995). *See also* Zeran v. America Online, 129 F.3d 327, 331 (4th Cir. 1997) (discussing the legislative history of the CDA).

[82] *Id.*

[83] 47 USC § 230(b)(4).

pertains to copyright. A law that effectively penalized technical innovation in this area would mean lost opportunities for both OSPs copyright owners—for whom ContentID provides payments totaling hundreds of millions of dollars each year.[84] The Copyright Office should view any proposal to amend section 512(m) on the basis of "improved" filtering technology with great skepticism.

12. Does the notice-and-takedown process sufficiently protect against fraudulent, abusive or unfounded notices? If not, what should be done to address this concern?

The notice-and-takedown process manifestly does not sufficiently protect against fraudulent, abusive, or unfounded notices. Intermediaries routinely receive groundless removal requests from individuals or companies seeking to silence critics, rivals, or competitors.[85] Still more requests come from people who are simply misinformed about the law, or are using DMCA notices to advance non-copyright claims. In far too many cases, intermediaries respond by removing perfectly legal—and potentially important or time-sensitive—content. Error-correction through counter-notice occurs only rarely, as discussed below in response to Questions 16 and 17.

The incentives that can lead intermediaries to remove lawful content are obvious.[86] Complying with a removal notice is easy, cheap, and avoids legal risk. Anecdotal evidence of

---

[84] *See* GOOGLE, HOW GOOGLE FIGHTS PIRACY 3 (2014), *available at* https://drive.google.com/file/d/0BwxyRPFduTN2NmdYdGdJQnFTeTA/view.

[85] For example, the General Counsel of Automattic/WordPress has reported that

> [m]any times per week, WordPress.com receives such DMCA takedown notices that target what we can plainly see is fair use. An all too common example is a notice directed at a blogger who is criticizing a company or its products, and therefore using screenshots of the company's website or a photo of the company's wares in their post. This isn't just an outlier case; given our unique vantage point, we see an alarming number of businesses attempt to use the DMCA takedown process to wipe criticism of their company off the internet.

Paul Sieminski, *Corporations Abusing Copyright Law Are Ruining the Web for Everyone*, WIRED, Jan. 17, 2014, http://www.wired.com/2014/01/internet-companies-care-fair-use/. *See also* Wendy Seltzer, *Free Speech Unmoored in Copyright's Safe Harbor: Chilling Effects of the DMCA on the First Amendment*, 24 HARV. J. L. & TECH. 171 (2010).

[86] This observation is nothing new. It, and related First Amendment concerns, are noted repeatedly in cases rejecting notice-based liability under Communications Decency Act Section 230. *See, e.g.,* Zeran v. America Online, 129 F.3d 327, 333 (4th Cir. 1997) ("[L]iability upon notice reinforces service providers' incentives to restrict speech…. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information…. [T]he sheer number of postings on interactive computer services would create an impossible burden in the Internet context. Because service providers would be subject to liability only for the publication of information, and not for its removal, they would have a natural incentive simply to remove messages upon notification, whether the contents were defamatory or not.

lawful content being removed through DMCA abuse is abundant, and is likely documented in other submissions. Quantitative data is not as common, but it exists. A list of studies on point is included below in response to Question 29. They consistently show high rates of over-removal—even among companies, like Google, that commit significant resources to identifying and rejecting abusive requests.

The most effective protections against removal of lawful content come from well-crafted removal procedures, which give both OSPs and copyright holders a role in reducing improper removals, and which provide accused users with notice and opportunity to defend their online content. Key DMCA provisions protecting users are:

- *The exclusion of monitoring requirements in section 512(m).* This is one of the most important protections against over-removal, as discussed above in response to Question 10.

- *The good faith belief and penalty of perjury statements at sections 512(c)(3)(A)(v) and (vi).* In the assessment of one author who has responded to removal notices from around the world, this "scary legal language" has a meaningful deterrent effect on over-reaching removal demands.

- *The clear and detailed form-of-notice requirements at section 512(c)(3)(A).* Notice-and-takedown systems that lack this element consistently lead to the same problems: Intermediaries do not receive enough information to meaningfully assess a legal claim, but they feel they must take prompt action or risk liability. In the DMCA, Section 512(c)(3)(A) serves the key function of letting the OSP know when it has enough information to assume the burden of action and proceed to the other steps of section 512(c).

A number of procedural tools that could protect users are weak or absent from the DMCA, however. These proposed procedural dials and levers complement one another, such that more robust protection through one mechanism might make another less necessary. An extensive menu of legal options to improve notice-and-takedown regimes can be found in the Manila

Thus, like strict liability, liability upon notice has a chilling effect on the freedom of Internet speech.") (internal citations omitted).

Principles,[87] which have been endorsed by numerous public interest organizations around the world. Some that particularly stand out with respect to the DMCA are listed below. To be clear, these are possible ways to correct for existing shortcomings in the law. They could not offset the threat to Internet users from a "notice-and-staydown" system.

- *Notice to the user accused of infringement.* The provisions at section 512(g) make it too easy for an OSP to simply not bother with this notice. See the responses below to Questions 16 and 17 for a full explanation of how this is so.
- *Notice to users and opportunity for counter-notice when the OSP unilaterally removes content based on a suspected "red flag."* Red flag removals are not covered by the DMCA's current counter-notice and restoration provisions.
- *Standards for counter-notice at section 512(g)(3).* The counter-notice mechanism is vastly under-used, as discussed below in response to Question 16. Either counter-notice should be easier, or the DMCA should supplement it with other meaningful protections.
- *The damages provision at section 512(f).* Under current law, a notifier can effectively insulate itself against these damages with minimal consideration of legal limits such as fair use.[88] This renders the provision fairly toothless for Internet users victimized by false requests.
- *Public transparency requirements.* As discussed below in response to Question 16, these are likely one of the most effective measures for identifying and correcting wrongful removals. There is room for debate about who should bear the burden of transparency: the notifier or the OSP.
- *Standards for outsourced DMCA reporting organizations.* The role of these entities in the DMCA process has expanded greatly in recent years and risks undermining the DMCA's protections for Internet users, as discussed above in response to Question 9.

[87] Manila Principles on Intermediary Liability, https://www.manilaprinciples.org/.

[88] *See* Lenz v. Universal Music Group, 801 F.3d 1126 (9th Cir. 2015), *opinion amended and superseded on denial of reh'g*, ___ F.3d ___ (9th Cir. 2016); Rossi v. Motion Picture Ass'n of Am. Inc., 391 F.3d 1000 (9th Cir. 2004).

- *Consequences for notifiers who submit bulk or robo-sourced removal requests with a high error rate.* For reporting organizations, such consequences could be incorporated in standards for those firms.
- *Special treatment for notices knowingly submitted for content that is plausibly protected by fair use.* At minimum, notifiers could be required to specially flag such notices for intermediaries' attention.

Some of these ideas may prove more practical than others, and meaningful improvement could be achieved with just a subset of them. The low-hanging fruit are changes the Copyright Office could achieve without legislative action—for example, by publicly opining that transparency about removals through organizations like Lumen (https://lumendatabase.org) is not itself an act of infringement.

15. Please describe, and assess the effectiveness or ineffectiveness of, voluntary measures and best practices—including financial measures, content ''filtering'' and takedown procedures—that have been undertaken by interested parties to supplement or improve the efficacy of section 512's notice-and-takedown process.

The "DMCA-plus" era of online copyright enforcement, in which voluntary notice-and-termination agreements between copyright owners and service providers supplement the DMCA, is well underway. The arrangements that define DMCA-plus enforcement are nominally voluntary (i.e., contractual or quasi-contractual), but publicly available information reveals that many of them result from political pressure and express or implied threats of governmental regulation.[89] The Office of the U.S. Intellectual Property Enforcement Coordinator ("IPEC") has consistently promoted such arrangements in the form of privately negotiated "best practices" statements or agreements.[90] In 2013, the House Judiciary Committee Subcommittee on Courts, Intellectual Property, and the Internet held a hearing to applaud existing private-sector voluntary agreements and to encourage their expansion.[91] In the same year, the Patent and Trademark

[89] *See* Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1523 (2015) (discussing the government's role in procuring voluntary agreements and the "paradox of non-regulatory regulation" in the anti-piracy and anti-counterfeiting space).

[90] *See, e.g.*, OFFICE OF THE U.S. INTELLECTUAL PROP. ENFORCEMENT COORDINATOR, 2013 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 35 (2013) ("As an Administration, we have adopted the approach of encouraging the private sector to develop and implement cooperative voluntary initiatives to reduce infringement that are practical and effective.") [hereinafter IPEC 2013 JOINT STRATEGIC PLAN].

[91] *See Role of Voluntary Agreements in the U.S. Intellectual Property System: Hearing Before the Subcomm. on Courts, Intellectual Prop., and the Internet of the H. Comm. on the Judiciary,* 113th Cong. (2013).

Office sought public comment on how a "Voluntary Best Practices Study" could be designed to quantify and evaluate the effectiveness of DMCA-plus agreements.[92] Rights owners submitting comments for the study made it clear that they are looking to the government to police compliance: "[I]t is important that these voluntary initiatives be benchmarked and measured to determine whether the private sector can adequately 'self-regulate' to deter infringing and other abusive behavior."[93]

In addition to pressure from the government, there are business reasons for some intermediaries to go beyond what the DMCA requires. As the online marketplace for digital entertainment evolves, intermediaries and copyright owners appear to be increasingly financially co-dependent, whether through mass content-licensing deals or corporate mergers that vertically integrate content-distributing and copyright-owning enterprises. Professor Bridy's forthcoming book chapter on "DMCA-plus" enforcement,[94] attached to these Comments as Appendix A, identifies YouTube's Content ID system as a prime example of DMCA-plus enforcement supporting a symbiotic business relationship.[95]

In this post-DMCA world, online intermediaries of all shapes and sizes face increasing pressure to do more than the law requires of them to police intellectual property rights. DMCA-plus arrangements can be beneficial if they are truly voluntary and reflect genuine consensus among copyright owners and Internet companies about how and why to adjust the obligations that flow from default liability rules and exceptions. For large Internet companies that have the infrastructure and economic wherewithal to implement DMCA-plus measures, such measures may be a reasonable way to simultaneously avoid new governmental regulation and secure new business opportunities. New entrants and smaller players may be disadvantaged, however, to the

---

[92] Request of the United States Patent and Trademark Office for Public Comments: Voluntary Best Practices Study, 78 Fed. Reg. 37,210 (2013).

[93] Comments of the Recording Indus. Ass'n of Am., Inc. ("RIAA") 2 (Aug. 19, 2013), *submitted in* U.S. PATENT AND TRADEMARK OFFICE, Docket No. PTO-C-2013-0036, *available at* http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf.

[94] Annemarie Bridy, *Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW (John A. Rothchild ed., forthcoming 2016).

[95] *See also* Ramon Lobato & Julian Thomas, *The Business of Anti-Piracy: New Zones of Enterprise in the Copyright Wars*, 6 INT'L J. COMMC'N 606, 612 (2012) (observing that Content ID "reflect[s] a significant reorientation in corporate IP policy, both by Google and various rights holders, toward a more pragmatic commercial engagement with copyright infringement").

extent that DMCA-plus measures adopted by major intermediaries like Google, Comcast, and PayPal up the ante for everyone.

DMCA-plus enforcement also raises a range of normative concerns for Internet users and merchants: "Best practices" agreements are negotiated privately, without input from the public or public interest groups. In this respect, they lack the deliberative transparency associated with public law-making. The protocols they prescribe often presume liability for the accused and entail rushed or summary adjudications by inexpert authorities. Such protocols may thus be procedurally inadequate to prevent the removal of non-infringing content or the punishment of innocent actors.[96] For the Internet as a whole to benefit from DMCA-plus enforcement, "best practices" must incorporate adequate protections for Internet users and online merchants, whose interests are at risk of being marginalized when copyright owners and online intermediaries hammer out new bargains without public involvement.

Appendix A contains Professor Bridy's detailed description and assessment of "DMCA-Plus" voluntary agreements between copyright owners and service providers of various types—some covered by the DMCA and some not.

Counter Notifications

16. How effective is the counter-notification process for addressing false and mistaken assertions of infringement?

We have not seen studies or significant public data on this question, though there will be useful information in the study just published by Urban, et al.[97] Based on our own experience and discussion with other practitioners, we believe that it is rare for users to file counter-notices. Counter-notices certainly appear to be far less common than the improper removals that they are intended to counteract.

[96] *See* Niva Elkin-Koren, *After Twenty Years: Revisiting Copyright Liability of Online Intermediaries*, *in* THE EVOLUTION AND EQUILIBRIUM OF COPYRIGHT IN THE DIGITAL AGE 29, 45 (Susy Frankel & Daniel Gervais eds., 2014) (asserting that voluntary agreements often lack adequate safeguards for securing users' rights).

[97] *See* Jennifer Urban, et al., *Notice and Takedown in Everyday Practice* (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628.

A handful of companies track counter-notices in their transparency reports. These companies don't appear to aggregate the data over time and, in some cases, they track it using non-parallel categories so that comparison is difficult. For example:

- Twitter's transparency report includes counter-notices, though seemingly only for tweets, not for Vine or Periscope material. Twitter's latest semiannual report says that 56,971 tweets were withheld pursuant to DMCA notice, and the company received counter-notices for 65 or 0.11%, all of which led to the restoration of the targeted content.[98]
- Tumblr's June 2015 report states that of the 77,357 posts that were removed pursuant to takedown notices, 0.08% were restored using the counter-notice process.[99] Tumblr received additional counter-notices that it did not honor, though it is unclear whether those counter-notices were rejected based on substantive copyright problems or formal noncompliance with section 512(g).
- Github reports some counter-notices, but counts them in the same category with retracted DMCA notices, reporting 17 counter-notices or retractions out of 258 notices, which may each have identified numerous alleged infringements.[100]
- Automattic reports, for its latest data set, that "less than 0.6% of the DMCA notices we received were later subject to a counter-notice; of those cases, we're aware of further action being taken by the original DMCA complainant only once."[101]

These tiny percentages are dwarfed by the portion of dubious DMCA removal requests that researchers have identified. (See studies reported in Appendix B.) Even if the studies are off by an order of magnitude in their estimates, the number of potentially mistaken or malicious notices still vastly exceeds the number of counter-notices.[102]

---

[98] Twitter, Transparency Report, Copyright Notices (2015), https://transparency.twitter.com/copyright-notices/2015/jul-dec.

[99] Tumblr, Copyright and Trademark Transparency Report (2015), http://static.tumblr.com/zyubucd/0uWntp2iw/iptransparencyreport2015a_updatedfinal.pdf.

[100] GitHub, Transparency Report (2014), https://github.com/blog/1987-github-s-2014-transparency-report.

[101] Automattic, Intellectual Property (2015), https://transparency.automattic.com/intellectual-property/intellectual-property-2015-jul-1-dec-31/.

[102] This calculation assumes that the rate of counter-notice for the data sets discussed in Appendix B is similar to the rates reported in the transparency data discussed above. We see no reason to expect otherwise.

Importantly, the companies issuing detailed transparency reports may be relatively unique among small intermediaries in their commitment to protecting users and offering them a chance to counter-notice. It is unclear whether the thousands of other companies that have registered DMCA agents with the Copyright Office assume similar costs and inconveniences to provide a viable counter-notice process.

The ineffectiveness of the DMCA counter-notice process may be attributable to a number of causes:

- *Intermediaries do not have significant incentive to bother notifying a user when her content has been removed based on a DMCA notice.* The section 512(g) counter-notification process refers only to 512(c) hosting providers, not other OSPs (e.g., search engines), for starters. Even for hosts, the only reason to offer counter-notice is to avoid liability to a user for improperly removing that user's lawful content. But few believe that hosts face any meaningful risk of such liability, regardless of section 512(g). "Wrongful removal" claims against intermediaries in US courts have consistently failed, based on contractual and other defenses.[103]

- *It is not clear how many users actually receive notice that their content has been removed.* Not all hosting services tie user-generated content to user email addresses or other contact information. For those that do, users may supply email addresses from temporary or old and unmonitored accounts. It is accordingly difficult to know how many users really find out when their posts have been removed.

- *The counter-notice process is intimidating.* Consent to jurisdiction, which is a required element of a counter-notice under section 512(g)(3)(D), is a meaningful legal concession, and is particularly problematic for users who do not reside in the United States. In addition, the 512 section (g)(3)(C) statement under penalty of perjury, while analogous to the similar requirement for the notifier, is likely to be far more intimidating to individual users responding without benefit of counsel. And the cost of error for a user if she is

[103] *See, e.g.*, Song Fi, Inc. v. Google, Inc., 2015 WL 3624335 (N.D. Cal. June 10, 2015); Lewis v. YouTube LLC, 2015 WL 9480614 (Cal. App. Ct. Dec. 28, 2015); Sikhs for Justice "SFJ," Inc. v. Facebook, Inc., 2015 WL 7075696 (N.D. Cal. Nov. 13, 2015).

mistaken about her copyright defenses is much higher than the cost of error for a copyright owner who is mistaken about her claims.

Collectively, these factors constitute a meaningful deterrent to counter-notice. The point we make here is not that Congress lacked the intent or policy basis for establishing the detailed hurdles for counter-notifiers in section 512(g). The problem is that, because counter-notice has not been an effective corrective for wrongful notices, section 512(g) alone cannot adequately protect Internet users from having their legal speech removed. For that reason, the other procedural protections for users in section 512, such as form-of-notice requirements and declarations of good faith by copyright owners, play a more important role than Congress may have foreseen. Robust interpretations and enforcement of those protections by the courts and the Copyright Office are critical to maintain the DMCA's carefully structured balance. A more detailed discussion of these other protections in is included above in response to Question 12.

In (weak) defense of section 512(g), the transparency and expectation of procedural fairness created by the counter-notice process may be acting as a deterrent for some bad faith removal requests. It is possible, however, that the value of counter-notice is far exceeded by the value of public transparency about particular removals, such as those posted through Lumen or noted by the OSP on the page from which content has been removed. This transparency allows the identification of erroneous DMCA notices to be crowd-sourced across interested individuals online. To our knowledge there are no public datasets that would allow us to test this hypothesis.

17. How efficient or burdensome is the counter-notification process for users and service providers? Is it a workable solution over the long run?

Our response to Question 16 above addresses the burden for users. For OSPs, providing a counter-notice process at any kind of scale is unavoidably somewhat burdensome. That said, requiring such a process is appropriate given the impact of wrongful removals on individual speakers. As stated above in response to Questions 1 and 12, the DMCA's counter-notice provision is a key to the balance Congress intended to establish through the legislation. It functions as a visible and concrete, even if largely symbolic, acknowledgment of the importance of users' expressive rights in the digital environment. Its inclusion brings some aspects of due process to the extrajudicial DMCA removal system.

As an operational matter, the counter-notice process requires a commitment of personnel and internal tracking systems—whether ad hoc or specially built by the company. Tracking multiple communications with copyright owners and counter-notice providers can be difficult in practice, since parties may send multiple communications by different channels, without including consistent identifying information. At small scale, this is a manageable problem. At large scale, it requires bespoke internal tools, significant time commitment by employees, or both.

Removing and restoring content also likely require time commitment from engineers, whose time may be, in the company's eyes, more valuably spent in developing the company's products. Lawyers who easily persuade their clients to dedicate engineering resources to DMCA removals may have a harder time explaining why restoration on counter-notice is a high priority. This is largely due to the fact that the value of the safe harbors for OSPs lies more or less exclusively in their limitation of liability vis-à-vis copyright owners, not users. Designing and implementing a counter-notice process may be an issue for small companies, in particular, since they are unlikely to have built any dedicated tools for DMCA compliance.

As discussed in our response to Question 16 above, restoration on counter-notice alone is not adequate to correct for the pattern of over-removal under the DMCA. That said, it is an important element of online speakers' procedural protections.

Legal Standards

19. Assess courts' interpretations of the ''actual'' and ''red flag'' knowledge standards under the section 512 safe harbors, including the role of ''willful blindness'' and section 512(m)(1) (limiting the duty of a service provider to monitor for infringing activity) in such analyses. How are judicial interpretations impacting the effectiveness of section 512?

The notice-and-takedown protocol is straightforward and highly prescriptive by design. When defining the safe harbors, Congress wanted to draw bright lines on which OSPs and their investors could rely, even in the face of evolving liability rules. With respect to the question of what constitutes a substantially compliant notification under section 513(c)(3)(A), Congress succeeded in that goal. A substantially compliant notification is not the only trigger, however, for a service provider's duty to remove content if it wants safe harbor. That duty is also triggered by

so-called "red flag" knowledge, defined in section 512(c)(1)(A) of the statute as "aware[ness] of facts and circumstances from which infringing activity is apparent."[104]

Under the DMCA, both sources of notice can operate to deprive a service provider of the DMCA's safe harbors. But whereas the requirements for a compliant notification are clear on the face of the statute, the precise contours of red flag knowledge are elusive. By muddying the statute's clear rules about notification with the ambiguous standard of red flag notice, Congress deprived OSPs of the certainty the DMCA was intended to create.[105] It has subsequently fallen to the courts to make sense of the statute's vexing mix of rules and standards with respect to actionable knowledge. So far, they have risen to the occasion by carefully interpreting red flag notice to preserve the express no-duty-to-monitor rule in section 512(m) and, thus, the balance of burdens that Congress struck in the safe harbors.

There are two major appellate cases interpreting the scope of the safe harbors with respect to red flag knowledge: *Viacom International, Inc. v. YouTube, Inc.*[106] in the Second Circuit and *UMG Recordings, Inc. v. Shelter Capital Partners LLC*[107] in the Ninth Circuit. The courts in both cases agreed on the principle that red flag knowledge must be item-specific; it is not a generalized knowledge of infringement that follows inexorably from the fact that a service can or has been be used to infringe.[108] The cases also establish that red flag knowledge incorporates both a subjective and an objective element: "[T]he red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."[109] The judicial opinions establishing these principles are well-reasoned based on the text and architecture of the statute. Moreover, the

---

[104] 17 U.S.C. § 512(c)(1)(A)(ii).

[105] *See* H.R. REP. 105–551 (II), at 49-50 (1998) ("[Title II] provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities."); S. REP. NO. 105–190, *supra* note 1, at 2 ("Title II will provide certainty for rights holders and Internet service providers with respect to copyright infringement liability online.").

[106] 676 F.3d 19 (2d Cir. 2012).

[107] 718 F.3d 1006 (9th Cir. 2013).

[108] *See UMG Recordings*, 718 F.3d at 1023 (holding that "[a provider's] general knowledge that it hosted copyrightable material and that its services could be used for infringement is insufficient to constitute a red flag"); *Viacom*, 676 F.3d at 32 (defining red flag knowledge as "awareness of facts or circumstances that indicate *specific and identifiable instances* of infringement") (emphasis added).

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

courts in these cases benefited from erudite, thorough briefing by counsel and countless amici on both sides of the litigation.

Beyond these two points of agreement, however, the decisional law on red flags gets very muddy very quickly, notwithstanding a legislative history that treats questions surrounding red flags as cut and dried. The legislative history of the DMCA contemplates that the red flag provision should have very narrow application, justifying imputation of knowledge to a provider only in cases involving "obvious and conspicuous circumstances," such as where a site is completely dedicated to infringing content and operates with no discernable lawful purpose.[110]

In retrospect, the provision's reach has not been so easy to cabin. Where copyright owners may see unrepentant bad actors,[111] others see legitimate businesses with copyright-intensive operating models—businesses the safe harbors were explicitly designed to protect. By invoking the red flag provision against popular service providers they believe are not sufficiently aggressive (read: proactive) in their enforcement efforts, some copyright owners have tried indirectly to chip away at section 512(m)'s no-duty-to-monitor rule.[112] The music industry's suit against video-sharing platform Veoh is a good example of this strategy, to which courts have rightly been unreceptive.[113]

The *UMG Recordings* case drove Veoh into bankruptcy[114] over the red flag question. Plaintiffs argued —ultimately unsuccessfully—that Veoh should be disqualified from safe harbor

---

[110] S. REP. NO. 105–190, *supra* note 1, at 49.

[111] *Cf.* Stuart Dredge, *BPI: 'Google Leads Consumers Into a Murky Underworld of Unlicensed Sites,'* MUSIC ALLY, Nov. 15, 2013, http://musically.com/2013/11/15/bpi-google-leads-consumers-into-a-murky-underworld-of-unlicensed-sites/; Richard Verrier, *MPAA Report Says Google, Other Search Engines a Major Gateway to Piracy*, L.A. TIMES, Sept. 18, 2013, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-mpaa-piracy-study-20130918-story.html.

[112] *See, e.g.*, Capitol Records, LLC v. Escape Media Grp., Inc., No. 12-CV-6646 AJN, 2015 WL 1402049, at *57 (S.D.N.Y. Mar. 25, 2015) (recognizing the tension between the doctrine of red flag knowledge and section 512(m)'s rule that providers have no duty to affirmatively police their services for infringing activity); Square Ring, Inc. v. Doe-1, No. CV 09-563 (GMS), 2015 WL 307840, at *6 (D. Del. Jan. 23, 2015) (accepting the plaintiff's argument that the operator of a streaming video site might be chargeable with red flag knowledge for failing to respond to takedown notices sent *in advance of* an anticipated infringement); Arista Records LLC v. Myxer Inc., No. CV 08-03935 GAF JCX, 2011 WL 11660773, at *26 (C.D. Cal. Apr. 1, 2011) (rejecting the plaintiff's argument that the defendant should be charged with red flag knowledge or willful blindness to red flags because it failed to implement a digital fingerprinting system that blocks user uploads when they match copyrighted reference files in the system's database).

[113] *UMG Recordings*, 718 F.3d 1006.

[114] Chloe Albanesius, *Veoh Co-Founder Confirms Bankruptcy*, PCMAG.COM, Feb. 12, 2010, http://www.pcmag.com/article2/0,2817,2359105,00.asp.

because it failed to show "initiative" by implementing "search and indexing tools to locate and remove" all files belonging to artists previously identified in the RIAA's section 512(c)(3)(A) notifications.[115] The underlying logic of UMG's argument was that a section 513(c)(3)(A) notification concerning a specific work by an artist ipso facto creates red flag knowledge of any other works by the same artist that may exist on the service. A provider's failure to find and remove such other works, UMG urged the court to hold, should deprive that provider of safe harbor. The court in Veoh's case was unwilling to accept such a broad reading of the red flag provision, which would have amounted to an impermissible judicial repeal of section 512(m)—requiring providers to scour their sites open-endedly for instances of potential infringement not identified in section 512(c)(3)(A) notifications.

Just as the red flag provision was not intended to impose an affirmative monitoring obligation on service providers, it was not intended to require service providers to make difficult judgment calls about possible infringements.[116] That is what the provision implicitly requires, however, insofar as it creates an amorphous form of notice (and a corresponding removal obligation) that operates entirely outside the clearer parameters of notice-and-takedown.[117] The DMCA's red flag provision is the notice exception that swallows the notice rule, requiring minute examination of specific facts to determine whether an accused service provider ignored "objectively obvious" individual infringements.[118]

---

[115] *UMG Recordings*, 718 F.3d at 1023-24.

[116] S. REP. NO. 105–190, *supra* note 1, at 49 ("The common-sense result of this 'red flag' test is that [service providers] would not be required to make discriminating judgments about potential copyright infringement.").

[117] See our response to Question 10 for a discussion of the difficulty providers' employees face when trying to identify infringement.

[118] *See e.g.*, Capitol Records, Inc. v. MP3tunes, LLC, No. 07 CIV. 9931 WHP, 2013 WL 1987225, at *4 (S.D.N.Y. May 14, 2013) ("Since something less than a formal takedown notice may now establish red flag knowledge…, the issue of Defendants' red flag knowledge cannot be resolved on summary judgment."); Capitol Records v. Vimeo LLC, 972 F. Supp. 2d 500, 521-22 (S.D.N.Y. 2013) ("Plaintiffs claim that Vimeo employees' interactions with these fifty-five Videos–in–Suit necessitates a determination that Vimeo had actual or red flag knowledge of the videos' infringing content. The Court disagrees…. Rather, the Court finds that a triable issue remains as to whether...this standard is met as to each of the fifty-five videos in question."); Disney Enterprises, Inc. v. Hotfile Corp., No. 11-20427-CIV, 2013 WL 6336286, at *28 (S.D. Fla. Sept. 20, 2013) ("[T]o the extent that communications with users should have alerted Hotfile to the infringing nature of files on its system that were owned by the Studios…, Hotfile might be deemed to have possessed red flag knowledge."). For a survey of the cases, see Methaya Sirichit, *Catching the Conscience: An Analysis of the Knowledge Theory Under § 512(c)'s Safe Harbor & the Role of Willful Blindness in the Finding of Red Flags*, 23 ALB. L.J. SCI. & TECH. 85 (2013).

Predictably, the legal outcomes of fact-sensitive inquiries about the obviousness of infringement fall all over the map, adding uncertainty to inefficiency.[119] The convoluted procedural histories of *Viacom* and *UMG Recordings* illustrate how difficult it has been for courts to apply the red flag standard and to determine which questions concerning red flags can be decided as a matter of law and which must go to a jury.[120] Viacom sued YouTube in 2007. The case finally settled, with its second appeal pending, in 2014—seven years and three judicial opinions later. Veoh sued UMG for declaratory judgment in 2007. Following a grant of summary judgment for Veoh in 2009, the Ninth Circuit affirmed in 2011. The panel later withdrew its opinion for reconsideration following the Second Circuit's decision in the first *YouTube* appeal. The Ninth Circuit issued its second (and final) opinion in *Veoh*, another affirmance, in 2013. Veoh closed shop in 2010, however, long before it could savor victory.[121] For anyone not keeping track, that's two cases, two circuits, eight judges, six opinions, one bankruptcy, seven years of litigation, and far too many lawyers and amici to count. So much for certainty.

If we continue to believe, as Congress did when it enacted the DMCA, that creating certainty for online businesses and their potential investors concerning the scope of copyright liability is an effective way to get and grow new platforms and services, then the design of the safe harbor regime should be optimized for certainty and for the encouragement of new entrants. To optimize for certainty, Congress should have opted for rules over standards when designing the safe harbors.[122] Instead, Congress created a hybrid design that mixes the rules for notice in section 512(c)(3)(A) with the red flag standard in section 512(c)(1)(A).

---

[119] *Compare, e.g.*, Columbia Pictures v. Fung, 710 F.3d 1020, 1043 (2013) (finding red flag knowledge as a matter of law where "[t]he material in question was sufficiently current and well-known" that its copyrighted and unlicensed status would have been obvious to a reasonable person) *with Capitol Records*, 972 F. Supp. 2d at 521 (declining to find red flag knowledge as a matter of law where the defendant's employees interacted with material that "would be characterized by many as popular, and in some cases legendary").

[120] *See* UMG Recordings, Inc. v. Veoh Networks Inc., 665 F.Supp.2d 1099 (C.D. Cal. 2009), *aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 667 F.3d 1022 (9th Cir. 2011), *opinion withdrawn and superseded on reh'g*, 718 F.3d 1006 (9th Cir. 2013), *and aff'd sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013); Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514 (S.D.N.Y. 2010) aff'd in part, vacated in part, remanded, 676 F.3d 19 (2d Cir. 2012); Viacom Int'l Inc. v. YouTube, Inc., 940 F. Supp. 2d 110, 113 (S.D.N.Y. 2013), appeal withdrawn (Mar. 19, 2014).

[121] *UMG Recordings*, 718 F.3d at 1006.

[122] *See* Duncan Kennedy, *Form and Substance in Private Law Adjudication*, 89 HARV. L. REV. 1685, 1688 (1976) (asserting that "the two great social virtues of formally realizable rules, as opposed to standards or principles, are the restraint of official arbitrariness and certainty").

The hybrid design appears at first blush to offer the best of both worlds: the certainty that comes with the relative predictability of rules and the incentive to behave cautiously that comes with the relative unpredictability of standards.[123] Experience has shown, however, that the actual costs of unpredictability in this arena have outweighed the potential benefits. By introducing an ambiguous notice standard into a regime otherwise defined by bright-line rules, Congress failed to align the design of the safe harbors with the goal of providing certainty.[124] Moreover, by leaving the definition of red flag notice to courts, which copyright owners have urged to interpret the provision expansively, Congress paved the way for ex post disruption of the balance of enforcement burdens it specified ex ante in the notice-and-takedown protocol. In that balance, copyright owners bear the costs associated with notice, including the cost of monitoring for infringements, and service providers bear the costs associated with content removal.[125] So far, the courts have safeguarded that balance through an interpretation of red flag notice that is item-specific, thereby giving meaning to the statute's no-duty-to-monitor rule in section 512(m).

Even in the wake of decisions limiting the scope of red flag notice to facts and circumstances indicating specific instances of infringement, however, the content of the standard remains elusive and case-specific. Given that the red flag standard implies there may be *some* duty to assess *some* subset of the universe of potential infringements on a provider's service, the DMCA's no-duty-to-monitor rule in section 512(m) can provide only a false sense of security for service providers. Many of the same providers that have asserted the safe harbors in litigation

---

[123] *See* Joseph William Singer, *The Rule of Reason in Property Law*, 46 U.C. DAVIS L. REV. 1369, 1374 (2013) ("Standards promote useful moral reflection and deter socially destructive behavior. Fuzziness at the edges of rules often prompts better decision making, both by market actors and by judges.").

[124] John Blevins proposes that the key to managing the uncertainty of the red flag standard is having courts interpret it as a bright line rule. John Blevins, *Uncertainty as Enforcement Mechanism: The New Expansion of Secondary Copyright Liability to Internet Platforms*, 34 CARDOZO L. REV. 1821, 1878 (2013). The conversion of the red flag standard into a rule through precedent would reduce the standard's inherent uncertainty. *See* Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 577-578 (1992) (discussing how standards can become rules over time through successive adjudications). At the end of the day, however, many—if not most—questions concerning which facts and circumstances make infringing activity obvious to a reasonable person will end up being jury questions. Moreover, the expense of converting a standard into a rule through repeated adjudications can be substantial for entities to which the standard applies. *See id.* at 579 (citing costs of obtaining legal advice while the law is developing and costs reflected in non-compliant behavior in the face of uncertainty about the content of the law).

[125] *See CCBill*, 488 F.3d at 1102 ("The DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright.").

have adopted monitoring technologies despite the fact that such systems are not required.[126] Copyright owners surely view this development as a benefit of the statute's mix of rules and standards, but it is hard to argue in light of section 512(m) that Congress intended proactive filtering to be a soft condition for safe harbor.

Time and experience have shown that the red flag provision in the safe harbors makes their scope unworkably uncertain, raising operating and legal costs for potentially eligible service providers. The provision has also proven difficult for courts to reconcile with the express no-duty-to-monitor rule in section 512(m). Courts, for their part, have ably done what they have been called upon to do, interpreting the red flag standard with due regard for the context in which it appears and with the aim of giving effect to all of the provisions that are key to the DMCA's balance of burdens and interests.

To better serve the DMCA's policy goals, however, Congress should consider making actual knowledge the exclusive scienter standard for safe harbor disqualification in cases involving claims of contributory infringement against eligible service providers.[127] Such knowledge could be proven directly or circumstantially, through 512(c) notifications or any other evidence showing the provider's subjective awareness of infringement acquired during operation of its service.

20. Assess courts' interpretations of the ''financial benefit'' and ''right and ability to control'' standards under the section 512 safe harbors. How are judicial interpretations impacting the effectiveness of section 512?

---

[126] Among service providers that have asserted the DMCA safe harbors in litigation with copyright owners, YouTube, Veoh, MySpace, Myxer, Hotfile, and Vimeo voluntarily implemented digital fingerprinting systems for filtering user-uploaded content either before or during the pendency of the litigation. *Viacom*, 718 F. Supp. 2d at 528; *UMG Recordings*, 667 F.3d at 1028; UMG Recordings, Inc. v. MySpace, Inc., 526 F. Supp. 2d 1046, 1054 (C.D. Cal. 2007); Arista Records LLC v. Myxer Inc., No. CV 08-03935 GAF JCX, 2011 WL 11660773, at *5 (C.D. Cal. Apr. 1, 2011); Disney Enterprises, Inc. v. Hotfile Corp., No. 11-20427-CIV, 2013 WL 6336286, at *4 (S.D. Fla. Sept. 20, 2013); Daniel Witt, *Copyright Match on Vimeo*, VIMEO BLOG, May 21, 2014, https://vimeo.com/blog/post/copyright-match-on-vimeo.

[127] This deviates from the common law standard for contributory infringement, which allows for both actual and constructive knowledge. *See generally* R. Anthony Reese, *The Relationship between the ISP Safe Harbors and the Ordinary Rules of Copyright Liability*, 32 COLUM. J. L. & ARTS 427 (2009) (exploring the non-identical relationship between DMCA safe harbor standards and corresponding common law copyright liability standards). Courts deciding safe harbor cases involving claims for vicarious infringement have held that some alteration of common law standards is necessary to give the safe harbors meaning. *See Viacom*, 676 F.3d at 38 (holding that "the right and ability to control infringing activity under § 512(c)(1)(B) requires something more than the ability to remove or block access to materials posted on a service provider's website," even if the ability to remove or block access to infringing materials is sufficient on its own under the common law to establish the control element of a claim for vicarious infringement).

At common law, a defendant can be vicariously liable for copyright infringement if it had, but declined to exercise, the right and ability to control or supervise a direct infringer from whose actions it directly profited.[128] For a plaintiff to meet its prima facie burden on the "control element" of a claim for vicarious copyright infringement, it must show both that the defendant had the legal right to control the actions of the direct infringer and that the defendant had the practical ability to do so.[129] For a plaintiff to meet its prima facie burden on the direct financial benefit element, it must demonstrate that the presence of infringing material on a service is causally related to user demand and revenue for the service.[130] The presence of infringing material on a service, by itself, does not prove the requisite causal relationship.[131] Nor is it enough for a plaintiff to show that infringing material is an "added benefit" for users. [132]

For sound reasons having to do with the structure and purpose of the safe harbors, courts have adjusted the substance of the common law control element in cases involving OSPs that raise statutory section 512 defenses. When Congress enacted the DMCA, it realized that secondary liability standards in the online context were still evolving in the courts, and it wanted that evolution to continue in an organic way based on the circumstances of individual cases.[133] Congress also wanted to create a statutory regime that would limit the liability of OSPs for *all* kinds of infringement, including vicarious infringement.[134] As the case law developed, courts realized that they could not apply the traditional common law control element without defeating

---

[128] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 & n.9 (2005).

[129] Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1173 (9th Cir. 2007) (citing *Grokster*, 545 U.S. at 930 n.9).

[130] *See* Ellison v. Robertson, 357 F.3d 1072, 1079 (9th Cir. 2004) (holding that there was no direct financial benefit where the record lacked evidence that the defendant service provider "attracted or retained subscriptions because of the infringement or lost subscriptions because of [its] eventual obstruction of the infringement").

[131] *See* Columbia Pictures Indus., Inc. v. Fung, 710 F.3d 1020, 1045 (9th Cir. 2013) (citing legislative history stating that a direct financial benefit cannot be established showing that a service provider "receive[d] a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities") (internal citation omitted).

[132] A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001), as amended (Apr. 3, 2001), *aff'd sub nom.* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002) *and aff'd sub nom.* A&M Records, Inc. v. Napster, Inc., 284 F.3d 1091 (9th Cir. 2002) (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 263–64 (9th Cir. 1996)).

[133] *See* S. REP. NO. 105–190, *supra* note 1, at 19 ("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.").

[134] *See id.* at 40 (1998) ("The limitations in subsections (a) through (d) protect qualifying service providers from liability for all monetary relief for direct, vicarious, and contributory infringement.").

the purpose of protecting providers from vicarious infringement claims. Thus, the law of DMCA vicarious infringement has evolved away from the common law of vicarious infringement when it comes to an analysis of the control element. By contrast, the analysis of the direct financial benefit element has so far remained the same under both bodies of law.[135] Congress neither failed to anticipate nor desired to avoid such doctrinal evolution.

In *A&M Records v. Napster*, the Ninth Circuit applied the common law standard without consideration of Napster's eligibility for safe harbor[136] and concluded that the "control element" of the prima facie case for vicarious liability is satisfied if the defendant reserves the right in its terms of service to terminate access for infringing users, and the architecture of the defendant's system enables the defendant to locate infringing material.[137] Unlike the court in *Napster*, however, courts in subsequent cases have had the opportunity to fully analyze the relationship between the common law "right and ability to control" and the conditions for safe harbor in section 512. Those courts—including the Second, Fourth, and Ninth Circuits—have consistently and correctly concluded that the *Napster* court's articulation of the control element cannot be reconciled with a safe harbor framework that conditions eligibility on a provider's terminating access for repeat infringers and removing allegedly infringing material upon receipt of notice from a copyright owner.[138] As the Ninth Circuit pointed out, "Congress could not have intended for courts to hold that a service provider *loses* immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically *required* by the DMCA to obtain safe harbor protection."[139] The logic is unavoidable: Applying *Napster*'s common law "right and ability to control" standard in cases involving assertion of the DMCA safe harbors would senselessly trap defendants in a Catch-22.[140]

---

[135] By contrast, courts in section 512 cases do apply the common law direct financial benefit standard, because they can do so without fatally undermining the structure and intent of the safe harbors. *See CCBill*, 488 F.3d at 1117 (holding that "'direct financial benefit' should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability").

[136] *See id.* at 1025 (stating that the issue of Napster's safe harbor eligibility "will be more fully developed at trial").

[137] *See A&M Records*, 239 F.3d at 1023–24.

[138] *Viacom*, 676 F.3d at 38; Costar Grp. Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688 (D. Md. 2001), *aff'd*, 373 F.3d 544 (4th Cir. 2004); *UMG Recordings*, 718 F.3d at 1027; *Columbia Pictures*, 710 F.3d at 1045.

[139] *UMG Recordings*, 718 F.3d at 1027 (quoting from the district court's opinion) (emphasis added).

[140] *See id.* at 1028 n.17 (collecting cases). *See also* Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 261 (2009).

Reinterpreting the control element to align it with the structure and intent of the safe harbors, courts have necessarily held that the right and ability to control infringing activity involves "something more" than having the general ability to locate infringing material and terminate users' access.[141] The OSP must also "exert substantial influence on the activities of users," which may include purposeful conduct—e.g. "culpable, inducing activity like that in [*MGM v.*] *Grokster*."[142] Several cases have given precise content to the "something more" requirement, providing necessary clarity and guidance for both OSPs and copyright owners concerning the kind of conduct that could disqualify a provider from safe harbor. For example, disqualifying activity may include active involvement in the listing, bidding, sale, and delivery of infringing items[143] or the provision of detailed instructions to site operators regarding the layout, appearance, and content of their websites.[144]

To prevent the safe harbors from becoming a nullity in the face of vicarious infringement claims, courts in safe harbor cases have done what the logic and structure of the DMCA dictate: they have interpreted the control element to require something more than the right to terminate service and the ability to locate and remove infringing material.[145] The "something more" requirement is needed to effectuate express Congressional intent to provide OSPs with a meaningful shield from claims for all species of copyright liability, including vicarious liability. The court in *Napster* did not fully analyze the interaction between the DMCA and the common law standards for vicarious liability, which derive from the physical "premises" cases of a bygone era.[146] Had it done so, it would have had to grapple with the inherent inconsistencies between the two liability paradigms, and it would certainly have arrived at the "something more" standard that subsequent courts, including the Ninth Circuit, have adopted.

---

[141] *UMG Recordings*, 718 F.3d at 1030; *Columbia Pictures*, 710 F.3d at 1045; *Viacom*, 676 F.3d at 38.

[142] *Columbia Pictures*, 710 F.3d at 1045.

[143] Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1094 (C.D. Cal. 2001).

[144] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1173 (C.D. Cal. 2002).

[145] *See UMG Recordings*, 718 F.3d at 1028 ("Given Congress' explicit intention to protect qualifying service providers who would otherwise be subject to vicarious liability, it would be puzzling for Congress to make § 512(c) entirely coextensive with the vicarious liability requirements, which would effectively exclude all vicarious liability claims from the § 512(c) safe harbor.").

[146] *See, e.g.*, Gershwin Pub. Corp. v. Columbia Artists Mgmt., Inc., 443 F.2d 1159 (2d Cir. 1971) (involving live community concerts); *Fonovisa*, 76 F.3d 259 (involving a brick-and-mortar swap meet).

Repeat Infringers

23. Is there sufficient clarity in the law as to what constitutes a repeat infringer policy for purposes of section 512's safe harbors? If not, what should be done to address this concern?

Compared to the detailed notice and takedown framework in section 512(c), the requirements in section 512(i) are much less specifically prescriptive. For example, the statute provides no definition of "repeat infringer" and is silent as to what "appropriate circumstances" for termination of access might be.[147] The statute does not define what it means for a policy to be "reasonably implemented," nor does it specify the means by which an ISP is expected to "inform subscribers" of its policy. As one court has observed, "the language of the statute and the legislative history of this section are less than models of clarity."[148] Although there are no one-size-fits-all definitions of some key terms in section 512(i), over almost two decades the case law has developed to set reasonably clear parameters for OSPs to follow as they exercise the discretion Congress gave them[149] to define and implement compliant repeat infringer policies.

When deciding cases involving section 512(i), courts have been guided by a legislative history expressing Congressional intent to preserve strong incentives for service providers to cooperate with rights owners.[150] At the same time, however, courts are bound to interpret section 512(i)'s requirements within the limits of section 512(m), the DMCA's no-duty-to-monitor rule, which expressly precludes courts from construing any provision in section 512 to condition safe harbor eligibility on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity."[151] So, while section 512(i) was designed to promote cooperation

---

[147] *See generally* Andres Sawicki, *Repeat Infringement in the Digital Millennium Copyright Act*, 73 U. CHI. L. REV. 1455 (2006). In *UMG Recordings, Inc. v. Veoh Networks Inc.*, the court declined to hold that termination of a user's access was required after a second notice when the first notice identified multiple alleged infringements. *UMG Recordings*, 665 F. Supp. 2d at 1118. The notices in the case were generated by the copyright owner using Audible Magic's filtering system. *Id.*

[148] *Cybernet Ventures*, 213 F. Supp. 2d at 1176.

[149] Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1101 (W.D. Wash. 2004) ("The notice and take-down provisions demonstrate that Congress infused the statute with specific detail when it so chose. The fact that Congress chose not to adopt such specific provisions when defining a [repeat infringer] policy indicates its intent to leave the policy requirements, and the subsequent obligations of the service providers, loosely defined.").

[150] *See In re* Charter Commc'ns, Inc., 393 F.3d 771, 782 (8th Cir. 2005) (quoting the legislative history of the DMCA to establish that "Congress wanted to create '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'" (quoting S. REP. NO. 105–190, *supra* note 1, at 40).

[151] 17 U.S.C. § 512(m)(1).

between rights owners and ISPs in online copyright enforcement, it cannot be read in light of section 512(m) to impose on qualifying ISPs any affirmative duty to monitor their services to identify repeat infringers.[152]

Given the express limitation established in section 512(m) concerning the burdens and costs that can legitimately be imposed on providers seeking safe harbor, courts have produced carefully calibrated interpretations of the reach of section 512(i), most in the context of defenses raised under section 512(c). For example, in *Corbis Corp. v. Amazon.com, Inc.*,[153] the court held that a properly adopted termination policy need not precisely track the language of the DMCA, and it need not disclose to users the precise criteria the provider will apply to determine when termination of access is appropriate.[154] Such a policy must, however, convey to users "who repeatedly or flagrantly abuse their access to the [I]nternet through disrespect for the intellectual property rights of others" that they face "a realistic threat of losing that access."[155] In *Perfect 10, Inc. v. Cybernet Ventures, Inc.*,[156] the court held that determining appropriate circumstances for termination does not require investigation by the provider into individual acts of infringement; however, the provider must act when it receives "sufficient evidence to create actual knowledge of blatant, repeat infringement by particular users, particularly infringement of a willful and commercial nature."[157]

Courts agree that a reasonably implemented policy is one that provides some system for tracking notices sent by copyright owners and connecting those notices to users.[158] They have reached differing conclusions, however, concerning whether multiple notices of infringement

---

[152] *See, e.g.*, Io Grp., Inc. v. Veoh Networks, Inc., 586 F. Supp. 2d 1132, 1145 (N.D. Cal. 2008) (stating that "section 512(i) does not require service providers to track users in a particular way or to affirmatively police users for evidence of repeat infringement").

[153] *Corbis Corp.*, 351 F. Supp. 2d 1090.

[154] *Id.* at 1101–02.

[155] *Id.* at 1101 (quoting H.R. REP. NO. 105–551, pt. 2, at 44 (1998)).

[156] *Cybernet Ventures*, 213 F. Supp. 2d 1146.

[157] *Id.* at 1177.

[158] *See, e.g.*, Disney Enterprises, Inc. v. Hotfile Corp., No. 11-20427-CIV, 2013 WL 6336286, at *21 (S.D. Fla. Sept. 20, 2013) (holding that Hotfile was not compliant with its obligations under § 512(i) because it "did nothing to tie notices to repeat infringers"); *CCBill*, 481 F.3d at 758 (holding that § 512(i) requires "a working notification system"); Ellison v. Robertson, 357 F.3d 1072, 1080 (9th Cir. 2004) (holding that a reasonable jury could conclude that implementation of a termination policy is not reasonable where notices of infringement have gone unheeded by the provider); *Corbis Corp.*, 351 F. Supp. 2d at 1102 (holding that § 512(i) requires adoption and implementation of a procedure for receiving complaints and conveying them to users).

from a copyright owner are sufficient, on their own, to justify charging a provider with actual knowledge of a particular user's blatant, repeat infringement.[159] The court in *BMG Rights Management v. Cox Communications*, following *UMG Recordings*, recently held that DMCA-compliant notices from copyright owners should be treated as "powerful evidence of a service provider's knowledge."[160] Because there is a substantial rate of error and abuse associated with DMCA notices, the best approach is to treat notices as strong but not conclusive evidence of a service provider's knowledge of infringement. The analysis should remain, as it has been, case-specific, taking into account the quality of the source of the notices as well as the actions of the service provider and its users.

The body of case law interpreting section 512(i)'s requirements is now sufficiently large and sufficiently consistent that there is no need for Congress to add specificity to the current language, which was purposely left imprecise to provide some range of motion for service providers of different shapes and sizes. Recently, Cox Communications and Escape Media Group were denied safe harbor for failing to comply with section 512(i).[161] Such results could not occur if the provision did not give courts sufficient guidance in separating providers operating in good faith from those that merely give lip service to their enforcement obligations under section 512(i). Moreover, broadband Internet access providers, which can qualify for the section 512(a) safe harbor, and trade groups representing major copyright owners are currently operating under the Memorandum of Understanding that created the Copyright Alert System (CAS), a privately managed notice-and-sanction system for dealing with allegations of repeat

---

[159] *Compare* Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1088 (C.D. Cal. 2004), *rev'd on other grounds*, 481 F.3d 751 (9th Cir. 2007) (concluding that "an internet service provider who receives repeat notifications that substantially comply with the requirements of § 512(c)(3)(A) about one of its clients, but does not terminate its relationship with the client, has not reasonably implemented a repeat infringer policy"), *with Corbis Corp.*, 351 F. Supp. 2d at 1105 (concluding that notices from a copyright owner function to bring a potential infringement to the provider's attention, but do not, in themselves, provide evidence of blatant copyright infringement because they could be erroneous).

[160] BMG Rights Mgmt. LLC v. Cox Commc'ns, Inc., No. 1:14-CV-1611, 2015 WL 7756130, at *19 (E.D. Va. Dec. 1, 2015) (quoting *UMG Recordings*, 718 F.3d at 1020).

[161] *Id.* at *14 ("Cox does not terminate access of repeat infringers under appropriate circumstances."); Capitol Records, LLC v. Escape Media Grp., Inc., No. 12-CV-6646 AJN, 2015 WL 1402049, at *6 (S.D.N.Y. Mar. 25, 2015) (citing, as disqualifying factors under section 512(i), "(1) Escape's failure to keep adequate records of infringement; (2) Escape's practice of actively preventing copyright owners from collecting information necessary to issue DMCA takedown notifications; and (3) Escape's failure to 'terminate' repeat infringers.").

infringement against broadband subscribers using peer-to-peer networks.[162] The CAS takes pressure off the safe harbors and the repeat infringer provision for the participating parties.

Other Issues

29. Please provide any statistical or economic reports or studies that demonstrate the effectiveness, ineffectiveness, and/or impact of section 512's safe harbors.

The recently published study by Urban, et al.,[163] mentioned above in response to Question 16, is a significant source of such data. Previous empirical studies of "over-removal" under the DMCA and other notice and takedown systems around the world are listed in Appendix B. We are also aware of two studies concerning the larger economic impact of copyright intermediary liability laws:

- The consulting firm Oxera, in research prepared for Google, attempted to quantify the economic impact of four countries' differing intermediary liability laws, and concluded that intermediary liability regimes indirectly affect the attractiveness of entrepreneurship and investment.[164]
- Booz & Company, in research funded by Google, surveyed venture capital angel investors, who reported that expanded or ambiguous copyright liability for intermediaries deters investment in early-stage start-ups.[165]

[162] For a full description of the CAS, see Appendix A.

[163] *See supra* note 97.

[164] Oxera, *The Economic Impact of Safe Harbours on Internet Intermediary Start-Ups*, Feb. 2015, http://www.oxera.com/getmedia/cba1e897-be95-4a04-8ac3-869570df07b1/The-economic-impact-of-safe-harbours-on-Internet-intermediary-start-ups.pdf.aspx?ext=.pdf.

[165] Booz & Co., *The Impact of U.S. Copyright Regulations on Early Stage Investment: A Quantitative Study*, http://www.strategyand.pwc.com/media/uploads/Strategyand-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf.

Respectfully Submitted,

/s/ Annemarie Bridy

Annemarie Bridy

Professor
College of Law
University of Idaho

Affiliate Scholar
Center for Internet and Society
Stanford Law School

/s/ Daphne Keller

Daphne Keller

Director, Intermediary Liability
Center for Internet and Society
Stanford Law School

Dated: March 30, 2016

Appendix A: Voluntary Agreements
Copyright Office Section 512 Study Comments
Annemarie Bridy and Daphne Keller

Copyright's Digital Deputies: DMCA-Plus Enforcement By Internet Intermediaries

Forthcoming in John A. Rothchild (ed.), Research Handbook on Electronic Commerce Law, Edward Elgar, 2016

Annemarie Bridy*

I. Introduction

For the first dozen years after passage of the Digital Millennium Copyright Act ("DMCA"), the safe harbors in Section 512 set the parameters for cooperative online enforcement between Internet intermediaries and the copyright industries.[1] The DMCA safe harbors account for both the types of online activities that typically give rise to secondary copyright liability and the types of service providers that typically engage in those activities.[2] For example, the safe harbors cover routing and caching of third-party content by broadband Internet service providers ("ISPs");[3] storage of third-party content by hosting services and user-generated content ("UGC") platforms;[4] and linking to third-party

* Professor, University of Idaho College of Law; Affiliate Scholar, Stanford University Center for Internet and Society (CIS).

[1] *See* 17 U.S.C. § 512.

[2] A "service provider" is defined broadly in the DMCA as "a provider of online services or network access, or the operator of facilities therefor." 17 U.S.C. § 512(k)(1)(B).

[3] *See* 17 U.S.C. § 512(a) (establishing a safe harbor for "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider").

[4] *See* 17 U.S.C. § 512(c) (establishing a safe harbor for "storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider"). The scope of Section 512(c) has been held to cover not only the storage of users' materials but also activities the service provider undertakes to provide users with access to their stored materials. *See* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1018 (9th Cir. 2013) (holding that the safe harbor covers "access-facilitating processes" as well as storage).

content by search engines.[5] As long as covered service providers adhere to the applicable conditions for safe harbor in the DMCA by providing specified enforcement assistance, they are insulated from claims for money damages arising from their users' copyright infringements.[6] The DMCA's *quid pro quo* is thus non-liability in exchange for limited aid from intermediaries whose relationship to acts of direct copyright infringement could otherwise leave them legally exposed.[7]

The copyright industries have never been satisfied with the bargain that was struck in the DMCA, however. In the words of the Motion Picture Association of America ("MPAA"), they are always looking for ways to "improve upon default legal standards (such as the DMCA)" and to exact promises of increased cooperation from "recalcitrant players."[8] As the Internet has grown exponentially in terms of both users and services, corporate rights owners and their trade groups have lobbied continuously for more aggressive enforcement from a wider range of intermediaries. In Congress, the courts, and the media, they have demanded that online intermediaries—both those covered by the DMCA and those falling outside the statute's ambit — do more to protect their intellectual property rights.[9] In particular, they have sought new ways to reach and shutter

---

[5] *See* 17 U.S.C. § 512(d) (establishing a safe harbor for "referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link").

[6] Each of the four safe harbors provides that "[a] service provider shall not be liable for monetary relief" if the conditions for safe harbor are met. 17 U.S.C. § 512(a), (b), (c), & (d).

[7] The legislative history of the statute documents this bargain. *See* S. REP. NO. 105-190, at 20 (1998) ("Title II preserves 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. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur in the course of their activities.").

[8] Comments of the Motion Picture Ass'n of Am., Inc. ("MPAA") 2–3 (Aug. 21, 2013), *submitted in* U.S. PATENT AND TRADEMARK OFFICE, VOLUNTARY BEST PRACTICES STUDY, Docket No. PTO-C-2013-0036, *available at* http://www.uspto.gov/ip/officechiefecon/PTO-C-2013-0036.pdf.

[9] *See, e.g., id.* at 2 (arguing that "all players in the Internet ecosystem," including "the various intermediaries that facilitate online commerce and speech…must play a meaningful role in addressing the problem of rampant piracy on the Web"); Comments of the Recording Indus. Ass'n of Am., Inc. ("RIAA") 1 (Aug. 19, 2013), *submitted in*

"pirate sites" that are beyond the reach of U.S. law.[10] In recent years, their demands have been answered through an expanding regime of "DMCA-plus" enforcement.

The arrangements that define DMCA-plus enforcement are nominally voluntary (i.e., contractual or quasi-contractual), but they come about largely as a result of political pressure and express or implied threats of governmental regulation.[11] The Office of the U.S. Intellectual Property Enforcement Coordinator ("IPEC") has consistently promoted such arrangements in the form of privately negotiated "best practices" statements or agreements.[12] In 2013, the House Judiciary Committee Subcommittee on Courts, Intellectual Property, and the Internet held a hearing to applaud existing private-sector voluntary agreements and to encourage their expansion.[13] In the same year, the Patent and Trademark Office sought public comment on how a "Voluntary Best Practices Study" could be designed to quantify and evaluate the effectiveness of DMCA-plus agreements.[14] Rights owners submitting comments for the study

---

U.S. PATENT AND TRADEMARK OFFICE, *supra* note 8 (asserting that "all responsible stakeholders in the Internet ecosystem…have a role to play in…deterring illegal activity").

[10] Their most controversial effort in this area was the famously failed lobbying campaign for the Stop Online Piracy Act (SOPA) and the PROTECT IP Act (PIPA). *See generally* Annemarie Bridy, *Copyright Policymaking as Procedural Democratic Process: A Discourse-Theoretic Perspective on ACTA, SOPA, and PIPA*, 30 Cardozo Arts & Ent. L.J. 153 (2012).

[11] *See* Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. ___ (forthcoming Sept. 2015) (discussing the government's role in procuring voluntary agreements and the "paradox of non-regulatory regulation" in the anti-piracy and anti-counterfeiting space).

[12] *See, e.g.*, OFFICE OF THE U.S. INTELLECTUAL PROP. ENFORCEMENT COORDINATOR, 2013 JOINT STRATEGIC PLAN ON INTELLECTUAL PROPERTY ENFORCEMENT 35 (2013) ("As an Administration, we have adopted the approach of encouraging the private sector to develop and implement cooperative voluntary initiatives to reduce infringement that are practical and effective.") [hereinafter IPEC 2013 JOINT STRATEGIC PLAN].

[13] *See Role of Voluntary Agreements in the U.S. Intellectual Property System: Hearing Before the Subcomm. on Courts, Intellectual Prop., and the Internet of the H. Comm. on the Judiciary*, 113th Cong. (2013) [hereinafter *Role of Voluntary Agreements Hearing*].

[14] Request of the United States Patent and Trademark Office for Public Comments: Voluntary Best Practices Study, 78 Fed. Reg. 37,210 (2013).

made it clear that they are looking to the government to police compliance: "[I]t is important that these voluntary initiatives be benchmarked and measured to determine whether the private sector can adequately 'self-regulate' to deter infringing and other abusive behavior."[15] In addition to pressure from the government, there are business reasons for some intermediaries to go beyond what the DMCA requires. As the online marketplace for digital entertainment evolves, intermediaries and copyright owners are increasingly financially co-dependent, whether through mass content-licensing deals or corporate mergers that vertically integrate content-distributing and copyright-owning enterprises. YouTube's Content ID system, discussed below, is a prime example of DMCA-plus enforcement as a symbiotic business relationship.[16]

The dilemma for intermediaries that volunteer to undertake DMCA-plus enforcement is that each new commitment they make raises the bar for what the copyright industries and policy makers regard as minimum standards.[17] The more intermediaries give, it seems, the more is expected of them. In the DMCA-plus enforcement world, the gap between what the law requires and what intermediaries are promising to do is growing. As that gap widens, there is reason to be concerned about the expressive and due process rights of users and website operators, who have no seat at the table when intermediaries and copyright owners negotiate "best practices" for mitigating online infringement, including which sanctions to impose, which content to remove, and which websites to block without judicial intervention.[18]

---

[15] Comments of the RIAA, *supra* note 9, at 2.

[16] *See* Ramon Lobato & Julian Thomas, *The Business of Anti-Piracy: New Zones of Enterprise in the Copyright Wars*, 6 INT'L J. COMMC'N 606, 612 (2012) (observing that Content ID "reflect[s] a significant reorientation in corporate IP policy, both by Google and various rights holders, toward a more pragmatic commercial engagement with copyright infringement").

[17] *See, e.g.*, IFPI, DIGITAL MUSIC REPORT 42 (2014), *available at* http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf. ("Search engines have pledged to do more to tackle online piracy, but there is still a long way to go."); Comments of the MPAA, *supra* note 8, at 4 (expressing disappointment in the best practices adopted by advertising networks and characterizing them as "merely an incremental step forward").

[18] *See* Niva Elkin-Koren, *After Twenty Years: Revisiting Copyright Liability of Online Intermediaries*, *in* THE EVOLUTION AND EQUILIBRIUM OF COPYRIGHT IN THE DIGITAL

This chapter surveys the current landscape of DMCA-plus enforcement by dividing such enforcement into two categories: Type 1 and Type 2. Type 1 DMCA-plus enforcement is cooperation by DMCA-covered intermediaries over and above what is required for safe harbor. Type 1 enforcers include broadband ISPs, UGC platform operators, and search engines. As shown in the table below, Type 1 enforcers have adopted voluntary, DMCA-plus measures in the form of graduated response, link demotion, and proactive content blocking. Type 2 DMCA-plus enforcement is cooperation by intermediaries that are not secondarily liable for their customers' copyright infringements and are thus not motivated by the need for safe harbor. Type 2 enforcers include payment system operators and advertising networks. As shown in the table below, Type 2 enforcers have adopted notice and termination protocols. Domain name registrars are a third category of Type 2 intermediary now in the crosshairs of both the copyright industries and the government agencies that watch out for their interests—IPEC and the Office of the United States Trade Representative ("USTR").[19] Efforts to deputize domain name registrars are nascent and, therefore, beyond the scope of this project, but it bears mentioning that if the copyright industries get their way, registrars will become active DMCA-plus enforcers in the near future.[20]

AGE 29, 45 (Susy Frankel & Daniel Gervais eds., 2014) (asserting that voluntary agreements often lack adequate safeguards for securing users' rights).

[19] *See MPAA & RIAA Demand DNS Action Against "Pirate" Domains*, TORRENTFREAK (May 14, 2015), https://torrentfreak.com/mpaa-riaa-demand-dns-action-against-pirate-domains-150514/ (reporting on a Congressional hearing at which a representative of the copyright industries testified that "domain name registrars . . . like other intermediaries in the e-commerce environment . . . must play their part to help address the plague of online copyright theft"); IPEC 2013 JOINT STRATEGIC PLAN, *supra* note 12, at 36 ("[IPEC] will continue to facilitate and encourage dialogue among different private sector entities that make the Internet function, which may include domain name registries and registrars . . . ."); UNITED STATES TRADE REPRESENTATIVE, 2014 OUT-OF-CYCLE REVIEW OF NOTORIOUS MARKETS 10 (2015) (identifying domain name registrars as a "new issue focus" in the USTR's "Special 301" process for targeting notorious global markets for piracy and counterfeiting).

[20] *See* Comments of the MPAA, *supra* note 8, at 8 ("Although implementation is still in the early stages, MPAA remains optimistic that the new ICANN requirements will be an important tool for combating copyright infringement on a more global level."). *But see* Brian Fung, *We Aren't the Copyright Cops, ICANN's President Says*, WASH. POST (June 9, 2015), https://www.washingtonpost.com/blogs/the-switch/wp/2015/06/09/we-arent-the-copyright-police-says-icanns-president/ (reporting on the ICANN president's vow to avoid mission drift in the face of pressure from interest groups to have ICANN regulate content online).

Enforcement Type	Intermediary Type	DMCA-Plus Measure
1	Broadband ISP	Graduated Response
	Search Engine	Link Demotion
	UGC Platform	Proactive Content Blocking
2	Payment Network	Notice and Termination/Blocking
	Advertising Network	
	(Domain Name Registrar?)	

II. Type 1 DMCA-plus enforcement

Type 1 DMCA-plus enforcement consists of voluntary, above-and-beyond measures that are undertaken by intermediaries whose compliance obligations are defined by the Section 512 safe harbors. To understand what it means for a service provider to exceed its safe-harbor obligations, it is first necessary to understand what those obligations are and how they vary depending upon the nature of the provider's operations and its relationship to allegedly infringing acts and actors.

To qualify for the statutory safe harbor, search engines and UGC platforms are required to comply with the notice-and-takedown protocol in Section 512(c) and with the obligation to terminate access for repeat infringers in Section 512(i). Under Section 512(c), a service provider is required, upon acquiring actual or "red flag" notice of a specific instance of infringement on its service, to promptly remove or disable access to the infringing content.[21] Under Section 512(i), a service provider is required to adopt and reasonably implement a program for terminating account access for repeat infringers in appropriate circumstances.[22] Broadband ISPs are not required to comply with the notice-and-takedown protocol in Section 512(c), because they do not control the content that transits their

[21] *See* 17 U.S.C. § 512(c) (setting forth the obligation of service providers seeking safe harbor to act promptly to take down allegedly infringing material upon receiving or acquiring notice that the material is infringing); § 512(c)(3)(A) (setting forth the required components of a DMCA notice).

[22] *See* 17 U.S.C. § 512(i) (requiring service providers to adopt and reasonably implement a policy for terminating the accounts of repeat infringers in appropriate circumstances and requiring service providers not to interfere with "standard technical measures" employed by copyright owners to prevent infringement of their works).

networks.[23] They are, however, required to comply with the repeat infringer provision in Section 512(i).[24]

In no case is safe harbor for any provider under the DMCA conditioned on that provider's affirmatively monitoring its service for infringing activity.[25] Notwithstanding the fact that this no-duty-to-monitor rule is explicit in Section 512(m), copyright owners have urged courts in high-profile litigation to hold that the DMCA's "red flag" notice provision implies a general obligation to monitor a site for infringement once a provider knows that some infringing content is present.[26] No court has ever accepted that argument, however, meaning that a service provider's prescribed enforcement role under the DMCA is reactive rather than proactive.[27] To the great frustration of rights owners, courts interpreting the DMCA have been clear that notice and takedown does not equate with notice and staydown. Accordingly, the service provider is not required to block an allegedly infringing file from being re-uploaded to its service after the file has been taken down in response to a copyright owner's notice.[28]

---

[23] *See In re* Charter Commc'ns, Inc., 393 F.3d 771, 776 (8th Cir. 2005) (noting that providers seeking safe harbor under § 512(a) do not have to comply with the DMCA's notice-and-takedown provisions).

[24] *See* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1109 (9th Cir. 2007) (stating that "[t]o be eligible for any of the four safe harbors at §§ 512(a)–(d), a service provider must first meet the threshold conditions set out in § 512(i)").

[25] *See* 17 U.S.C. § 512(m)(1) ("Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on . . . a service provider monitoring its service or affirmatively seeking facts indicating infringing activity.").

[26] *See, e.g.*, UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1110 (C.D. Cal. 2009) ("UMG argues that Veoh should have sought out actual knowledge of other infringing videos by searching its system for all videos by the artists identified in the RIAA notices."), *aff'd in relevant part sub nom.* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006 (9th Cir. 2013).

[27] *See id.* ("Requiring Veoh to perform such searches would…conflict with the principle…that the DMCA notification procedures place the burden of policing copyright infringement…squarely on the owners of the copyright.") (internal citation and quotation marks omitted).

[28] *Cf. id.* at 1111 ("UMG has not established that the DMCA imposes an obligation on a service provider to implement filtering technology . . . .").

Copyright owners have also urged courts to hold that the repeat infringer provision in Section 512(i) requires service providers to terminate users who have been the subject of multiple allegations of infringement in a single notice from a copyright owner.[29] Another interpretation of the repeat infringer provision once popular among rights owners is that a user should be "out" (i.e., have his or her account terminated or suspended) after a set number of "strikes" (i.e., consecutive notices of infringement)—usually three.[30] That approach, known as graduated response, never took hold in the case law interpreting Section 512(i).[31] Recognizing that Congress declined to specify any precise criteria for account termination when it adopted Section 512(i), no court has ever interpreted the DMCA's repeat infringer provision to require a provider to terminate a user's account after three (or any other specific number) of DMCA notices.[32] The case law is mixed even on the basic

---

[29] *See id.* at 1118 (declining to hold that Veoh was required to terminate access for a subscriber after a single notice alleging multiple instances of infringement).

[30] *Cf.* Liza Porteus Viana, *Three Strikes and You're Offline: Music Industry, ISPs May Cut Internet Access for File-Sharers*, FOX NEWS (Mar. 26, 2009), http://www.foxnews.com/story/2009/03/26/three-strikes-and-youre-offline-music-industry-isps-may-cut-internet-access-for.html (reporting on the copyright industries' support for mandatory three-strikes repeat infringer policies).

[31] Adoption of a "three strikes" model of graduated response would be sufficient but is not necessary to bring a provider within the protection of the safe harbors with respect to Section 512(i). *See* Annemarie Bridy, *Graduated Response and the Turn to Private Ordering in Online Copyright Enforcemen*t, 89 OR. L. REV. 81, 100 (2010). *See also* Disney Enters., Inc. v. Hotfile Corp., No. 11-20427-CIV, 2013 WL 6336286, at *24 (S.D. Fla. Sept. 20, 2013)

("Although the Court is mindful that the DMCA does not specify the characteristics of a reasonably implemented policy, it is unaware of any situation in which a three-strikes policy has been found to be ineffective.").

[32] *See* Corbis Corp. v. Amazon.com, Inc., 351 F. Supp. 2d 1090, 1101 (W.D. Wash. 2004) ("Given the complexities inherent in identifying and defining online copyright infringement, § 512(i) does not require a service provider to decide, *ex ante*, the specific types of conduct that will merit restricting access to its services. As Congress made clear, the DMCA was drafted with the understanding that service providers need not make difficult judgments as to whether conduct is or is not infringing.") (internal citation and quotation marks omitted).

question of whether a notice from a copyright owner, without more, can establish that a person is an infringer for statutory purposes.[33]

Whereas copyright owners have been unsuccessful in getting courts to interpret the DMCA to require proactive monitoring and graduated response, they have been successful in getting various service providers to agree to implement one or the other measure following private negotiations undertaken at the government's urging. In 2011, five of the largest broadband ISPs in the United States agreed in a Memorandum of Understanding ("MOU") with film and music industry trade groups to implement a "six strikes" graduated response protocol for mitigating unauthorized peer-to-peer file sharing.[34] In 2007 and 2014, respectively, UGC platforms YouTube and Vimeo began proactively filtering user uploads to block files that match reference files in a database populated by rights owners.[35] In addition, in 2012, Google voluntarily altered its search algorithm to demote "pirate sites" in search rankings.[36] What follows is a detailed discussion of these Type I DMCA-plus implementations.

---

[33] *Compare* Perfect 10 v. CCBill, 340 F. Supp. 2d 1077, 1088 (C.D. Cal. 2004) (concluding that "an internet service provider who receives repeat notifications that substantially comply with the requirements of § 512(c)(3)(A) about one of its clients, but does not terminate its relationship with the client, has not reasonably implemented a repeat infringer policy"), *rev'd in part on other grounds*, 488 F.3d 1102 (9th Cir. 2007) *with Corbis*, 351 F. Supp. 2d at 1105 (concluding that notices from a copyright owner function to bring a potential infringement to the provider's attention, but do not, in themselves, provide evidence of blatant copyright infringement, because they could be erroneous).

[34] *See* Annemarie Bridy, *Graduated Response American Style: "Six Strikes" Measured Against Five Norms*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1 (2012) [hereinafter Bridy, *Graduated Response American Style*]; Mary LaFrance, *Graduated Response by Industry Compact: Piercing the Black Box*, 30 CARDOZO ARTS & ENT. L.J. 165 (2012).

[35] *See* Steve Chen, *The State of Our Video ID Tools*, GOOGLE OFFICIAL BLOG (June 14, 2007), http://googleblog.blogspot.com/2007/06/state-of-our-video-id-tools.html (announcing beta testing of Content ID); David Murphy, *Vimeo Rolls Out "Copyright Match" for Flagging Content*, PCMAG.COM (May 22, 2014), http://www.pcmag.com/article2/0,2817,2458440,00.asp.

[36] *See* Chloe Albanesius, *Google to Demote Sites with "High Number" of Copyright Complaints*, PCMAG.COM (Aug. 10, 2012), http://www.pcmag.com/article2/0,2817,2408341,00.asp.

A. Graduated response by broadband access providers

The "six strikes" MOU creates what the parties characterize as a "common framework of 'best practices' to effectively alert subscribers, protect copyrighted content and promote access to legal online content."[37] The participating ISPs are AT&T, Verizon, Comcast, Cablevision, and Time Warner.[38] The participating copyright owners are the MPAA, the Recording Industry Association of America ("RIAA"), the American Association of Independent Music ("A2IM"), and the Independent Film and Television Alliance ("IFTA").[39] At the core of the common framework is the Copyright Alert System ("CAS"), a privately designed and administered enforcement system to which members of the public opt in through contractual terms of service with their broadband providers.[40] CAS operations are overseen by a specially created entity called the Center for Copyright Information ("CCI").[41] CAS applies only to users of residential broadband services and is intended to address infringement only over P2P networks.[42]

The CAS protocol consists of an escalating sequence of six warnings, or "copyright alerts," separated by seven-day grace periods.[43] To begin the process, a copyright owner sends a notice of infringement to a subscriber's ISP, which then generates an alert and sends it to the subscriber whose Internet protocol ("IP") address was identified in the notice.[44] To prevent ISPs from being overwhelmed by an unmanageable volume of notices, the MOU requires participating copyright owners to allocate among themselves an unspecified (but presumably fixed) number

---

[37] Mike Palmedo, Content Owners and ISPs Announce System of "Copyright Alerts" and "Mitigation Measures," INFOJUSTICE.ORG (July 7, 2011), http://infojustice.org/archives/4145.

[38] *See* MEMORANDUM OF UNDERSTANDING 24 (Attachment A) (July 6, 2011), *available at* http://www.copyrightinformation.org/wp-content/uploads/2013/02/Memorandum-of-Understanding.pdf [hereinafter MOU].

[39] *Id.* at 2, 25 (Attachment B).

[40] *Id.* at 7 (requiring party ISPs to amend their terms of service or acceptable use policies to incorporate CAS).

[41] *Id.* at 3–4.

[42] *See id.* at 2 (defining the scope of the program).

[43] *Id.* at 7. An ISP may send additional alerts during grace periods, but those alerts do not count toward the total number of six. *Id.* at 10.

[44] *Id.* at 7.

of notices per month.[45] In addition to that limit, ISPs have discretion to temporarily stop processing notices if the demand on their systems and resources becomes unreasonable.[46] Any temporary stoppage must be followed, however, by prompt notice to copyright owners and a collaborative effort to correct the "over-provisioning."[47]

The first two copyright alerts are educational in nature and require no response or action from the subscriber.[48] They explain that copyright infringement is illegal, that there are lawful ways of obtaining copyrighted content, and that users who persist in infringing copyrights will be subject to sanctions.[49] The third and fourth alerts contain sterner language and require the subscriber to acknowledge receipt.[50] The required acknowledgment can occur by means of either a click-through pop-up window or a click-through landing page to which the user's browser is diverted.[51] At the acknowledgment stage, the subscriber must indicate that he or she agrees to immediately stop any infringing conduct in which he or she may have been engaged.[52]

Sanctions, or "mitigation measures," are not triggered until a fifth alert is sent.[53] The MOU avoids being prescriptive when it comes to sanctions, specifying instead a range of mitigation measures from which ISPs can choose.[54] Such measures include, but are not limited to, a temporary reduction in transmission speed, a temporary step-down in the subscriber's service tier, a temporary redirection to a landing page for completion of a program of copyright instruction, a temporary redirection to a landing page until the subscriber contacts a customer service

---

[45] *Id.* at 16.

[46] *Id.*

[47] *Id.*

[48] *Id.* at 8–9. An ISP may elect to send only one educational alert instead of two. *See id.* at 8. The default number of alerts contemplated in the MOU, however, is six, with four coming after an initial "educational" step. *Id.* at 7–8.

[49] *Id*. at 8.

[50] *Id.* at 9–10.

[51] *Id.* at 10.

[52] *Id.* The subscriber also "agrees to instruct other users of the Subscriber's account to cease infringing conduct, if any exists." *Id.*

[53] *Id.* at 10–12.

[54] *Id.* at 11–12.

representative, or a temporary suspension of access.[55] No ISP operating under the MOU is required to suspend access for any subscriber.[56] (This point should be emphasized, because it represents a departure from the typical graduated response model, which prescribes termination of a user's account after a set number of "strikes.") In lieu of imposing a mitigation measure with the fifth alert, the ISP may elect to waive the measure and send a standalone fifth warning alert.[57] The sixth alert, however, must be accompanied by some mitigation measure.[58] The mitigation measure can be the same one that was applied with the fifth alert, assuming the sanction was not waived at that stage, or a different one.[59] After the sixth alert has been sent, the ISP has no further obligation to continue sending alerts to the subscriber, but it is required to keep count of any additional notices received from copyright owners concerning that subscriber.[60] At every stage, the system will "reset" for the subscriber if twelve months pass without the receipt of an additional alert.[61]

Before any mitigation measure is imposed, the recipient of a fifth or sixth alert has fourteen days to appeal the alert via a non-judicial process outlined in the MOU.[62] The appeal process, which the MOU calls the "Independent Review Program," is a non-exclusive dispute resolution system administered by the American Arbitration Association ("AAA") under contract with CCI.[63] The copyright owner representative and ISP groups split the overall costs of administration.[64] At the individual case level, an appealing subscriber pays a thirty-five dollar filing fee, which

---

[55] *Id.*

[56] *Id.* at 12.

[57] *Id.*

[58] *Id.* at 12–13.

[59] *Id.*

[60] *Id.* at 13.

[61] *Id.*

[62] *Id.* at 14.

[63] *Id.* at 26 (Attachment C); Press Release, Center for Copyright Information Announces Three Major Steps Towards Implementation (Apr. 2, 2012), http://www.copyrightinformation.org/press-release/center-for-copyright-information-announces-three-major-steps-towards-implementation/.

[64] MOU, *supra* note 38, at 14.

AAA may waive at its discretion.[65] The filing fee is refundable if the subscriber prevails in his or her appeal.[66] The appeal process is designed to be "automated to the maximum extent practicable."[67]

A single reviewer chosen by AAA from a panel of neutrals decides each appeal.[68] Reviewers must be lawyers, but they need not have the level of legal and case management experience that AAA arbitrators deciding other kinds of cases have.[69] All reviewers deciding CAS appeals are trained by a AAA-commissioned, CCI-approved copyright expert to apply prevailing legal principles as determined by federal courts.[70] By the terms of the MOU, this copyright expert must agree to receive input from the participating copyright owners as well as ISPs concerning what the prevailing legal principles are.[71]

A subscriber initiates an appeal by completing an online form wherein the subscriber asserts a defense or defenses to the allegations in the alert.[72] The MOU limits a subscriber's grounds for review to exactly six: (1) account misidentification; (2) unauthorized use of account; (3) authorized use of content; (4) fair use; (5) misidentification of content; and (6) work published before 1923.[73] The MOU mentions no other defenses, although a number of other defenses to copyright infringement claims are available to defendants in civil cases brought under the Copyright Act.[74] With respect to each of the six possible grounds for review, the burden of proof is on the subscriber, effectively creating a presumption of infringement.[75] Unless the subscriber overcomes that presumption, thereby winning her appeal, her ISP will impose a sanction.

---

[65] *Id.* at 30.

[66] *Id.* at 28.

[67] *Id.* at 34.

[68] *Id.* at 31.

[69] *Id.* at 33.

[70] *Id.* at 35.

[71] *Id.* at 35.

[72] *Id.* at 29.

[73] *Id.* at 26.

[74] *See* 17 U.S.C. §§ 107–122 (limitations on exclusive rights).

[75] *See* MOU, *supra* note 38, at 26–28 (explaining the standard of review for each of the six defenses).

When asserting one or more of the six cognizable grounds for review, the subscriber must provide sufficient factual information to allow the reviewer to evaluate the merits of the defense(s).[76] Once an appeal has been initiated, the reviewer also receives a standard package of information concerning the subscriber's contacts with CAS leading up to the appeal.[77] The reviewer may request supplemental information from the copyright owner or the ISP if she needs such information to decide the appeal.[78] Beyond requests for supplemental information, the MOU provides that there be no communication concerning pending appeals among the reviewer, the ISP, the copyright owner, and the subscriber.[79] The entire appeal process is designed to be completed within ten days of the reviewer's receipt of a complete file and within about thirty days of the initiation of the appeal.[80] If the subscriber prevails, the copyright alert in question is invalidated.[81]

In light of the program's light sanctions and educational focus, CAS has not been as controversial an implementation of graduated response as some of the more draconian "three strikes" programs operating abroad, which can entail monetary fines and sustained Internet disconnection.[82] In its first year of operation, CAS sent 1.3 million copyright alerts to broadband subscribers. It reported that it expected to double that number in 2014.[83] More than seventy percent of alerts fell within the first two steps of the process: education and acknowledgement. Fewer than three percent were sent in the final step of the protocol, at which imposition of a mitigation measure is mandatory.[84] Recipients of alerts filed 265 requests for review with AAA, 47 of which were

---

[76] *Id.* at 29.

[77] *Id.* at 31–32.

[78] *Id.* at 32.

[79] *Id.* at 33.

[80] *See id.* at 31–35 (prescribing deadlines for successive phases of the review process).

[81] *Id.* at 28.

[82] *See* Rebecca Giblin, *Evaluating Graduated Response*, 37 COLUM. J.L. & ARTS 147 (2014) (surveying statutory graduated response programs in France, New Zealand, South Korea, Taiwan, and the United Kingdom).

[83] CTR. FOR COPYRIGHT INFO., THE COPYRIGHT ALERT SYSTEM: PHASE ONE AND BEYOND 1 (2014), *available at* http://www.copyrightinformation.org/wp-content/uploads/2014/05/Phase-One-And_Beyond.pdf.

[84] *Id.*

successful.[85] CCI's claims for the program during its first year of operation were modest. In its end-of-year report, it asserted that the program's educational message is reaching consumers, and it expressed the view that CAS will be even more effective when it scales up to reach a wider population of P2P users.[86] Time will tell. Scholars evaluating France's statutory graduated response program, Hadopi, have been mixed in their empirical assessments of its efficacy for reducing infringement and steering users toward licensed services.[87]

B. Proactive filtering by UGC platforms

Although the DMCA does not impose an affirmative monitoring obligation on intermediaries seeking safe harbor, the popular video-sharing sites YouTube and Vimeo offer content screening and filtering tools that can be configured by copyright owners to block users from uploading copyrighted content. Each platform implemented its program—Content ID for YouTube; Copyright Match for Vimeo—while copyright litigation was pending against it in federal court. Google launched Content ID shortly after acquiring YouTube and getting sued by Viacom and other copyright industry plaintiffs for billions of dollars in statutory damages.[88] Vimeo adopted Copyright Match not long after it was handed a mixed summary judgment ruling in a lawsuit brought by Capitol Records and other record labels.[89] In both cases, Google and Vimeo asserted the

---

[85] *Id.*

[86] *Id.* at 3.

[87] *Compare, e.g.*, Brett Danaher et al., *The Effect of Graduated Response Anti-Piracy Laws on Music Sales: Evidence from an Event Study in France*, 62 J. INDUS. ECON. 541, 542 (2014) (finding that increased consumer awareness of a graduated response law in France caused iTunes music sales in France to increase by 22–25%) *with* Michael Arnold et al., *Graduated Response Policy and the Behavior of Digital Pirates: Evidence from the French Three-Strike (Hadopi) Law* (May 28, 2014), *available at* http://ssrn.com/abstract=2380522 (concluding that the French graduated response law has had no significant deterrent effect).

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

[89] *See* Capitol Records, LLC v. Vimeo, LLC, 972 F. Supp. 2d 500 (S.D.N.Y. 2013) (denying in part Vimeo's motion for summary judgment); Todd Spangler, *Vimeo Starts Scanning Videos for Copyright Violations*, VARIETY (May 21, 2014), https://variety.com/2014/digital/news/vimeo-starts-scanning-videos-for-copyright-violations-1201188152/ (reporting on Vimeo's launch of Copyright Match).

DMCA's Section 512(c) safe harbor as an affirmative defense to the plaintiffs' claims of copyright infringement.

Content ID and Copyright Match preempt the DMCA's reactive content-removal mechanism by giving copyright owners the option to prevent disputed content from "going up" in the first place. The technology underlying both systems relies on digital fingerprinting to sample an uploaded file and compare it against a database of reference files provided by participating copyright owners.[90] With Content ID, if the comparison between an uploaded file and a reference file results in a match, Google will apply one of four policies, based on what the copyright owner elected when it enrolled in the program: (1) it will mute matched audio in an uploaded video; (2) it will completely block a matched video; (3) it will monetize a matched video for the copyright owner by running advertisements against it; or (4) it will track a matched video's viewership statistics.[91] According to Google, most copyright owners elect to monetize content, making Content ID both an anti-piracy tool and a revenue generator for Google and copyright owners, who share the ad-generated revenue.[92]

Content ID's policies can be tailored, so that copyright owners can block uploaded content in some instances and monetize in others, depending on the extent to which an uploaded file and its corresponding reference file match.[93] For example, a copyright owner can elect to monetize an uploaded video that contains less than a specified amount or proportion of matched content while blocking any uploaded video that

---

[90] *See* Brad Stone & Miguel Helft, *New Weapon in Web War over Piracy*, NY TIMES (Feb. 19, 2007), http://www.nytimes.com/2007/02/19/technology/19video.html (discussing fingerprinting technologies for identifying audio and video). For a technical discussion of how fingerprinting is used to identify copyrighted content, see Craig Seidel, *Content Fingerprinting from an Industry Perspective*, IEEE 2009, 1524–27.

[91] *How Content ID Works*, YOUTUBE, https://support.google.com/youtube/answer/2797370?hl=en-GB.

[92] GOOGLE, HOW GOOGLE FIGHTS PIRACY 10 (2014), *available at* https://drive.google.com/file/d/0BwxyRPFduTN2NmdYdGdJQnFTeTA/view.

[93] Kyle Harrison, *Over 1,000 Content Owners Now Using Content ID*, YOUTUBE BIZ BLOG (Sept. 16, 2009), http://ytbizblog.blogspot.com/2009/09/over-1000-content-owners-now-using.html.

contains more.[94] The system is also capable of blocking audio and video independently of each other, so that the video portion of an uploaded file containing a matched copyrighted sound recording can stay up even if the sound recording copyright owner wants the audio portion blocked.[95] In such cases, Google offers users the ability to swap a licensed sound recording file for the blocked one.[96]

Vimeo has not stated publicly what options it gives to participating copyright owners, but Audible Magic, the technology vendor with which Vimeo contracts for the service, describes a process in which the copyright owner's "business rules"—indicating whether matched content should be blocked or allowed—are automatically conveyed to its customer along with confirmation of a match.[97] The company's literature goes on to explain that copyright owners and UGC platforms sometimes negotiate direct licensing agreements and specify business rules that include tracking or monetization.[98] Based on Audible Magic's general description of the service it provides to Vimeo, Copyright Match closely resembles Content ID in terms of the options it makes available to copyright owners.

Both programs allow users to dispute a copyright owner's claim on content. With Content ID, a user can dispute a claim if she believes the system misidentified her uploaded video or if she has the rights required to use the video.[99] Google provides a fillable web form for submitting Content ID disputes. After a user has submitted a dispute, the copyright owner has thirty days to respond. If the copyright owner fails to respond within thirty days, the claim expires. A responding copyright owner can choose to either release the claim or uphold the claim. If the copyright owner upholds the claim, the user can appeal if she acts within a set period

---

[94] *Id.*

[95] *Id.*

[96] *What Is a Content ID Claim?*, YOUTUBE, https://support.google.com/youtube/answer/6013276?hl=en.

[97] Audible Magic, *Copyright Compliance Service: Compliance Automation for Media Sharing Platforms*, AUDIBLE MAGIC, https://www.audiblemagic.com/compliance-service/#how-it-works/.

[98] *Id.*

[99] *Dispute a Content ID Claim*, YOUTUBE, https://support.google.com/youtube/answer/2797454.

of time and has a verified account in good standing. If the user appeals, the copyright owner again has thirty days to respond and can either release the claim or file a DMCA takedown notice to have the content removed. With Copyright Match, a user can dispute a match on grounds that she is using the content with permission, she is using the content in keeping with fair use, or she is using content that the system misidentified.[100] Like Content ID, Copyright Match allows a user to prevent a video containing claimed audio from being blocked by swapping the claimed audio track with a licensed track from Vimeo's catalog.

In 2014, Google reported that the Content ID program generates hundreds of millions of dollars in revenue per year for over 5,000 partners that have contributed more than 25 million active reference files to the database.[101] The system, it seems, is working well for both Google and copyright owners. Some users have complained, however, that the system overblocks, that it presumes a user's guilt by automatically diverting revenue to a copyright owner as soon as a claim is filed, and that its dispute resolution process can take up to a month to play out.[102]

C. Search demotion

A search engine operator is potentially liable for contributory copyright infringement, insofar as it "substantially assists websites to distribute their infringing copies to a worldwide market and assists a worldwide audience of users to access infringing materials."[103] Search engines fall within the scope of the DMCA's safe harbor for "information

---

[100] *Copyright Match*, VIMEO, https://vimeo.com/help/faq/legal-stuff/copyright-match/.

[101] GOOGLE, *supra* note 92, at 3, 10.

[102] *See* Erik Kain, *YouTube Responds to Content ID Crackdown, Plot Thickens*, FORBES.COM **(**Dec. 17, 2013), http://www.forbes.com/sites/erikkain/2013/12/17/youtube-responds-to-content-id-crackdown-plot-thickens/ (documenting cases of overblocking); Paul Tassi, *The Injustice of the YouTube Content ID Crackdown Reveals Google's Dark Side*, FORBES.COM (Dec. 19, 2013), http://www.forbes.com/sites/insertcoin/2013/12/19/the-injustice-of-the-youtube-content-id-crackdown-reveals-googles-dark-side/ (complaining about presumption of guilt, automatic revenue diversion, and lengthy dispute resolution).

[103] Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007).

location tools" and are required to comply with the notice and takedown protocol in Section 512(c) as a condition for safe harbor eligibility. Operationally speaking, a search engine indexes the entire contents of the public World Wide Web in order to return relevant and comprehensive search results in response to user queries. When a search engine user queries a popular song or film title, the results returned—to the extent that they are complete—will inevitably include links to "pirate sites." How prominently those links are featured is a major source of disagreement between trade groups representing corporate copyright owners and those representing search providers.

According to the International Federation for the Phonographic Industry ("IFPI"), a music industry trade group, links to websites containing infringing content dominate search results for all three major search engines (Google, Yahoo!, and Bing), and almost three-quarters of consumers surveyed said they used search engines as a "discovery or navigational tool" to find unlicensed services.[104] The Computer and Communications Industry Association ("CCIA"), a trade group to which Google and the other major search providers belong, countered those findings, citing a statistic that only fifteen percent of traffic to alleged "pirate sites" was referred by search engines.[105] Moreover, the CCIA asserted, operators of licensed content services do little to optimize their sites in ways that would organically improve their search rankings.[106] Such public sparring across industry trade groups is a clear sign that search has become a major battleground in the Internet's ongoing copyright wars. When it comes to policy makers, it appears that the copyright industries are landing their punches. In a Congressional hearing in 2014 on possible amendments to the DMCA safe harbors, members of the House Judiciary Committee Subcommittee on Courts, Intellectual Property, and the

---

[104] IFPI, DIGITAL MUSIC REPORT 29 (2013), *available at* http://www.ifpi.org/content/library/DMR2013.pdf; IFPI, DIGITAL MUSIC REPORT (2014), *supra* note 17, at 42.

[105] MATT SCHRUERS, THE SEARCH FIXATION: INFRINGEMENT, SEARCH RESULTS, AND ONLINE CONTENT 2 (2013), *available at* http://cdn.ccianet.org/wp-content/uploads/2013/08/CCIA_TheSearchFixation.pdf.

[106] *Id.* at 5.

Internet peppered Google's representative with questions about what more Google can do with search to voluntarily fight online piracy.[107]

As the dominant player in the market for online search, Google has been a primary target of anti-piracy efforts for the film and music industries.[108] Industry trade groups and some of their larger member firms contract with a growing number of third party vendors to both identify infringing links in web searches and send DMCA takedown notices to Google and other search providers.[109] In recent years, Google has streamlined the takedown process for search by designing and implementing automated tools for bulk submission of Section 512 notices.[110] These tools include the Trusted Copyright Removal Program, which allows large copyright owners with a proven track record for submitting accurate notices to become "trusted partners" for the purpose of submitting DMCA notices in bulk.[111] The number of links Google removes from search results in response to copyright notices on an annual basis is staggering. For example, in 2013, Google removed over 222 million links to unique web addresses (URLs).[112] It reports that the average turnaround time for the removal of a link subject to a copyright owner notice is now less than six hours.[113] In copyright litigation over its

---

[107] *See Section 512 of Title 17: Hearing Before the Subcomm. on Courts, Intellectual Prop., and the Internet of the H. Comm. on the Judiciary*, 113th Cong. 82ff (2014) [hereinafter *Section 512 Hearing*].

[108] *See generally* Daniel Seng, *The State of the Discordant Union: An Empirical Analysis of DMCA Takedown Notices*, 18 VA. J.L. & TECH. 369 (2014).

[109] *See id.* at 395 (discussing the rise of third-party DMCA reporters and reporting agents).

[110] *Section 512 Hearing*, *supra* note 107, at 47-48 (Testimony of Katherine Oyama, Sr. Copyright Policy Counsel, Google, Inc., at 4-5), *available at* http://judiciary.house.gov/_cache/files/be93d452-945a-4fff-83ec-b3f51de782b3/031314-testimony---oyama.pdf.

[111] GOOGLE, *supra* note 92, at 14.

[112] *See* Dave Lee, *Google Changes "To Fight Piracy" by Highlighting Legal Sites*, BBC NEWS (Oct. 20, 2014), http://www.bbc.com/news/technology-29689949.

[113] GOOGLE, *supra* note 92, at 3.

content removal practices for search, Google has been held to qualify for the Section 512(d) safe harbor.[114]

The film and music industries argue, however, that bulk removal of links from search results is insufficient cooperation from search engine operators.[115] The IFPI, the RIAA, and the MPAA have all demanded that search engine operators work more aggressively to channel users to licensed content services and away from unlicensed ones.[116] They have also asked Google to alter the operation of the autocomplete function, which predicts the next term in a user's incomplete search query based on how the majority of past users completed queries using the same initial terms.[117] Over time, Google has acceded to both requests. It altered its PageRank search algorithm in 2012 to take into account the number of DMCA-compliant notices received for a given website.[118] The PageRank algorithm is proprietary, and beyond stating that the number of DMCA notices received for a given site is "one signal among the hundreds" that it weighs when ranking search results, Google has never disclosed how much weight it gives to this factor. With respect to autocomplete, Google promised in 2010 to prevent terms closely associated with piracy from appearing in autocomplete results.[119] In 2014, it began demoting

---

[114] Perfect 10, Inc. v. Google, Inc., No. CV 04-9484 AHM SHX, 2010 WL 9479059, at *1 (C.D. Cal. July 26, 2010) (granting partial summary judgment for Google on its § 512(d) defense for web and image search).

[115] RIAA, *Google's New Report: Big on Data, But Where's the Impact?*, MUSIC NOTES BLOG (Sept. 10, 2013), http://www.riaa.com/blog.php?content_selector=riaa-news-blog&blog_selector=wheres-the-impact&news_month_filter=9&news_year_filter=2013 ("At least in the case of search results . . . it is increasingly clear we are making insufficient progress against piracy.").

[116] IFPI, DIGITAL MUSIC REPORT (2013), *supra* note 104, at 29.

[117] *See* Ernesto, *RIAA Wants Google to Implement Five-Point Anti-Piracy Plan*, TORRENTFREAK (Jan. 14, 2014), http://torrentfreak.com/riaa-demands-google-deal-with-piracy-140114/ (reporting on the RIAA's demand that Google "[s]top leading users to illegal sites through autocomplete").

[118] *See* Andrea Peterson, *How Google Search Is Changing To Fight Online Piracy*, WASH. POST (Oct. 20, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/10/20/how-google-search-is-changing-to-fight-online-piracy/.

[119] Kent Walker, *Making Copyright Work Better Online*, GOOGLE PUBLIC POLICY BLOG (Dec. 2, 2010), http://googlepublicpolicy.blogspot.com/2010/12/making-copyright-work-better-online.html.

autocomplete predictions that returned search results containing a large number of DMCA-demoted sites.[120]

Copyright owners have been less than pleased with Google's efforts at demoting "pirate sites" in search results. A study commissioned by the MPAA compared the three months before and after implementation of the demotion signal and found that the share of search referrals to the 2,000 sites that appeared most often in DMCA takedown notices actually increased slightly, from nine percent to almost ten percent.[121] The RIAA released its own "report card" six months after the algorithm change, concluding that "[the demotion] signal does not result in a meaningful change in search rankings of noticed sites on the first page of search results when a user searches for an mp3 or download of popular songs."[122] In 2014, Google reported that it had further refined the DMCA demotion signal in search, but it did not specify the nature of the refinement.[123] It also pointed out that users do not typically formulate their search queries in the ways tested by the RIAA and MPAA (i.e., with the words "mp3," "free stream," or "download" following a movie or song title); rather, they usually search simply for the name of an artist or the title of a song or movie.[124] Google search queries formulated as users typically formulate them do not return results with "pirate sites" on the first pages.[125]

III. Type 2 DMCA-plus enforcement

---

[120] Katherine Oyama, *Continued Progress on Fighting Piracy*, GOOGLE PUBLIC POLICY BLOG (Oct. 17, 2014), http://googlepublicpolicy.blogspot.com/2014/10/continued-progress-on-fighting-piracy.html.

[121] MILLWARD BROWN DIGITAL, UNDERSTANDING THE ROLE OF SEARCH IN ONLINE PIRACY 10 (2014), *available at* http://www.mpaa.org/wp-content/uploads/2014/03/Understanding-the-role-of-search-in-online-piracy.pdf.

[122] RIAA, SIX MONTHS LATER—A REPORT CARD ON GOOGLE'S DEMOTION OF PIRATE SITES 2 (2013), *available at* http://riaa.com/media/3CF95E01-3836-E6CD-A470-1C2B89DE9723.pdf.

[123] GOOGLE, *supra* note 92, at 18.

[124] *Id.* at 19.

[125] *Id.*

Type 2 DMCA-Plus enforcement is comprised of voluntary measures undertaken by intermediaries that fall outside the ambit of the DMCA because their activities do not subject them to secondary copyright liability. Type 2 intermediaries include payment system operators, such as MasterCard, Visa, and PayPal, and advertising networks, such as Google and Yahoo!. These intermediaries give websites the wherewithal to generate revenue, which has made them a logical target for copyright owners seeking to choke the flow of money to "pirate sites." In its 2013 green paper, *Copyright Policy, Creativity, and Innovation in the Digital Economy*, the Department of Commerce Internet Policy Task Force identified a "follow the money" approach as one among several "potential new tools" for addressing "the gaps and shortcomings in existing legal tools" for fighting online piracy.[126]

"Existing legal tools" do not capture Type 2 intermediaries because their relationship to direct infringers and acts of direct infringement is too attenuated. That, at any rate, is what the Ninth Circuit Court of Appeals held in *Perfect 10 v. Visa*, a closely watched case that tested the reach of copyright's secondary liability rules in the e-commerce environment.[127] Perfect 10 argued that Visa was contributorily and vicariously liable for infringement of its copyrighted images because Visa accepted payments from websites on which those infringements occurred.[128] The court rejected Perfect 10's argument as to both theories of secondary liability. On the question of contributory infringement, it held that having "the power to undermine the commercial viability of infringement" does not constitute material contribution to infringement or inducement to infringe.[129] The court's conclusion that Visa and other payment-industry defendants could not be held liable as contributory infringers rested in part on the finding that they did not aid users in locating

---

[126] DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COPYRIGHT POLICY, CREATIVITY, AND INNOVATION IN THE DIGITAL ECONOMY 61, 67–70 (2013), *available at* http://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf.

[127] Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788 (9th Cir. 2007). Judge Kozinski filed a sharp dissent in the case, and legal scholars have recognized the extent to which the outcome was policy driven in the face of unstable doctrine. *See* Mark Bartholomew & Patrick F. McArdle, *Causing Infringement*, 64 VAND. L. REV. 675, 711 (2011).

[128] *Perfect 10*, 494 F.3d at 792.

[129] *Id.* at 800.

infringing material—unlike search engines—and in part on the finding that they did not store or route any infringing material on or across their payment networks.[130] On the question of vicarious infringement, the court held that a payment processor's ability to affect online infringement by making it less profitable is not the same as an ability to supervise and control infringing activity, which is required for vicarious liability.[131] The same reasoning extends to advertising networks, which are situated similarly to payment systems in terms of their relationship to the infringing activities that occur on their customers' websites: although advertising networks have the power to make direct infringement on third-party websites less profitable, they do not provide the site or facilities for infringing acts, and they do not have the ability to control or supervise those acts.[132]

From a policy perspective, well-defined and carefully circumscribed secondary liability rules are necessary to prevent the unfairness that could easily result from making one party pay for another's bad acts.[133] Rights owners, however, view limitations on the scope of secondary liability for Type 2 intermediaries as a bug, not a feature of copyright law. They believe that "all players in the Internet ecosystem," meaning everyone in a position to do anything to reduce infringement, should function as deputy enforcers, regardless of their ability to directly control infringing content.[134] In 2011, with prodding from IPEC, five major payment networks—American Express, Discover, MasterCard,

---

[130] *Id.*

[131] *See id.* at 804 ("Defendants . . . cannot take away the tools the offending websites use to reproduce, alter, and distribute the infringing images over the Internet. They can only take away the means the websites currently use to sell them.").

[132] A disclaimer to this effect appears in the opening paragraphs of the best practices document that advertising networks adopted in 2013. *See* Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting 1, *available at* http://blog.aol.com/2013/07/15/ad-networks-best-practices/ ("Ad Networks do not control the content on third-party websites and are not able to remove websites from the Internet.").

[133] *See* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 435 (1984) (acknowledging that secondary infringement liability presents the "problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another").

[134] Comments of the MPAA, *supra* note 8, at 2.

Visa, and PayPal—agreed to a set of voluntary best practices to combat online piracy and counterfeiting.[135] In 2013, the major online advertising networks—AOL, Google, Microsoft, and Yahoo!—did the same.[136]

A. Notice and termination by payment processors

Payment processors implemented their best practices agreement in January 2012 with the launch of the Payment Processor Initiative, an inter-industry enforcement effort run by the International AntiCounterfeiting Coalition ("IACC") under the registered trademark "RogueBlock."[137] Following the program's initial implementation, PULSE and Diners Club joined.[138]

The IACC's role in administering the RogueBlock Payment Processor Initiative is roughly analogous to the role that CCI plays in administering CAS.[139] Similar to the graduated response protocol in CAS, to which broadband users become bound through terms of service with their providers, the enforcement protocol in the best practices agreement becomes binding on merchants through payment processors' policies, which prohibit the use of card services for illegal transactions.[140] There is,

---

[135] *See* IPEC 2013 JOINT STRATEGIC PLAN, *supra* note 12, at 36.

[136] *See* Victoria Espinel, *Coming Together to Combat Online Piracy and Counterfeiting*, WHITE HOUSE BLOG (July 15, 2013), https://www.whitehouse.gov/blog/2013/07/15/coming-together-combat-online-piracy-and-counterfeiting.

[137] *See IACC Payment Processor Initiative*, IACC, http://www.iacc.org/rogueblock.html (stating that "[t]he initiative launched in January 2012, following rights-holder negotiations with the payment industry to develop a set of best practices in addressing rogue websites, as encouraged by the U.S. Intellectual Property Enforcement Coordinator, Victoria Espinel").

[138] *See Payment Processor Initiative & Portal Program*, https://web.archive.org/web/20130119105913/http://c.ymcdn.com/sites/members.iacc.org/resource/resmgr/IACC_PaymentProcessorInitiat.pdf (listing participating payment processors).

[139] *See* Bridy, *Graduated Response American Style*, *supra* note 34, at 27–30 (explaining the role of the Center for Copyright Information).

[140] *See* KRISTINA MONTANARO, IACC PAYMENT PROCESSOR PORTAL PROGRAM: FIRST YEAR STATISTICAL REVIEW 3 (2012), *available at* http://www.gacg.org/Content/Upload/MemberNewsDocs/October%202012%20Report%20to%20IPEC%20-%20FINAL.pdf ("The Portal Program is dependent on Card

however, a very important difference between the voluntary best practices agreement for payment processors and the MOU that created CAS: the former is, by its express terms, not legally binding on the participating parties.[141] Although the terms of the agreement are sufficiently specific to be enforced, the parties disclaim contractual intent.

At the core of the best practices agreement for payment processors is a notice-and-termination protocol. The protocol is operationalized through the RogueBlock "Portal Program," which is a web-based software system for managing communications between rights owners and payment processors concerning alleged "rogue sites."[142] Copyright and trademark owners pay annual fees for access to the program.[143] The program's front end is a secure online portal through which participating rights owners submit complaints containing information specified in the best practices agreement.[144] The Portal provides a standardized, fillable web form for this purpose.[145] On the program's back end, the IACC reviews complaints and relays them to the relevant payment processor, which takes action as specified in the best practices agreement.[146] The payment processor then reports back to the IACC about the outcome of each complaint. Rights owners can track the status of complaints and view outcomes via the online portal.[147]

A complaint from a rights owner under the agreement must contain four elements to be actionable: (1) a description of the alleged infringement and the "Illegitimate Products," including the identity of the

---

Network policies, which prohibit merchants from using card services for illegal transactions. Use of card services for sales of counterfeit or pirated goods constitutes a breach of these policies, and thus provides for remediation of the corresponding merchant account.").

[141] *See* Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet 4 (May 16, 2011) ("These best practices are voluntary and not legally binding.") (on file with author).

[142] *See IACC Payment Processor Initiative*, *supra* note 137.

[143] *Payment Processor Initiative & Portal Program*, *supra* note 138.

[144] *Id.*

[145] *See* MONTANARO, *supra* note 140, at 5 (reproducing a screen shot of the standardized form).

[146] *See Payment Processor Initiative & Portal Program*, *supra* note 138.

[147] *Id.*

website in question; (2) evidence that infringing products are available on the website using the payment processor's services (e.g., a screenshot of a payment processor's logo on the site); (3) a copy of a cease-and-desist letter or DMCA notice from the rights owner notifying the website's owner of the allegation of infringement, or an attestation that, to the best of the rights owner's knowledge, the site is not licensed or authorized to distribute the products; and (4) evidence that the requester owns the copyright or trademark in question.[148] If the payment processor requires additional information concerning the complaint, the rights owner must provide the information promptly.[149] The agreement does not require test transactions as part of the complaint submission.[150] Nor does it require any pre-complaint direct communication between the rights owner and the accused merchant.

Upon receiving a complaint, the payment processor must conduct an investigation.[151] Once a complaint has been filed, the agreement puts the onus on the accused merchant to produce "credible evidence" that it is not engaged in infringing transactions.[152] If the merchant fails to respond or doesn't meet its burden, or if the payment processor "determines in its reasonable opinion that the merchant is engaged in sales of Illegitimate Products," then the merchant is ordered to block future infringing transactions.[153] If the merchant continues to engage in such transactions, then the payment processor "shall suspend or terminate payment services to that merchant with United States account holders."[154] The agreement

---

[148] Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet, *supra* note 141, at 1-2.

[149] *Id.* at 2.

[150] *Id.* at 1.

[151] *Id.* at 2.

[152] *Id.*.

[153] *Id.*

[154] *Id.*

contemplates but does not specify additional "appropriate remedies."[155] Termination is the typical sanction.[156]

For merchants that believe they have been wrongly sanctioned, payment processors must "have a process in place to allow for prompt review of remedial measures."[157] The agreement is silent, however, as to what or how much process is due when a merchant requests a review. There is no provision for third-party review or for a stay of termination pending resolution of the review.[158] In cases where the merchant disputes termination, and the payment processor reasonably concludes that the accused merchant is operating legitimately, the agreement implicitly contemplates that the payment processor may nevertheless impose or sustain termination if the rights owner is willing to indemnify it for any resulting legal liability.[159] This risk-shifting provision effectively gives the complaining rights owner final say over termination decisions.

In 2013, the IACC reported that 26,000 payment channels[160] on 7,500 accused websites and over 2,100 individual merchant accounts had

---

[155] *Id.* at 3.

[156] *See Payment Processor Initiative & Portal Program*, *supra* note 138 ("How do I know the results of my submitted claims? The information received back from the Trace Message will identify the merchant processing the transactions. Typically, that merchant is then terminated. . . .").

[157] Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet, *supra* note 141, at 3.

[158] This is in contrast with the CAS, which provides for a stay of sanctions pending review. *See* Bridy, *Graduated Response American Style*, *supra* note 34, at 33–37 (explaining the process for appealing a mitigation measure in CAS).

[159] *See* Best Practices to Address Copyright Infringement and the Sale of Counterfeit Products on the Internet, *supra* note 141, at 3 ("A Payment System Operator may request a written agreement by the Right-Holder to support the Payment System Operator fully in connection with a dispute where, in the Payment System Operator's reasonable opinion, the merchant provides credible evidence supportive of the merchant's position that it is not engaged in illegal conduct, including by defending, holding harmless and indemnifying the Payment System Operator for any costs, expenses (including legal fees) or liabilities arising in connection with such dispute.").

[160] A website has multiple payment channels if it accepts cards or payments from multiple payment processors.

been terminated.[161] The cost of account termination for a merchant is high, considering that it can take at least a week to establish a new merchant account, assuming the terminated merchant can meet the due-diligence requirements of a new card-servicing bank.[162] Given the high cost of error for a terminated merchant, it is troubling that the payment processors' best practices agreement provides no stay of termination pending review and no specific set of dispute-resolution procedures for merchants that contest termination of their accounts. And because payment processors can look to rights owners for indemnification if a merchant decides to fight termination, error costs for payment processors are relatively low, which may create an incentive for them to overblock.

B. Notice and termination by advertising networks

The voluntary best practices agreement for advertising networks is less detailed in its prescriptions than the one for payment processors, but it incorporates the same basic notice-and-termination protocol and becomes binding on a network's customers in the same way—through terms of service. Each network agrees as an initial matter to maintain and publish policies prohibiting network participation by websites that are "principally dedicated to . . . engaging in copyright piracy and have no substantial non-infringing uses."[163] There is no central clearinghouse or portal for administering the advertising network best practices; instead, each participating network agrees to establish and implement its own internal procedures. This differs from the IACC's "one size fits all" implementation for payment processors. As in the best practices agreement for payment processors, the best practices agreement for advertising networks expressly disclaims contractual intent.[164] It also

---

[161] *Role of Voluntary Agreements Hearing*, *supra* note 13, at 56 (Written Testimony of Robert C. Barchiesi on Behalf of the IACC, at 5).

[162] MONTANARO, *supra* note 140, at 14.

[163] Best Practices Guidelines for Ad Networks to Address Piracy and Counterfeiting, *supra* note 132, at 2.

[164] *Id.* at 3 ("[I]t is understood that the voluntary best practices reflected in this Statement should not, and cannot, be used in any way as the basis for any legal liability or the loss of any applicable immunity. . . .").

expressly disclaims any affirmative monitoring obligation, essentially importing the DMCA's no-duty-to-monitor rule.[165]

A copyright owner initiates the notice-and-termination process by filing a complaint with a participating advertising network.[166] To be actionable, a complaint must contain six elements, many of which overlap with the elements of a DMCA notice under Section 512(c)(3)(A): (1) a description of the alleged illegitimate activity, including the specific URL where the activity is occurring, and contact information for the accused website; (2) evidence of the allegedly infringing activity in the form of a time-and-date stamped screenshot of the website showing an advertisement from the network displayed on the site; (3) a copy of a DMCA notice or a cease-and-desist letter sent to the operator of the website; (4) a statement under penalty of perjury that the complainant has a good faith belief that the allegedly infringing activity is unauthorized, and that the complainant is either the copyright owner or the copyright owner's authorized agent; (5) contact information for the copyright owner; and (6) a physical or electronic signature of the complainant.[167] Unlike the best practices for payment processors, which do not condition the filing of a complaint on any prior contact between the complainant and the targeted website, the best practices for advertising networks require a complainant to have contacted the accused website operator first. This policy reflects the principle, made explicit in the agreement, that best practices should "encourage and supplement, not replace, responsible and direct independent actions taken by intellectual property owners to enforce their intellectual property rights."[168]

Following receipt of a sufficiently specific complaint, the advertising network undertakes an "appropriate investigation."[169] In its investigation, the network may consider any credible evidence submitted by the accused website to rebut the claim that it is principally dedicated to

---

[165] *Id.*

[166] *Id.* at 2.

[167] *Id.* at 4–5.

[168] *Id.* at 1.

[169] *Id.* at 3.

piracy and lacks substantial non-infringing uses.[170] Such evidence may consist of a DMCA counter-notice—yet another instance of conscious parallelism between the advertising network best practices and the DMCA.[171] If, after investigation, the network concludes that the complaint was legitimate, it may impose one of a number of sanctions: it may ask the accused website to stop engaging in infringing activity; it may stop serving ads on the accused website as whole, or only on certain pages within the website, until it verifies that the infringing activity has stopped; or it may terminate the website from the network.[172] Unlike the best practices for payment processors, the best practices for advertising networks do not include any review or appeal process for a website that wishes to contest an adverse finding against it. The threshold for an adverse finding is much higher with advertising networks, however, than it is with payment processors; payment processors terminate merchants without first having to find that their websites are principally dedicated to piracy and lack substantial non-infringing uses.

Public interest groups view the advertising networks' strict standard for termination favorably, because it limits non-judicial enforcement to clear-cut cases involving demonstrably bad actors, leaving close or ambiguous cases to traditional dispute resolution fora.[173] The MPAA, by contrast, is critical of the advertising networks' best practices, complaining that they "place nearly all of the burden of ensuring that ads do not appear on sites dedicated to piracy upon rightsholders."[174] That allocation of burdens, in which copyright owners are primarily responsible for enforcing their own rights online, is consistent with the congressional intent expressed in the DMCA.[175] It appears skewed only when viewed

---

[170] *Id.*

[171] *Id.* For the required elements of a DMCA counter-notice, see 17 U.S.C. § 512(g)(3).

[172] *Id.*

[173] *See, e.g.*, David Sohn, *Ad Networks Pledge Voluntary Practices Against Piracy*, CTR. FOR DEMOCRACY & TECH. BLOG (July 16, 2013), https://cdt.org/blog/ad-networks-pledge-voluntary-practices-against-piracy/.

[174] Comments of the MPAA, *supra* note 8, at 5.

[175] *See* UMG Recordings, Inc. v. Shelter Capital Partners LLC, 718 F.3d 1006, 1022 (9th Cir. 2013) ("Congress made a considered policy determination that the DMCA . . . would place the burden of policing copyright infringement . . . squarely on the owners

from the DMCA-plus perspective that rights owners and online intermediaries are somehow equally responsible for online enforcement and equally well situated (if intermediaries are not better situated) to undertake it. Notably, the DMCA-plus perspective represents a significant departure from existing secondary liability doctrines in intellectual property law.[176]

IV. Conclusion

The DMCA-plus era of online copyright enforcement is well underway. In this post-DMCA world, online intermediaries of all shapes and sizes face increasing pressure to do more than the law requires of them to police intellectual property rights. DMCA-plus arrangements can be beneficial if they are truly voluntary and reflect genuine consensus among copyright owners and Internet companies about how and why to adjust the obligations that flow from default liability rules and exceptions. For large Internet companies that have the infrastructure and economic wherewithal to implement DMCA-plus measures, such measures may be a reasonable way to simultaneously avoid new governmental regulation and secure new business opportunities. New entrants and smaller players may be disadvantaged, however, to the extent that DMCA-plus measures adopted by major intermediaries like Google, Comcast, and PayPal up the ante for everyone.

DMCA-plus enforcement also raises a range of normative concerns for Internet users and merchants: "Best practices" agreements are negotiated privately, without input from the public or public interest groups. In this respect, they lack the deliberative transparency associated

---

of the copyright.") (internal citation and quotation marks omitted); Viacom Int'l Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 523 (S.D.N.Y. 2010) ("[I]mpos[ing] responsibility on service providers to discover which of their users' postings infringe a copyright would contravene the structure and operation of the DMCA."), *aff'd in part, vacated in part, remanded*, 676 F.3d 19 (2d Cir. 2012).

[176] Courts in cases involving contributory trademark infringement claims against online intermediaries have also rejected the argument that intermediaries, as putative "cheaper cost avoiders," should bear the primary burden of policing trademarks online. *See* Tiffany (NJ) Inc. v. eBay, Inc., 576 F. Supp. 2d 463, 518 (S.D.N.Y. 2008) ("[E]ven if it were true that eBay is best situated to staunch the tide of trademark infringement to which Tiffany and countless other rights owners are subjected, that is not the law."), *aff'd in part, rev'd in part*, 600 F.3d 93 (2d Cir. 2010).

with public law-making. The protocols they prescribe often presume liability for the accused and entail rushed or summary adjudications by inexpert authorities. Such protocols may thus be procedurally inadequate to prevent the removal of non-infringing content or the punishment of innocent actors. For the Internet as a whole to benefit from DMCA-plus enforcement, "best practices" must incorporate adequate protections for Internet users and online merchants, whose interests are at risk of being marginalized when copyright owners and online intermediaries hammer out new bargains under IPEC's watchful eye.

APPENDIX B: Summary of Over-Removal Studies
Copyright Office Section 512 Study Comments
Annemarie Bridy and Daphne Keller

EMPIRICAL EVIDENCE OF "OVER-REMOVAL" BY INTERNET COMPANIES UNDER INTERMEDIARY LIABILITY LAWS

Adapted from Daphne Keller, *Empirical Evidence of "Over-Removal" by Internet Companies Under Intermediary Liability Laws* (2015), http://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws

The "Over-Removal" Issue

Most intermediaries offer legal "Notice and Takedown" systems – tools for people to alert the company if user-generated content violates the law, and for the company to remove that content if necessary. Twitter does this for tweets, Facebook for posts, YouTube for videos, Google for search results, local news sites for user comments, etc. National law varies in terms of what content must be removed, but some version of Notice and Takedown exists in every major market. Companies receive a remarkable mix of requests – from those identifying serious and urgent problems, to those attempting to game the Notice and Takedown system as a means to silence speech they disagree with, to those stating wildly imaginative claims under nonexistent laws.

What do companies do with these removal requests? Many of the larger companies make a real effort to identify bad faith or erroneous requests, in order to avoid removing legal user content. (I worked on removals issues for Google for years, and can attest to the level of effort there.) But mistakes are inevitable given the sheer volume of requests – and the fact that tech companies simply don't know the context and underlying facts for most real-world disputes that surface as removal requests.

And of course, the easiest, cheapest, and most risk-avoidant path for any technical intermediary is simply to process a removal request and not question its validity. A company that takes an "if in doubt, take it down" approach to requests may simply be a rational economic actor. Small companies without the budget to hire lawyers, or those operating in legal systems with unclear protections, may be particularly likely to take this route.

Much of the publically available information about over-removal by intermediaries is anecdotal. But empirical evidence of over-removal – through error or otherwise – keeps trickling in from academic studies. This data is important to help policy-makers understand what intermediary liability rules work best to protect the free expression rights of Internet users, as well of the rights of people with valid claims to removal. This post lists the studies I have seen.

These studies were mostly conducted by academics or advocates with a particular interest in protecting user free expression and ensuring that legal content remains available online. One day I hope we will see more data from the other side – advocates for rightsholders, defamation plaintiffs, or other groups harmed by online content that violates their legal rights. That could help build a more complete picture of the over-removal issue as well as any related under-removal problem – intermediaries failing to remove content when notified, even though applicable law requires removal.

The Studies

- Jennifer Urban and Laura Quilter's 2006 review of copyright-based removals from Google's services under the US Digital Millennium Copyright Act (DMCA), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2210935. Relying on information released to the Chilling Effects (now Lumen) database by the company about processed removals (i.e. the ones where the company agreed to remove, not the ones it declined), the authors found that 55% of notices involved disputes between competitors, and 31% presented significant issues regarding the validity of the copyright infringement claim. (Daniel Seng's more recent work with a similar but much larger data set has great detailed statistics on DMCA removal trends, but his published conclusions do not include analysis of the validity of the claims processed. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2563202)

- The 2004 Brennan Center study on removals and free expression, http://www.fepproject.org/policyreports/WillFairUseSurvive.pdf: Reviewing a data set of 320 copyright and trademark-based removal requests, the authors concluded that 47% stated weak claims or involved speech with important fair use or free expression legal defenses.

- Rishabh Dara's detailed experiment and study of over-removals by Indian intermediaries, http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf: Dara submitted increasingly unreasonable removal requests to various intermediaries, and carefully documented the responses. His results show considerable over-removal, including removal based on clearly invalid legal claims and removal of content not targeted by the requests.

- The 2004 Bits of Freedom study of Dutch ISPs, http://www.theregister.co.uk/2004/10/14/isp_takedown_study/: The group created accounts with ten Dutch ISPs and used them to post copies of a famous, public domain, 19th century political essay. It then used different contact information to send copyright "infringement notices" to the ISPs, under Dutch law implementing the eCommerce Directive. Of the ten ISPs, seven removed the content despite its age and public domain status.

- Oxford Program in Comparative Media Law and Policy's smaller experiment with UK and US ISPs, http://pcmlp.socleg.ox.ac.uk/wp-

content/uploads/2014/12/liberty.pdf: Researchers posted John Stuart Mill's 1859 discussion of media freedom from "On Liberty" – which is in the public domain. They then used different accounts to request its removal via UK and US ISPs. The UK ISP removed the essay without question, while the US ISP responded by requiring the requester to comply with the more formal requirements of the US DMCA, including "good faith belief" and "penalty of perjury" attestations.

- Company transparency reports: Transparency reports from Twitter, Google, Yahoo, Facebook, Microsoft and others offer some data about removal requests. The data is valuable for other purposes, but usually not great for sussing out the validity or even volume of complaints. Most reports list only requests from government sources, which represent a small minority of legally-based content removals. Some show the overall percentage of requests accepted and rejected; or include anecdotal examples. In some cases, particularly for Google's "Right to Be Forgotten" (RTBF) removals, this data is supplemented by news reports. For example, coverage last summer suggested that most RTBF claims come from non-public figure requestors. It is also reported that relatively few requesters take their claims to Data Protection Agencies when Google rejects their removal requests; and that when they do the Agencies often agree with Google's decision.
    - Twitter: https://transparency.twitter.com/removal-requests/2014/jul-dec
    - Google: https://www.google.com/transparencyreport/
    - Yahoo: https://transparency.yahoo.com/government-removal-requests/index.htm
    - Facebook: https://govtrequests.facebook.com/
    - Microsoft: https://www.microsoft.com/about/business-corporate-responsibility/transparencyhub/crrr/

- The Lumen database and other research drawing on it: Lumen, formerly known as Chilling Effects, maintains a remarkable database containing millions of removal requests made public by companies and other contributors. https://lumendatabase.org/ Significant academic research has been carried out using the database, much of it relevant for over-removal questions. An overview of this literature as of 2010 is in Chilling Effects amicus brief from Perfect 10 v. Google. https://www.eff.org/node/58197
- Judith Townsend's research on removals by journalists and bloggers, http://policyreview.info/articles/analysis/online-chilling-effects-england-and-wales: This survey concerns removals by publishers rather than intermediaries, but contains interesting data on the frequency of requests and compliance, as well as availability of legal counsel to those receiving removal requests.

More studies and data sources surely exist, or will exist. I have heard in particular of one from Pakistan, but have not found it so far. If you know of other sources, please let me know or post them in the Comments section so this page can become a more useful resource for people seeking this information.