U.S. Copyright Office

Section 512 Study
[Docket No. 2015–7]

Comments of Annemarie Bridy and Daphne Keller

February 21, 2017

These comments are responsive to the following questions in the Request for Additional Comments issued on November 8, 2016: 1, 2, 3, 8, 9, 10, 12, and 14.

1. As noted above, there is great diversity among the categories of content creators and ISPs who comprise the Internet ecosystem. How should any improvements in the DMCA safe harbor system account for these differences? For example, should any potential new measures, such as filtering or stay-down, relate to the size of the ISP or volume of online material hosted by it? If so, how? Should efforts to improve the accuracy of notices and counter-notices take into account differences between individual senders and automated systems? If so, how?

Our response to this question will focus on the concerns of ordinary Internet users. As discussed in our response to Question 2, this broad class includes both individual content creators and consumers—and people who are both at once. For this class, the takedown/staydown proposals create many potential harms that arise even if filtering requirements apply only to large OSPs. They include:

- **Removal of lawful speech and harm to the global Internet ecosystem**

Filters embedded in the infrastructure of the Internet are tools begging for misuse, including by human rights-abusing governments. Compelling Internet companies to build such tools for limited purposes (such as countering piracy) effectively makes the same tools available to suppress legitimate access to information.

Powerful Internet control technologies consistently pose the same question for civil liberties advocates: do the benefits of a new tool (fighting piracy, phishing, or other harms) outweigh its costs (enabling future censorship, surveillance, or other rights violations)? The trade-offs were starkly illustrated recently, when Apple removed the *New York Times* app from

its Chinese app store, and both Google and Apple removed the LinkedIn app from their Russian stores.[1] The companies' centralized control of the app stores has real value, letting them protect users' security and fight online harms including copyright infringement. But that same control, as Farhad Manjoo noted in the *Times*, permits "a more effective form of censorship."[2]

Adoption of filtering tools raises the same issues. OSPs already face pressure to use content filters for ever-expanding purposes. Publicly disclosed examples include efforts by European plaintiffs to force Google to filter content that violates Data Protection or "Right to Be Forgotten" laws.[3] As has been widely reported, French regulators maintain that Google must globally remove information under these laws, regardless of conflicting free expression laws in other countries.[4] With legal pressures of this sort coming even from European democracies, it would be naïve to expect any less interest in filtering tools on the part of authoritarian regimes. Any cost-benefit analysis of filtering obligations should take very serious account of this problem, and the interests of both political dissidents and ordinary Internet users around the world.

- **Removal of lawful speech through filtering errors**

Even if filters were used solely to fight piracy, harms to free expression and lawful use of content would persist. There is no algorithm that can do the kind of contextual and legal analysis required to identify fair use. Even full copies of works can be legal in some contexts—as with

[1] Farhad Manjoo, *Clearing Out the App Stores: Government Censorship Made Easier*, NEW YORK TIMES, Jan. 18, 2017, https://www.nytimes.com/2017/01/18/technology/clearing-out-the-app-stores-government-censorship-made-easier.html.

[2] *Id.* Third party app stores exist, but have far fewer users. *See* Steve Ranger, *iOS Versus Android. Apple App Store Versus Google Play: Here Comes the Next Battle in the App Wars*, ZDNET, Jan. 16, 2015, http://www.zdnet.com/article/ios-versus-android-apple-app-store-versus-google-play-here-comes-the-next-battle-in-the-app-wars/.

[3] *See, e.g.*, Mosley v. Google, [2015] EWHC 59 (QB); Daniel Hegglin v. Google Inc ([2014] EWHC 2808 (QB)); Ashley Hurst, *Data Privacy and Intermediary Liability: Striking a Balance between Privacy, Reputation, Innovation and Freedom of Expression*, INTERNAT'L FORUM FOR RESPONSIBLE MEDIA BLOG, May 14, 2015, https://inforrm.wordpress.com/2015/05/14/data-privacy-and-intermediary-liability-striking-a-balance-between-privacy-reputation-innovation-and-freedom-of-expression-part-1-ashley-hurst/, (discussing "right to be forgotten" claims as a potential basis to compel proactive content removal by OSPs).

[4] Alex Hern, *Google Takes Right to Be Forgotten Battle to France's Highest Court*, THE GUARDIAN, May 19, 2016, https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court.

the time-shifting of entire programs in *Sony* or the publication of entire emails in *Diebold*.[5] Over-removal is an issue even for state-of-the-art systems like Content ID. Filters developed by companies with less money and engineering talent than YouTube would presumably generate still higher error rates. As discussed in our response to Question 3, it does not appear that counter-notice is an effective mechanism to correct such errors.

- **Economic harm to victims of wrongful removal**

Ordinary businesses, including content creators, have a lot to lose if their material is unfairly removed from popular platforms—consider the illustrator who sells her work on Etsy; the musician finding fans through Facebook; or the animator operating her own website using a host like Amazon Web Services. Studies tell us that groundless removal demands often come from one small business competitor targeting another.[6] Being removed from important platforms can seriously harm these businesses, and a climate of unpredictable removals hurts the economy for online businesses generally. Requiring filters for only larger platforms would not solve these problems, since the larger platforms are often the most commercially relevant for small businesses.

- **Competitive and consumer harms**

YouTube's ContentID cost a reported $60 million and years of engineering investment. No small potential competitor can afford an effort of this sort. Engineering costs aside, companies seeking to develop their own filters would have an enormous task just negotiating licenses from rightsholders for use of reference files. Mandating technology that only incumbents can afford would effectively deter investment in competing and innovative platforms, to the detriment of consumers.[7] From this perspective, differential treatment of smaller competitors might be appealing. It is hard to imagine implementing such a rule without

[5] *See, e.g.,* Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984); OPG v. Diebold, 337 F. Supp. 2d 1195 (N.D. Cal. 2004). This context-specific legality makes copyright filtering fundamentally different from existing filtering systems for child pornography, because the latter is illegal regardless of context.

[6] Jennifer Urban and Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMPUTER & HIGH TECH. L. J. 621 (2006).

[7] *See also* Martin Husovec, *Accountable, Not Liable: Injunctions against Intermediaries* (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2773768 (offering a law and economics analysis of cost allocation in blocking orders).

legal uncertainty and market distortion, however, including gamesmanship on the part of OSPs as they approach whatever size threshold the law set.

- **Other concerns**

The idea of different copyright law requirements for large and small actors raises other concerns as well. As participants in the 2016 California roundtable pointed out, important Internet actors can be very difficult to classify for this purpose. For example, classifying platforms by user volume would likely make Wikipedia a "major platform," but filtering of this sort would be both economically unfeasible for them and technically incompatible with their crowdsourced model. It is unclear how a law varying copyright obligations based on a platform's size would work in practice—or even which mid-sized platforms such a law would apply to, given that the biggest platforms already employ filtering technologies voluntarily.

2. Several commenters noted the importance of taking into account the perspectives and interests of individual Internet users when considering any changes to the operation of the DMCA safe harbors. Are there specific issues for which it is particularly important to consult with or take into account the perspective of individual users and the general public? What are their interests, and how should these interests be factored into the operation of section 512?

The interests of Internet users should be central to this inquiry. Their relevance compares to that of patients in debates over health policy, or of rural telephone users in telecommunications policy. We need a clear understanding of their concerns—as creators, distributors, and receivers of online information, and often as all of these things at once.

Interests of this commercially and politically marginalized group do not necessarily align with those of large companies on any side of the current debate. A young filmmaker, for example, might care deeply about fighting piracy, but at the same time support new distribution models outside the control of traditional industry titans. Or she may fear that filters like ContentID will remove her documentary movie trailer because of its fair use excerpts from other works. A tech startup founder, similarly, may depend on safe harbors in developing her business, but fear that large platforms' voluntary adoption of filtering measures sets a precedent for changes in the law that will make her own business impossible.

Internet users have significant interests in the operation of the DMCA safe harbors. The safe harbors directly affect their ability to engage in legal speech, share legal information, and find legal information. By shaping the incentives for technical entrepreneurs and cultural creators, the DMCA also indirectly—but strongly—shapes the online tools and content available to ordinary Internet users.[8] Our current online environment of open platforms and democratic public participation is directly attributable to intermediary immunities—as courts around the world have recognized.[9]

Any DMCA change or interpretation should be vetted against *all* of these rights—not just the interests of major players. As a conspicuous example, the "takedown/staydown" model discussed in Question 1 requires close consideration of impact on the speech rights of Internet users.

3. Participants expressed widely divergent views on the overall effectiveness of the DMCA safe harbor system. How should the divergence in views be considered by policy makers? Is there a neutral way to measure how effective the DMCA safe harbor regime has been in achieving Congress' twin goals of supporting the growth of the Internet while addressing the problem of online piracy?

The DMCA debate has become highly contentious and polarized—to the detriment of the "content" and "tech" industry participants in the debate and the many people affected by copyright law whose interests do not align with either side. As the question notes, there are

[8] A recent report on intermediary liability and human rights by a group of European academics listed "the right to freedom of expression, the right to access information, the right to privacy, data protection rights, the right to a fair trial, the right to an effective legal remedy, the freedom to conduct a business and the freedom to provide services." Christina Angelopoulos, et al., *Study of Fundamental Rights Limitations for Online Enforcement through Self-Regulation* (2016), http://www.ivir.nl/publicaties/download/1796#page=57.

[9] *See* MTE v. Hungary (2016) ECtHR 22947/13 (Para. 82) (courts could not require OSP to monitor for defamatory speech in news forum comments, because of threat to users' speech and information rights); Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10, ECR 2011:771 (Para. 52) (courts could not require OSP to monitor for copyright infringement, in part because of threat to users' rights); SABAM v. Netlog, Case C-360/10, ECLI:EU:C:2012:85 (Para. 48) (same); Shreya Singhal v. Union of India, No. 167/2012 (S. Ct. of India, Crim. 2015) (construing notice and takedown statute to mandate removal only based on court or other government order, because of threat to users' speech and information rights); Belén Rodríguez c/Google y Otro s/ daños y perjuicios, R.522.XLIX (Corte Suprema [S. Ct.] of Argentina, Civ. 2014) (courts may not require OSPs to monitor user content, because of threat to users' speech and information rights); *but see* Delfi AS v. Estonia (2015) ECtHR 64659/09 (courts could require OSPs to monitor for unprotected hate speech in news forum comments).

highly divergent views about correct policy outcomes, and often divergent views on the underlying facts and their proper interpretation.

For the most part, though, we believe reasonable parties on all sides should be able to agree on common baseline beliefs about fact-based methodologies for empirical inquiry. Facts are real, and social science includes standard tools and methodologies for finding them. One key reference point may be the recent "Open Letter on Ethical Norms in Intellectual Property Scholarship," published in the *Harvard Journal of Law and Technology* and signed by a diverse group of some fifty scholars.[10] Their recommendations include, among others, (1) disclosure of direct and indirect funding sources for both individual researchers and institutions; (2) a prohibition on quid pro quo or prior approval rights for funders; and (3) when possible, given constraints such as confidentiality, disclosure of data sufficient to allow other researchers to replicate or dispute research conclusions. We believe the stakeholders in the DMCA discussion can agree on principles along these lines, and can identify a shared body of facts about current DMCA practice, even as we differ in policy preferences and analysis of research results. We should not abandon this effort or accept any "view" as equally valid in the absence of empirical data.

While input from interested parties at Copyright Office roundtables can be helpful in understanding the range of experiences various stakeholders are having with the current DMCA safe harbor framework, it is important to recognize the limited value of personal anecdotes in understanding the behavior of complex systems and weighing their costs and benefits. Roundtable participants with resources and inclination to attend bi-coastal meetings on the copyright system are a self-selected group drawn from a fairly narrow cross-section of the people and businesses that are affected daily by the operation of the DMCA safe harbors. Their views matter to be sure, but they cannot substitute for independent, statistically validated, evidence-based research. Accordingly, the Office should refrain from forming significant policy recommendations that rely too heavily on personal or purely qualitative accounts documented in roundtable transcripts.

[10] Feldman, Robin, et al., *Open Letter on Ethical Norms in Intellectual Property Scholarship* (2016), Stanford Pub. L. Working Paper No. 2714416; Duke I & E Research Paper No. 16-7; Duke Law School Pub. L. & Legal Theory Series No. 2016-9, https://ssrn.com/abstract=2714416 or http://dx.doi.org/10.2139/ssrn.2714416.

The Berkeley/Columbia Report

The 2016 *Notice and Takedown in Everyday Practice* report by researchers at UC Berkeley and Columbia ("the Berkeley/Columbia Report") offers uniquely comprehensive and robust data regarding DMCA practice.[11] A qualitative section draws on unprecedented access to internal stakeholder processes, among both rightsholders and OSPs. A quantitative section analyzes publicly available data from the Lumen database. The Berkeley/Columbia Report is scrupulous in spelling out methodology and acknowledging limitations of the data set. Inevitably, given the highly politicized debate around the DMCA, the report has attracted criticism.[12] Because we believe the Berkeley/Columbia Report is a critical source of empirical information for policymaking and illuminates a landscape far more complex than many reports would suggest, we address some of those concerns here.

The report does not exhaust the research possibilities in the field and is not perfect. Some of the key data can never be released because researchers obtained it under strict confidentiality agreements. And, as many critics pointed out, significant funding for the report came from Google.[13] Funding from a diverse array of stakeholders would be preferable for research in this or any contested area. None of this takes away, however, from the report's very real accomplishments in documenting, in an unprecedented level of detail, everyday notice and takedown practice across a range of actors.

One critique we have seen is that the Berkeley/Columbia research should have addressed different topics or drawn on different data. For instance, Kevin Madigan & Devlin Hartline faulted it for not investigating the effectiveness of the DMCA in deterring online piracy overall.

---

[11] Jennifer Urban et al., *Notice and Takedown in Everyday Practice*, UC Berkeley Pub. L. Research Paper No. 2755628 (2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2755628.

[12] *See, e.g.*, Stephen Carlisle, *Google Funded Study Concludes Google Needs More Legal Protection From Small Copyright Owners!* (April 14, 2016), http://copyright.nova.edu/google-funded-takedown-study/; Kevin Madigan & Devlin Hartline, *Separating Fact from Fiction in the Notice and Takedown Debate* (April 25, 2016), http://cpip.gmu.edu/2016/04/25/separating-fact-from-fiction-in-the-notice-and-takedown-debate/; David Newhoff, *Reports of DMCA Abuse Likely Exaggerated* (April 18, 2017), http://illusionofmore.com/reports-dmca-abuse-exaggerated/.

[13] The Stanford Center for Internet and Society also receives funding from Google, and one author of this submission previously worked for the company. Both CIS and the Berkeley/Columbia Report prominently disclose this funding relationship, and prohibit any donor control over academic work. *See* About Us, STANFORD CIS, http://cyberlaw.stanford.edu/about-us ("All donors to the Center agree to give their funds as unrestricted gifts, for which there is no contractual agreement and no promised products, results, or deliverables"); Urban, et al., *supra* note 11, at iv, 27 (Neither of its two funders "directed our approach in any way, and neither funder reviewed any methods, data, results, or reporting before public release.").

While certainly a valid subject for research, this is an entirely different topic and one that would require a vast additional data set, drawing on the entire Internet. A thorough review of the topic would also likely depend on sensitive or confidential information from rightsholders. Madigan and Hartline also suggested that data from Google Web Search removals was not representative because web search is different from hosting services—a distinction the report itself discusses at length.[14] They propose that researchers should instead look to data from Facebook or YouTube. Unfortunately, those data sets are not available: neither Facebook nor YouTube sends takedown information to Lumen. If they did, it would be much harder to assess DMCA complaints' validity, because unlike with web search links, researchers would have no way to view content that was removed. The upshot is that this research may be the best we can hope for in terms of publicly available empirical data sources, barring major changes in company transparency practices. The Berkeley/Columbia authors call attention to the lack of transparency by both OSPs and rightsholders, identifying it as "[t]he primary obstacle to more systematic accounts of the notice and takedown process."[15]

Some other key issues raised by critics boil down to questions of policy or philosophy. For example, several commenters suggested that DMCA notices that fail to comply with DMCA statutory requirements should not be counted as flawed.[16] Some even suggested that notices targeting the wrong work (i.e., a work not belonging to the notifier) should be considered valid, because the erroneously listed URLs presumptively also contain infringement.[17] There is room for philosophical difference about what formalities or process should be required by law before an OSP deletes or de-indexes Internet users' online speech. Rightsholders may understandably feel that formalities should be reduced in light of the volume of online infringement. Civil liberties advocates may counter that more stringent formalities are needed as a proxy for the due process that alleged infringers would receive in court. But Congress has answered this question, spelling out what elements must be included to make a DMCA notice valid.[18] Notices that lack

[14] *Id.* at 67-73. This includes a section titled "The Disproportionate Role of Google Web Search."

[15] *Id.* at 9.

[16] The report adopted a very conservative metric for identifying non-compliant notices. For example, adult industry notices that listed the work at issue merely as "video and image series by [principal name]" were deemed compliant. *Id*. at 94-95.

[17] Newhoff, *supra* note 12.

[18] 17 U.S.C. § 512(c)(3)(A)(iii).

these elements are unquestionably flawed under the law and were rightly counted as such in the study.

Similarly, the study identified 7.3% of targeted webpages as having "characteristics that weigh favorably toward fair use," and included "mashups, remixes, or covers" in this count.[19] One critic noted that this group might in theory "not provide so much as a single fair use defense that would hold up in court."[20] But the study did not claim to have adjudicated fair use status—appropriately, given the uncertainty of fair use outcomes. The data it does provide, about *potential* fair uses targeted by DMCA requests, is directly relevant to the questions raised in this Request for Additional Comments. For example, when assessing the role of automated processes in DMCA notice generation, it's important to know how often human judgment may be required, particularly in light of the holding in *Lenz v. Universal Music Group*[21] that the DMCA requires copyright holders to consider fair use before sending a takedown notification.[22]

Finally, several of the critiques identified highly relevant data that is not in the report and that is possible (though potentially difficult) to obtain.[23] The report itself lists some of the same topics in a section titled "Future Avenues for Research and Fact-Finding."[24] There, the authors list seven areas for which additional research is urged. To avoid redundancy we will not list them here, but we particularly agree with the need for research on the following topics identified in the report: (1) the experience of small rightsholders, (2) the experience of Internet users whose content is removed, (3) the experience of a broader swath of DMCA agents, and (4) counter-notice practice.

On the subject of counter-notice, the report states,

> by all accounts, the actual use of counter notices is extremely infrequent. Only one respondent among both service providers and rightsholders reported receiving

[19] Urban et al., *supra* note 11, at 95.

[20] Newhoff, *supra* note 12; *see also* Madigan and Hartline *supra* note 12.

[21] 815 F. 3d 1145 (9th Cir. 2015).

[22] *Id.* at 1148.

[23] *See, e.g.*, Carlisle, *supra* note 12 (Researchers "[f]ailed to interview any small business or individual copyright holders who sent takedown [or] a single person who had either been the "target" of a notice or filed a counter-notice.").

[24] Urban et al., *supra* note 11, at 140-142.

more than a handful per year. Many—including some large services handling thousands of notices per year—reported receiving none.[25]

This conclusion is reinforced by the data about counter-notice included in our own 2016 submission. In transparency reports we reviewed, the rates of counter-notice ranged from 0.08% to 0.6%.[26] This supports concerns raised in many of the 2016 submissions about the inadequacy of counter-notice as a mechanism to correct over-removal. We agree with the report's authors that additional research is needed to better understand whether and to what extent counter-notice practices are acting as an effective check on mistaken or excessive removals.

Underresearched Aspects of DMCA Practice

In addition to the areas of inquiry identified above, the following topics are highly relevant to the Office's questions:

- How effective are different methods for identifying erroneous DMCA removals? In particular, can we quantify the number of erroneous removals that have been identified—and hopefully also corrected—as a result of (1) standard notice to the alleged infringer under section 512(g)(2)(A); (2) removal notices shown to third party end users by OSPs (such as the video removal notices on YouTube); and (3) disclosure of specific DMCA removal requests through the Lumen database or similar public repositories?

- How many OSPs send users notice when their content is removed under section 512(c)? As discussed in our 2016 submission, hosts may not always have incentive or organizational capacity to provide notice to alleged infringers.[27]

- How many users actually *receive* notice when their content is removed under section 512(c)? This is a separate question because, as discussed in our 2016 submission, notices of content removal may be ineffective if delivered to outdated or unmonitored accounts.[28]

---

[25] *Id.* at 44.

[26] *See* Annemarie Bridy & Daphne Keller, Comments Submitted in Response to U.S. Copyright Office's Dec. 31, 2015 Notice of Inquiry, at 28.

[27] *Id.* at 29.

[28] *Id.*

Many of these questions concern individual Internet users. As a result, hard data may be difficult to come by—as is often the case for questions about diffuse public interest, or about people underrepresented in policy disputes. But such data is clearly relevant to the subjects of this Request for Additional Comments.

Broader Economic Research

Below are some possibilities for broader economic research regarding intermediary liability regimes. We base these on our own legal research and conversations with economics researchers. We are not economists or statisticians ourselves and will therefore not suggest any detailed methodologies.

- **Internet sector country comparisons**

The United States' strong safe harbors from intermediary liability are widely credited as one cause of the exceptional innovation and economic growth in our technology sector. In his article *How Law Made Silicon Valley*, UC Davis Professor Anupam Chander, for example, writes that "legal innovations in the 1990s that reduced liability concerns for Internet intermediaries, coupled with low privacy protections, created a legal ecosystem that proved fertile for the new enterprises of what came to be known as Web 2.0."[29] This claim could be tested, with respect to the DMCA, by country-to-country comparisons, assessing both national laws and economic or other indicators relating to intermediary businesses. Relevant data could include investment rates, revenue, number of companies launched and failed, and number of platform users.

- **Copyright and infringement country comparisons**

Researchers could compare costs and benefits to rightsholders, intermediaries, and Internet users under different legal notice and takedown regimes. Comparatively straightforward data sets are likely to be available on topics such as revenues, piracy rates, and Internet usage rates. Researchers can also attempt to quantify less tangible benefits in cultural production,

[29] Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L. J. 639, 642 (2013).

access, and innovation. Professor Mike Smith at Carnegie Mellon has worked and published extensively in this area, and his writings may suggest additional avenues for exploration.[30]

- **Before and after comparisons in countries with changed laws**

Within individual countries, researchers could compare infringement rates and content and tech sector economic indicators before and after a meaningful change in intermediary liability law. For example, a study might consider Chile before and after its 2010 copyright law[31] or Argentina before and after the landmark *Belén Rodríguez* Supreme Court ruling.[32] Professor Josh Lerner of Harvard Business School has published work that might present models for methodology and statistical analysis of these transitions.[33]

- **Costs and consequences of mandating filters**

Even if one were to put aside the many harmful effects of filters discussed in our response to Question 1 above, their likely real world costs and benefits are poorly understood. These costs matter, in part as a way to quantify the chilling effect of filtering requirements on new investment and innovation. Relevant considerations for informed assessment of takedown/staydown proposals would include:

- error rates of existing filtering technologies and the ability of researchers to track and understand error rates;
- expert opinion from computer scientists on potential future technologies;
- development costs of existing proprietary filters such as Facebook's or YouTube's;

---

[30] *See* Mike Smith, *Research List*, http://mds.heinz.cmu.edu/research/ (last accessed Feb. 12, 2017). One source of "noise" in data about other countries may be the prominent role of US OSPs, applying US law, including the DMCA, to services used in those countries.

[31] Law No. 20.435, May 04, 2010, Art. 85, http://bcn.cl/nol (last accessed Feb. 12, 2017).

[32] *See Belén Rodríguez*, *supra* note 9. India's Supreme Court reached a comparable outcome. *See Shreya Singhal*, *supra* note 9.

[33] *See, e.g.*, Josh Lerner, *The Empirical Impact of Intellectual Property Rights on Innovation: Puzzles and Clues*, AMERICAN ECON. REV.: PAPERS & PROCEEDINGS 99, No. 2, at 343–348 (2009); Josh Lerner and Greg Rafert, *Lost in the Clouds: The Impact of Changing Property Rights on Investment in Cloud Computing Ventures* (2014), Harvard Business School Working Paper, No. 15-082 (2015), http://www.hbs.edu/faculty/Publication Files/15-082_ce76cd68-19d3-4328-9df0-fb74913cd5db.pdf (providing analysis of changes in VC investment in the wake of the Second Circuit's *Cartoon Network* ruling).

- real cost, including implementation and engineering costs, of licensed filtering technologies such as Audible Magic;
- the competitive landscape for licensed filtering technologies, including (1) viable alternatives to Audible Magic and (2) the role of reference file licensors (i.e., rightsholders) as potential gatekeepers to new filter developers.

8. For ISPS acting as conduits under section 512(a), what notice or finding should be necessary to trigger a repeat infringer policy? Are there policy or other reasons for adopting different requirements for repeat infringer policies when an ISP is acting as a conduit, rather than engaging in caching, hosting, or indexing functions?

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.[34] The statute also does not define what it means for a policy to be "reasonably implemented." As one court has observed, "the language of the statute and the legislative history of this section are less than models of clarity."[35] But the statute is non-specific by design, as the court in *Corbis Corp. v. Amazon.com, Inc.*[36] pointed out:

> 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.[37]

Although there are no one-size-fits-all definitions of some key terms in section 512(i), the case law has developed over almost two decades to set reasonably clear parameters for OSPs of all types to follow as they exercise the discretion Congress purposely gave them to define and implement repeat infringer policies tailored for and appropriate to their systems and services.

---

[34] *See generally* Andres Sawicki, *Repeat Infringement in the Digital Millennium Copyright Act*, 73 U. CHI. L. REV. 1455 (2006).

[35] Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1176 (C.D. Cal. 2002).

[36] 351 F. Supp. 2d 1090 (W.D. Wash. 2004).

[37] *Id.* at 1101.

The Request for Additional Comments correctly suggests that section 512(a) Internet access providers are differently situated from types of providers that give users access to a much narrower and more limited set of online services—e.g., social media platforms, cloud storage lockers, or online search. Unlike other safe-harbor-eligible providers, section 512(a) providers are the public's gateway to the whole Internet and its vast offering of applications, products, services, and information. A broadband subscriber whose account is terminated loses access not only to a single service he or she may have used to share copyrighted material without authorization, but to an entire universe of other services unrelated to entertainment: online banking, shopping, education, public libraries, telemedicine, employment-related information and job application portals, videoconferencing, government programs, state and federal tax preparation and filing services, and an unending list of others. Moreover, some of these services have migrated completely online over the years or were born digital, precluding use by anyone without Internet access. The Internet can no longer be considered a "place" of diversion that exists apart from people's lives in the "real" world; it is now fully and inextricably embedded in the institutions and practices of everyday life—so much so that the United Nations Human Rights Council has condemned as a human rights violation official actions that terminate or deny citizens Internet access, including for violations of intellectual property rights.[38]

With all of that said, we do not believe that any changes to section 512(i) are necessary at this time to recognize or reflect the unique position of section 512(a) Internet access providers as gatekeepers to the whole Internet. Section 512(i) as it is currently drafted—with flexible standards instead of detailed, provider-specific rules—gives providers of all types, including section 512(a) access providers, the latitude they need (and that courts have, in practice, given them) to adopt and implement repeat infringer policies tailored to the specific nature of their services. "Appropriate circumstances" for account termination vary from one type of service and provider to the next. It stands to reason that "appropriate circumstances" for termination of a life-critical service like broadband Internet access are relatively rare. In keeping with the principle that one size does not fit all, section 512(i) in its current form accommodates service-specific

[38] *See* Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, A/HRC/17/27, United Nations Human Rights Council, May 16, 2011, para. 78 ("The Special Rapporteur considers cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights.").

approaches to compliance. There is currently no problem in need of a solution with the repeat infringer component of section 512(i).

9. Many participants supported increasing education about copyright law generally, and/or the DMCA safe harbor system specifically, as a non-legislative way to improve the functioning of section 512. What types of educational resources would improve the functioning of section 512? What steps should the U.S. Copyright Office take in this area? Is there any role for legislation?

We do not see any need for legislation here, but we do see a role for the Copyright Office. Under section 701 of the Copyright Act, the Office and its staff have authority to "[c]onduct…programs regarding copyright."[39] The Copyright Act specifically authorizes the Office to conduct educational programs for foreign and international audiences, but it also gives the Office broader leave to undertake programs that are "appropriate in furtherance of the functions and duties specifically set forth in [the Copyright Act]."[40] Providing balanced and accessible educational materials on copyright to the American public falls logically within this grant of authority.

Evidence in the DMCA literature of flawed and erroneous notices[41] strongly suggests that members of the public who send such notices often do not understand what types of material are protected by copyright, what types of unlicensed borrowing are protected by fair use, when it is appropriate to send a DMCA takedown notice to an online provider, and what a takedown notice must contain in order to be compliant with section 512(c)(3)(A). Lack of knowledge of both the basic principles of copyright law and the mechanics of the DMCA can lead to frustration and wasted effort for both notice senders and notice recipients. Misunderstanding the rules of the game can lead notice senders to believe that notice recipients are acting in bad faith when they reject or challenge non-compliant notices, and can exacerbate an existing climate of distrust around the DMCA process for both creators and providers.

Educational materials for service providers, who are not uniformly sophisticated about the DMCA process, would also be useful. For example, the Office could provide information

[39] 17 U.S.C. § 701(b)(4).

[40] *Id.*

[41] *See* Urban, et al., *supra* note 11, at 87-96.

about the importance of registering a DMCA agent and instructions for registration. It could also provide, in addition to information about notice formalities, model web forms for notices and counter-notices that providers could make available on their websites.

Many industry trade associations and public interest groups already provide copyright educational materials free of charge to the public. Some are better than others in terms of their balance, accuracy, and completeness. Those that focus narrowly on enforcement and piracy-deterrence tend to be the least helpful when it comes to informing the public in a nuanced and holistic way about copyright law and its animating policies. Attention to fair use and other exceptions and limitations is important but often goes unpaid in anti-piracy materials in the interest of "keeping it simple." But it is possible to produce sophisticated educational materials about copyright that convey complex rules in a way that is readily understandable. Professor Bridy was involved over the last two years in the production and review of responsible, nuanced digital copyright curricula for middle- and high-school educators by the iKeepSafe Coalition, sponsored by the Center for Copyright Information.[42]

When it comes to digital copyrights and the DMCA, there is a deficit in public understanding that the Office's expert staff is uniquely situated to fill with sophisticated, balanced, and accessible educational resources. Educating copyright holders, service providers, and users about the law can correct misconceptions and minimize mistakes in the DMCA system, leading to a better online experience for everyone. The Copyright Office can and should produce materials of its own to help the public understand the reach (and limits) of copyright and the reach (and limits) of the DMCA.

10. How can the adoption of additional voluntary measures be encouraged or incentivized? What role, if any, should government play in the development and implementation of future voluntary measures?

Rightsholders and online service providers, including—among others—payment processors and online advertising networks, have already undertaken a range of privately ordered "DMCA-plus" enforcement initiatives in response to active encouragement from members of

[42] *See* Copyright and Creativity for Ethical Digital Citizens, IKEEPSAFE.ORG, http://archive.ikeepsafe.org/copyright/ (last accessed Jan. 27, 2017).

Congress and Executive Branch officials.[43] Implementation of these voluntary measures has followed a familiar and problematic pattern: their design is negotiated behind closed doors with no public input, and they strongly prioritize convenience and efficiency for participating rightsholders and service providers over fair process for accused infringers.[44] The government and the Copyright Office should not support or encourage any additional voluntary measures that follow this troubling pattern. To better serve the public's interest in the expanding area of private, DMCA-plus copyright enforcement, the government should promote the creation and adoption of policies and procedures that are transparent and fair to accused infringers, in addition to being efficient for rightsholders and service providers.[45]

The recently abandoned Copyright Alert System is a good place to start when thinking about better design for voluntary notice-and-action programs.[46] The governing legal document for the CAS was made available to the public through the Center for Copyright Information, albeit only after the document had been executed. Through that detailed document, the public

---

[43] *See* Annemarie Bridy, *Copyright's Digital Deputies: DMCA-Plus Enforcement by Internet Intermediaries*, *in* RESEARCH HANDBOOK ON ELECTRONIC COMMERCE LAW (John Rothchild ed., 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2628827 (describing various voluntary agreements and their notice-and-action protocols); NATASHA TUSIKOV, CHOKEPOINTS: GLOBAL PRIVATE REGULATION ON THE INTERNET (2016).

[44] The most recent example is the "trusted notifier" program adopted by the MPAA and Donuts, a registry operator for hundreds of new gTLDs in the Domain Name System. *See* Annemarie Bridy, *Remember That Time We Saved the Internet?*, STANFORD CIS BLOG, Jan. 18, 2017, https://cyberlaw.stanford.edu/blog/2017/01/remember-time-we-saved-internet.

[45] Outside the U.S., some intermediary liability experts argue that governments have affirmative duties to promote more fair and transparent notice and takedown procedures, in order to protect Internet users' rights to free expression and due process. *See, e.g.*, Council of Europe, *Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content: Comparative Considerations* (2016), at 786-87, http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet (summarizing arguments for liability of private OSPs for voluntary removals, or liability of governments for encouraging or permitting such removals); Christina Angelopoulos et al, *Study of Fundamental Rights Limitations for Online Enforcement Through Self-Regulation* (2016), http://www.ivir.nl/publicaties/download/1796 (identifying arguments based on human rights law). US law may put different parameters on government actors when they encourage private intermediaries to remove more content than the law requires. In some cases, such actions can violate the First Amendment. *See, e.g.*, Backpage.com LLC v. Dart, 807 F.3d 229 (7th Cir. 2015) (sheriff violated First Amendment by urging credit card companies to suspend payment to lawfully operating website); *see also* Derek Bambauer, *Against Jawboning*, 100 MINN. L. REV. 51 (2015).

[46] The system operated between 2013 and 2017. *See* Ted Johnson, *Internet Service Providers, Studios and Record Labels Call It Quits on Copyright Alert System*, VARIETY, Jan. 27, 2017, https://variety.com/2017/digital/news/copyright-alerts-piracy-mpaa-comcast-att-1201971756/ (reporting on the discontinuation of the program). For detailed discussions and critique of the design of CAS, see Mary LaFrance, *Graduated Response by Industry Compact: Piercing the Black Box*, 30 CARDOZO ARTS & ENT. L.J. 165 (2012); Annemarie Bridy, *Graduated Response American Style: "Six Strikes" Measured Against Five Norms*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1 (2012).

and interested academic researchers were able to understand and qualitatively evaluate the program, to which millions of broadband subscribers were subject. The CAS program incorporated procedural protections for broadband subscribers who believed they had been wrongly identified as repeat infringers by an automated (and audited) content-fingerprinting system. Before any sanction was imposed, accused infringers under the CAS were guaranteed access to an inexpensive, non-judicial dispute resolution process with a neutral, trained adjudicator who applied a clear set of substantive rules (albeit unpublished ones). A serious flaw in the CAS, however, was its lack of public reporting and transparency concerning outcomes.[47]

Post-CAS voluntary initiatives, including those adopted by online advertising networks, payment processors, and new gTLD registry operators, do not compare favorably to the CAS when it comes to programmatic design that supports expert, consistent, and fair treatment for accused infringers.[48] If the Copyright Office and other government actors in the copyright policy arena (e.g., IPEC, USPTO) intend to encourage the continued existence and expansion of private, DMCA-plus enforcement measures, they should do so only on the condition that such programs promote transparency and incorporate adequate protections for accused infringers, which no existing program does.

12. Several study participants have proposed some version of a notice-and-staydown system. Is such a system advisable? Please describe in specific detail how such a system should operate, and include potential legislative language, if appropriate. If it is not advisable, what particular problems would such a system impose? Are there ways to mitigate or avoid those problems? What implications, if any, would such as system have for future online innovation and content creation?

We believe the costs of a notice-and-staydown requirement for innovators, users, and the Internet ecosystem as a whole would outweigh the potential benefits of such a requirement for rightsholders. We therefore do not advise converting the DMCA's existing notice-and-takedown

[47] In the four years that CAS operated, the Center for Copyright Information issued only a single report to the public. *See* Center for Copyright Information, *The Copyright Alert System: Phase One and Beyond* (2014), www.copyrightinformation.org/wp-content/uploads/.../Phase-One-And_Beyond.pdf. No raw data from the program was ever made available to independent researchers.

[48] *See* Bridy, *Copyright's Digital Deputies*, *supra* note 43 (comparing procedures under various DMCA-plus voluntary agreements); Annemarie Bridy, *Internet Payment Blockades*, 67 FLA. L. REV. 1524 (2015) (discussing the regulatory status of voluntary agreements in general and providing a detailed description and analysis of the payment processor voluntary agreement).

framework into a notice-and-staydown framework. We explained in detail in our response to Question 1 some of the specific, systemic harms that we believe would inevitably flow from imposing filtering obligations on OSPs. The initial and ongoing costs of filtering systems to OSPs can be extremely steep. Costs to users and content creators for mistaken removals can also be high, as we explained above. And neither of those assessments takes into account the harder-to-quantify costs to democratic values associated with the wide deployment of filtering technologies throughout the Internet's infrastructure.

It is important to recognize that the introduction of a notice-and-staydown requirement for OSPs would represent a radical restructuring—and not just a slight recalibration—of the balance of enforcement burdens embodied in the DMCA's existing policy architecture. We are aware of no way to implement "notice and staydown" that would not require repealing the no-duty-to-monitor rule in section 512(m) of the DMCA. For almost two decades, that rule has given innovators runway to develop and grow new content-sharing and distribution systems without having to bear the significant costs associated with proactive and constant copyright enforcement. As we mentioned above, many of the large online platforms have already voluntarily adopted filtering systems, because they have both resources and business incentives to do so.

Given the many costs and drawbacks associated with filtering, we believe it is wise to leave the safe harbors as they are, unless there are objective reasons to believe that today's and tomorrow's innovators no longer need the legal protections from liability that were so critical to the success of yesterday's.

14. Several study participants mentioned concerns regarding certain case law interpretations of the existing provisions of section 512. Additionally, two new judicial decisions have come out since the first round of public comments was submitted in April 2016. What is the impact, if any, of these decisions on the effectiveness of section 512? If you believe it would be appropriate to address or clarify existing provisions of section 512, what would be the best ways to address such provisions (i.e., through the courts, Congress, the Copyright Office, and/or voluntary measures)? Please provide specific recommendations, such as legislative language, if appropriate.

We assume the new cases referenced in this question are *BMG Rights Management (US) v. Cox Communications, Inc.*[49] and *Capitol Records, LLC v. Vimeo LLC*.[50] We believe that *BMG*, which implicates section 512(i), was correctly decided given the court's factual finding that Cox blatantly failed to implement the repeat infringer policy it belatedly adopted. We believe that *Capitol Records*, which implicates the red flag knowledge standard in section 512(c)(1)(A), was a well-reasoned application of the Second Circuit's prior decision in *Viacom International, Inc. v. YouTube, Inc.*[51] We discuss each case briefly below to explain our conclusion that no changes to section 512 are warranted based on either case. With respect to earlier-decided cases implicating provisions of section 512—in particular the red flag knowledge provision—we incorporate by reference our comments filed last year in response to the initial Request for Comments in this proceeding.[52]

BMG Rights Management (US) v. Cox Communications, Inc.

BMG sued Cox for contributory and vicarious infringement based on Cox users' peer-to-peer file sharing activity. Cox asserted the DMCA safe harbors in its defense, and BMG argued that Cox should be ineligible for safe harbor for failing to comply with section 512(i) of the DMCA, which requires providers to adopt and reasonably implement a policy for terminating the accounts of repeat infringers in appropriate circumstances.[53]

As discussed above in response to Question 8, the DMCA doesn't define "repeat infringer" or "appropriate circumstances," leading courts to conclude that Congress intended for providers to have broad discretion over the substance and implementation of their section 512(i) policies. The case law has never been clear on whether a provider may legitimately take the position, adopted by Cox, that the only customers who should be treated as repeat infringers under the DMCA are those who have been repeatedly adjudicated and repeatedly found liable for infringement. In this case, Cox failed to persuade the court that it should be required to terminate user accounts only in cases involving adjudicated infringers.[54]

---

[49] 149 F. Supp. 3d 634 (E.D. Va. 2015).

[50] 826 F.3d 78 (2d Cir. 2016).

[51] 676 F.3d 19 (2d Cir. 2012).

[52] *See* Bridy & Keller, *supra* note 26.

[53] *See* 17 U.S.C. § 512(i).

[54] *See BMG Rights Management*, 149 F. Supp. 3d at 654, 661.

Cox also failed to persuade the court that notices of infringement from copyright holders are insufficient as a matter of law to confer actual knowledge of a user's infringement on a provider.[55] The court acknowledged conflicting decisions on the point but quoted the Ninth Circuit's decision in *UMG Recordings v. Shelter Capital Partners* for the proposition that notices can be "powerful evidence of a service provider's knowledge," even if they are not sufficient on their own to establish that knowledge.[56] The evidence of knowledge in Cox's case was particularly strong, the court said, because Cox received not one or two but at least fourteen notices of infringement for multiple individual users over a six-month period.[57] In addition, emails from customers who were the subjects of repeat notices and whose accounts were eligible for termination under Cox's published policy contained admissions from the customers themselves that they had been sharing copyrighted files.[58] On the facts, this was not a good case for Cox; the record quite clearly showed that Cox was calculatedly lax in its enforcement of its repeat infringer policy, hanging on to well-documented violators for the stated purpose of preserving revenue.[59]

We have some concern that the trial court's decision in this case failed to acknowledge the unique position of section 512(a) providers as the public's gatekeepers to the whole Internet.[60] At the end of the day, however, the judgment can be read as resting on the fact-specific determination that Cox simply (and badly) failed to reasonably implement its own "graduated response" policy.[61] To use the court's words, "Cox's implementation rendered the

---

[55] *Id.* at 662–663.

[56] *Id.* at 662.

[57] *Id.*

[58] *Id.*

[59] *Id.* at 657.

[60] See our response to Question 8 *supra*. Given the state of the market for fixed broadband services, many households in the United States do not have more than a single broadband provider that serves them. *See* Jon Brodkin, *US Broadband: Still No ISP Choice for Many, Especially at Higher Speeds*, ARS TECHNICA, Aug. 10, 2016, https://arstechnica.com/information-technology/2016/08/us-broadband-still-no-isp-choice-for-many-especially-at-higher-speeds/. The stakes of a copyright-related account termination are significantly higher for subscribers in these underserved markets than they are for subscribers in markets with two or more providers.

[61] *See BMG Rights Management*, 149 F. Supp. 3d at 662 ("Moreover, the account holders referenced in the emails above had already been through Cox's entire graduated response procedure. That means Cox had received, not one or two, but at least *fourteen* infringement notices tied to their accounts in a six-month period…. By the time an account holder reaches the end of Cox's graduated response procedure, the chance that the account holder is not a willful infringer has substantially lessened.").

policy an 'absolute mirage.'"[62] Notably, the court did not find any fault with the liberality of Cox's policy, which allowed for over a dozen notices over a six-month period before termination. Had it done so, we would be more troubled about the potential implications of this case.

We are hopeful that the Fourth Circuit, which is now considering Cox's appeal, will expressly acknowledge in its decision that the unique position of section 512(a) providers justifies their adoption of repeat infringer policies that reflect the increasingly indispensable, utility-like nature of the service they provide. If the appellate court fails to make that point, then an amendment to section 512(i) that does make it may be advisable. Any such amendment at this time, however, would be premature.

Capitol Records, LLC v. Vimeo, LLC

Capitol Records' lawsuit against Vimeo, running in federal court since 2009, raised important and unsettled questions concerning the scope of safe harbors—questions remaining in the wake of the Second Circuit's landmark decision in *Viacom.*[63] Three issues were in play in the case: (1) whether the safe harbors—which are a creature of federal copyright law—may be raised as a defense to allegations of infringement involving pre-1972 sound recordings, which are not within the scope of federal copyright law; (2) whether a service provider can be charged with "red flag" knowledge of infringement if its employee views a video containing all or almost all of a popular sound recording; and (3) whether Vimeo showed "willful blindness" to its users' infringements and was thereby disqualified from the safe harbors. We believe the court decided all three these issues correctly; however, in the interest of brevity we address only the second of these issues in our response to this question.

As a condition for eligibility, the safe harbors require service providers to remove material that they either actually know or should know from surrounding facts or circumstances (i.e., "red flags") to be infringing. In *Viacom*, the Second Circuit interpreted red flag knowledge under the DMCA to mean a provider's subjective awareness of facts or circumstances from

[62] *Id.* at 658.

[63] 676 F.3d 19 (2d Cir. 2012).

which specific instances of infringement would be objectively obvious to a reasonable person.[64] The standard is a mixed subjective/objective one that requires courts to wade into the swampy terrain of what a hypothetical reasonable person should be able discern in light of the facts in front of her.

District courts deciding safe harbor disputes have often declined to grant summary judgment on the issue of red flag knowledge.[65] This is true in part because "reasonableness" in any area of the law is an elusive concept and in part because there has been no authoritative definition in the context of the DMCA of what a hypothetical "reasonable tech company employee" should be expected to know concerning potential instances of infringement that she might run across at work. This case helps to fill that vacuum, sensibly establishing that a reasonable person for DMCA purposes is none other than copyright law's "ordinary person"—more specifically, one who is "not endowed with specialized knowledge or expertise concerning music or the laws of copyright."[66]

Considered from the perspective of an ordinary employee of a tech company, the court held, the act of viewing some part of a user-uploaded video that contains all or virtually all of a "recognizable" song does not necessarily give rise to red flag knowledge (i.e., does not make infringement objectively obvious).[67] The court offered several reasons why this is true: (1) the employee might not have viewed the whole video (and therefore might not have known that it contained all or virtually all of a song); (2) the employee's reason for viewing the video might have been wholly unrelated to copyright; (3) the employee might not actually have recognized the "recognizable" song in question for a variety of reasons, including the employee's age and

---

[64] *Id.* at 31.

[65] *See, e.g.*, Disney Enters., 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."); Capitol Records, LLC 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."); 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.").

[66] *Capitol Records*, 826 F.3d at 93-94.

[67] *Id.* at 94.

taste in music; and (4) the employee might have had no expertise in copyright and could therefore not have distinguished between infringing and non-infringing content.[68] In light of these factors, the court said, a plaintiff must do more to prove a defendant's red flag knowledge than simply offer proof that an employee to some extent viewed a video that contained all or most of a popular copyrighted song.[69]

Capitol Records argued that requiring plaintiffs to show more to establish the objective obviousness of an infringement would collapse red flag knowledge into actual knowledge, effectively reading red flag knowledge out of the statute as a separate basis for disqualification from safe harbor.[70] The court disagreed, writing that "[i]f the facts actually known by an employee of the service provider make infringement obvious, the service provider cannot escape liability…on the ground that the person with knowledge of those facts never thought of the obvious significance of what she knew in relation to infringement."[71] To put it another way, awareness of facts that would make an infringement obvious to a reasonable person can disqualify a provider without any proof that the particular employee in question put two and two together to reach a subjective conclusion that material was infringing. As long as a reasonable person would have done the math, the plaintiff's burden is met regardless of what the provider's employee actually believed. By contrast, for a provider to be disqualified based on an employee's actual knowledge, the employee must be shown to have reached a subjective conclusion that the material was infringing. Actual knowledge and red flag knowledge are thus distinct and distinguishable, with a lower burden of proof for the latter. The red flag math in this case was just not as easy as the plaintiffs made it out to be, for the reasons the court cited.

Even as the court rejected the plaintiffs' argument that a holding for Vimeo would gut red flag knowledge, it acknowledged that the scope of red flag knowledge under its application of the statute is narrow.[72] Such knowledge, it recognized, is likely to be provable in only a small number of cases. "Assuming this is so," the court wrote, "it is of no significance."[73] A narrow

[68] *Id.* at 96-97.
[69] *Id.* at 97.
[70] *Id.*
[71] *Id.*
[72] *Id.*
[73] *Id.*

scope for red flag knowledge, the court explained, is consistent with Congress' primary goals for the safe harbors, which were to be accomplished mainly through the operation of the notice-and-takedown framework.[74] That framework, after all, requires no inferences or guessing and is the true engine of the DMCA when it comes to content removal.

Contrary to alarms that the court's decision in this case gutted red flag knowledge, the standard is actually alive and well. It's just not trivially easy to prove, and that's as it should be given both the goals of the statute and the severe consequences (i.e., potentially bankrupting statutory damages) for providers that don't qualify for safe harbor. The Second Circuit appreciated in this case that a broad and uncertain scope for red flag knowledge would make asserting the safe harbors little more than a game of chance, which is definitely not what Congress intended.

The Role of Flexible Standards in Sections 512(c) and 512(i)

As with any piece of legislation that incorporates flexible standards in addition to more rigidly prescribed rules, the DMCA has required judicial interpretation to give meaning to its more hermeneutically open provisions. As a result of this iterative, case-driven process, the DMCA's standards have become more rule-like and more predictable over time, bringing a needed level of legal certainty for all affected businesses.[75] Two standards-based provisions that have spawned a significant amount of litigation are the red flag knowledge provision in section 512(c) and the repeat infringer provision in section 512(i).

In our prior comments in this proceeding, we acknowledged how challenging it has been for commercial actors to comprehend and for courts to apply the red flag knowledge standard.[76] Asked how section 512 might be legislatively improved, we argued in those comments that altogether eliminating red flag knowledge as an alternative form of scienter to the more predictable standard of actual knowledge would be a bold and highly effective solution to the indeterminacy surrounding the concept of red flags and their implications for section 512(m).[77]

---

[74] *Capitol Records*, 826 F.3d at 97.

[75] *See generally* 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).

[76] Bridy & Keller, *supra* note 26, at 32.

[77] *Id.* at 37.

As we pointed out in those comments, the road to stable meaning and predictable application of the red flag standard has been long and expensive for litigants on both sides of DMCA cases.[78] On the whole, however, we think the courts in the major cases to confront the issue—including *Viacom International, Inc. v. YouTube, Inc.*, *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, and now *Capitol Records v. Vimeo*—have interpreted the standard with the restraint necessary to reconcile it with the policy objectives underlying the safe harbors and, in particular, with the express no-duty-to-monitor rule in section 512(m).[79] Section 512(m), by legislative design, requires a narrow scope for red flag knowledge and is a critical element of the balance of burdens in the safe harbors.

In general, the case law with respect to both section 512(c) and section 512(i) has developed reasonably and in keeping with the goals Congress intended for the DMCA when the statute was enacted. In our view, no legislative intervention is required at this time to correct any outcomes from the two cases discussed above.

Respectfully submitted,[*]

Annemarie Bridy

Professor
College of Law
University of Idaho

Affiliate Scholar
Center for Internet and Society
Stanford Law School

Affiliated Fellow
Information Society Project
Yale Law School

Daphne Keller

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

Dated: February 21, 2017

[78] *Id.* at 36.

[79] *Id.*

[*] Institutional affiliations are for purposes of identification only. The views expressed herein are solely the views of the authors.