Before the

U.S. COPYRIGHT OFFICE, LIBRARY OF CONGRESS

In the Matter of

Section 512 Study

Docket No. 2015-7

Additional Comments of Electronic Frontier Foundation

February 21, 2017

Submitted by:

Corynne McSherry
Mitch Stoltz
Kerry Maeve Sheehan[1]
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
corynne@eff.org

The Electronic Frontier Foundation (EFF) appreciates the Copyright Office's efforts to consider the impact of section 512 of the Digital Millennium Copyright Act. EFF is a member-supported, nonprofit, public interest organization dedicated to ensuring that copyright law advances the progress of science and the arts and enhances freedom of expression. Founded in 1990, EFF represents tens of thousands of dues-paying members, including consumers, hobbyists, computer programmers, entrepreneurs, students, teachers, and researchers, who are united in their desire for a balanced copyright system that provides adequate incentives for creators, facilitates innovation, and ensures broad access to information in the digital age.

EFF has been involved, as amicus or party counsel, in numerous court cases interpreting section 512, including *Lenz v Universal, Lessig v. Liberation Music, MoveOn v. Viacom, Tuteur v. Wesley Corcoran, Sapient v. Geller, SHARK v. PRCA*, *Viacom v. YouTube*, *UMG Recordings v. Veoh*, and *Columbia Pictures v. Fung*. We regularly counsel

[1] Kerry Maeve Sheehan is not admitted to practice law.

individuals who have been targeted by takedown notices pursuant to the DMCA regarding their rights and options. We have also represented the interests of users and innovators on multiple formal and informal public processes assessing the notice and takedown system, in the United States and abroad. In particular, we have worked to highlight the impact of section 512 on online expression and innovation, and to ensure that section 512 is properly understood by courts, policymakers and the public.

Question 1: [T]here is great diversity among 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?

Diversity within the Internet ecosystem is precisely what the DMCA was intended to engender. Congress created broad categories of service providers that were flexible and clear enough to accommodate subsequent innovation. Attempting to construct a new set of subcategories will undermine that clarity, to the detriment of everyone involved. Moreover, such an attempt won't solve the important problems. For example, everyone who sends a takedown notice or counternotice, whether or not they use automated systems, must consider whether their allegation is being made in good faith.[2] Modifying that requirement is unlikely to improve accuracy in the system. Finally, it is difficult to imagine a sustainable set of subcategories, given shifting business models and technical developments.

Question 2: 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 public has several overlapping interests in the operation of the section 512 safe harbors, because those safe harbors helped launch the Internet as an open environment for free expression, access to information, and cultural and technological innovation.

As we explained in our initial comments, by 1997 the Supreme Court had already "recognized that the Internet . . . was assuming a central role in disseminating speech protected by the First Amendment."[3] Today, it provides the means through which billions of people communicate, access information and ideas, form communities, and engage

---

[2] 17 U.S.C. § 512(c)(3)(A)(v).

[3] Initial Comments of the Electronic Frontier Foundation ("EFF Comments") at 17 (citing *Reno v. American Civil Liberties Union*, 521 U.S. 844, 870 (1997)).

with creative works.[4] The Internet today plays a critically important role in facilitating freedom of expression by providing a platform for users to exercise their free speech rights, including their rights to "receive information and ideas."[5] Internet intermediaries provide the backbone for Internet users' expression and are key to the public's ability to exercise these rights.[6]

Accordingly, the public has a strong interest in ensuring that the Internet remains a viable and accessible platform for free expression and innovation, and in ensuring that online platforms don't unduly remove, filter, or block speech from the Internet.

These interests are reflected in the structure of section 512, and were a key consideration of the statute's drafters.[7] First, the statute's legislative history reflects Congress's understanding that the public has an interest in the growth and development of Internet services, stating that section 512 "ensures that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will expand."[8] The public has strong interest in ensuring that copyright liability neither stifles these services, nor makes it impossible for innovators to develop and market new ones.

---

[4] ITU, *ITU Releases 2015 ICT Figures, Statistics Confirm ICT Revolution of the Past 15 Years* (May 26, 2015), https://www.itu.int/net/pressoffice/press_releases/2015/17.aspx (all URLs last visited Feb. 19, 2017) ("Globally, 3.2 billion people are using the Internet, of which two billion live in developing countries.").

[5] *See* EFF Comments at 17 (citing *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas."); *Board of Education v. Pico*, 457 U.S. 853, 867 (1982) (stating the right to receive information "is a necessary predicate to the recipient's meaningful exercise of his own rights of speech, press, and political freedom.")).

[6] *See* David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression to the Human Rights Council*, ¶ 2, U.N. Doc. A/HRC/32/38 (May 11, 2016) (stating "[t]he contemporary exercise of freedom of opinion and expression owes much of its strength to private industry, which wields enormous power over digital space, acting as a gateway for information and an intermediary for expression.").

[7] *See* Initial Comments of Annemarie Bridy and Daphne Keller ("Bridy & Keller Comments") at 11 (stating "user interests are a vital part of the balancing the safe harbors were intended to accomplish"); *see also* Initial Comments of the Library Copyright Alliance at 2 ("This framework would balance the interests of rights holders, service providers and users to promote the development of a robust Internet and the creation of works of authorship."); Initial Comments of the Organization for Transformative Works at 10 ("Shielding intermediaries was not something Congress did for simply for the sake of shielding them. Congress sought to make OSPs a useful path by which speakers could reach audiences.").

[8] S. Rep. 105-190, at 8 (1998).

Second, the public has a strong interest in ensuring that speech is not unnecessarily or improperly removed or blocked from the Internet. Section 512's legislative history explains that "[t]he provisions in the bill balance the need for rapid response to potential infringement with the end-users legitimate interests in not having material removed without recourse."[9] These same interests are reflected in 512(f)'s remedies against inaccurate and abusive takedown notices,[10] and in 512(g)'s put-back provisions.[11] As explained in the legislative history, 512(g)'s "put back procedures were added . . . 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."[12] When content is removed without proper justification, it doesn't just hurt the targeted user, it harms the larger public as well.[13]

Congress also recognized that the public has a strong interest in ensuring that that individual speakers aren't denied access to the Internet without adequate justification. The legislative history thus explains that the statute "contains . . . important procedural protections for individual Internet users to ensure that they will not be mistakenly denied access to the World Wide Web."[14]

Third, the public has a strong interest in privacy, which Congress addressed through section 512(m). Privacy is often a precondition for engaging in speech-based activities, as those whose communications and actions are subject to constant monitoring and potential exposure may fear to seek necessary, but controversial information, voice unpopular or minority opinions, or associate with others.[15] Many Internet users are already wary of the

---

[9] *Id*. at 21.
[10] *Id.* at 49-50 (addressing then-subsection 512(e)'s "misrepresentations," which is identical to 512(f), and stating "[t]his subsection is intended to deter knowingly false allegations to service providers in recognition that such misrepresentations are detrimental to rights holders, service providers, and Internet users").
[11] *Id.* at 21 (referring to the replacement provisions in then-subsection 512(f)). According to Professors Bridy and Keller, these provisions "indicate a deep Congressional concern with the implications of the notice-and-takedown systems 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." Bridy & Keller Comments at 12-13.
[12] S. Rep. 105-190, at 50.
[13] For example, when content removals target political ads during a campaign season, the public is deprived of information relevant to their political choices. *See* Elliot Harmon, *Once Again, DMCA Abused to Target Political Ads*, Deeplinks (Nov. 17, 2015), https://www.eff.org/deeplinks/2015/11/once-again-dmca-abused-target-political-ads;
[14] S. Rep. 105-190, at 9.
[15] Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, ¶ 79, U.N. Doc. A/HRC/23/40 (Apr. 17, 2013) ("Privacy and freedom of expression are interlinked and mutually dependent;

extent to which their activities are subject to monitoring by their ISP, advertisers, and government agencies.[16] By including 512(m), which the legislative history explains "is designed to protect the privacy of Internet users,"[17] Congress recognized that monitoring users' Internet activities would actively harm the public's interests both in the privacy of their personal information and in free expression.

Question 4: What are the most significant practical barriers to use of the notice-and-takedown and counter-notice processes, and how can those barriers best be addressed (e.g. incentives for ISPs to use a standardized notice/counter-notice form, etc.)?

Please see our response to Question 6, below.

Question 5: Are changes to the section 512 timeline needed? If so, what timeframes for each stage of the process would best facilitate the dual goals of encouraging online speech while protecting copyright holders from online piracy?

No. Focusing in particular on the counter-notice process, lengthening the timeline would worsen the detrimental effect on speech when, as is common, the DMCA process is abused to take down lawful speech, particularly speech of a time-sensitive nature. Shortening the timeline, however, might make it difficult for senders to draft papers that can withstand legal scrutiny. The best way to protect online speech is to ensure that the cause of action created by section 512(f) for false takedowns is meaningful, making counter-notices less necessary in the first place.

---

an infringement upon one can be both the cause and consequence of an infringement upon the other. Without adequate legislation and legal standards to ensure the privacy, security and anonymity of communications, journalists, human rights defenders and whistleblowers, for example, cannot be assured that their communications will not be subject to States' scrutiny."); *see also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 499 n. 104 (2006) ("Monitoring, if prevalent, certainly kills free discourse and spontaneous utterances.") (quoting *United States v. White*, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting); Electronic Frontier Foundation, https://www.eff.org/issues/anonymity.

[16] Analysis by the National Telecommunications and Information Administration of survey data from the U.S. Census revealed that privacy concerns, including concerns related to "data collection or tracking by online services, loss of control over personal data, [and] data collection or tracking by government," may be "prompting some Americans to limit their online activity." Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities* (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities; *see also* Karen Gullo, *Surveillance Chills Free Speech–As New Studies Show–And Free Association Suffers*, Deeplinks (May 19, 2016), https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association.

[17] S. Rep. 105-190, at 55.

Question 6: Participants also noted disincentives to filing both notices and counter-notices, such as safety and privacy concerns, intimidating language, or potential legal costs. How do these concerns affect use of the notice-and-takedown and counter-notice processes, and how can these disincentives best be addressed?

The counter-notice procedure was designed to serve as a safeguard for users whose content is targeted for removal.[18] In practice, however, it has proved largely ineffective at countering false, abusive, or erroneous takedown notices. Recent empirical research suggests that counter-notices are rarely used.[19] According to that study,

> "[B]y all accounts, the actual use of counter notices is extremely infrequent. Only one respondent among both service providers and rights holders reported receiving more than a handful per year. Many–including some large services handling thousands of notices per year–reported receiving none."[20]

The study's conclusions are backed up by data from some service providers' transparency reports.[21] In our earlier comments, EFF described some of the reasons why the counter-notice procedure has proven ineffective.[22]

Allowing users to send counter-notices anonymously, by designating a proxy or agent to accept service of legal process on their behalf, could ameliorate a major obstacle preventing effective use of the counter-notice system. Under the current system, many users may feel intimidated or fear harassment or reprisal if they reveal their personal information to the sender of the takedown notice, particularly where the users' content is critical, a parody, or addresses controversial subject matter. It appears that counter-notice senders' fears are not unfounded. One OSP surveyed in the study by U.C. Berkeley School of Law researchers described "cases where allegedly abusive ex-husbands have filed DMCA complaints against images their ex-wife had posted as a means of attempting to get her current address."[23] According to an amicus brief filed on her behalf in *Lenz v. Universal Music*, when YouTube creator Rebecca Prince considered filing a counter-notice in response to an abusive notice, she "feared that gaining her sensitive information was in fact what this person wanted so he or she could use it to 'dox' her – that is, to release her identifying information online to further harass and intimidate her –

---

[18] *Id.* at 50.
[19] *See* Jennifer M. Urban, Joe Karaganis, & Brianna Schofield, *Notice and Takedown in Everyday Practice* ("Urban Study") 44 (UC Berkeley Public Law Research Paper No. 2755628, Mar. 29, 2016), *available at* https://ssrn.com/abstract=2755628.
[20] *Id.*
[21] *See* Bridy & Keller Comments at 28 (providing data on numbers of counter-notices received or processed from four companies' transparency reports, including Twitter, Tumblr, Github, and Automattic).
[22] EFF Comments at 16-17.
[23] Urban Study at 45 n. 131.

which in fact happened."[24] In their Initial Comments in this study, the Organization for Transformative Works noted "we have found that individuals (particularly young women) are generally intimidated by the prospect of counter-notifying even when they believe, correctly, that their use is fair."[25]

We recognize that notice senders are also required to disclose identifying information and may have the same concerns. However, we do not see how the remedial measures designed to address takedown abuse can be effective without revealing the source of the takedown notice and so that information, at least, must be disclosed.

Question 7: How could [the penalties under section 512 for filing false or abusive notices or counter-notices] be strengthened? Would the benefits of such a change outweigh the risk if dissuading notices or counter-notices that might be socially beneficial?

The problem of false and abusive takedown notices is common and well documented. Our previous comments provide numerous examples of such abuses.[26] And, as we highlighted in those comments, the recent study by U.C. Berkeley School of Law researchers revealed a staggering amount of inaccurate takedowns targeting legitimate content.[27] Perhaps most damning, the study revealed that, in a sample of automated takedown notices, 4.2%, that is, nearly 4.5 million takedown requests, "targeted content that clearly did not match the identified infringed work" and 7.3% (clearly more than 4.5 million) involved potential fair uses.[28] Prior studies, comments, testimony and reports from Internet companies support these findings.[29] The harms can get worse where

---

[24] Brief of Amici Curiae Yes Men, Rebecca Prince, and May First in Support of Petitioners, at 18, *Lenz v. Universal Music Corp.*, U.S. Supreme Court No. 16-217 ("Yes Men Brief"), *available at* http://www.scotusblog.com/wp-content/uploads/2016/09/16-217-amicus-cert-yes-men-et-al.pdf.

[25] *See* Comments of the Organization for Transformative Works at 18; *see also* Yes Men Brief at 19.

[26] *See* EFF Comments at 9-13 and accompanying footnotes.

[27] Urban Study at 88.

[28] *Id.*

[29] *See, e.g.*, Daphne Keller, *Empirical Evidence of "Over-Removal By Internet Companies Under Intermediary Liability Laws"*, Stanford Center for Internet and Society Blog (Oct. 12, 2015), https://cyberlaw.stanford.edu/blog/2015/10/empirical-evidence-over-removal-internet-companies-under-intermediary-liability-laws; Comments of Engine, GitHub, Kickstarter, Medium, and Redbubble at 9-10; Comments of Automattic at 3; Google, *How Google Fights Piracy* 34, 45-46, https://drive.google.com/file/d/0BwxyRPFduTN2TmpGajJ6TnRLaDA/view (listing examples of abusive notices sent to YouTube and Google Web Search, and stating "Google refused to remove or reinstated more than 11 million webpages from our search results"); *Section 512 of Title 17: Hearing Before the H. Subcomm. on Courts, Intellectual Property and the Internet of the H. Comm. On the Judiciary,* 113th Cong. 59

takedown notices target upstream network providers. For example, a takedown notice aimed at silencing a parody website run by the culture-jamming activists the Yes Men and sent to the site's upstream network provider, resulted in the removal of 38,000 websites.[30]

Further, without an effective remedy against improper takedowns, the notice and takedown system becomes an easy vehicle for censorship of unpopular or critical speech by both government and private entities.

In our initial comments, we mentioned the government of Ecuador's campaign to silence critics of Ecuadorean President Rafael Correa. Since at least 2010,[31] the Spanish law firm Ares Rights has been issuing DMCA takedown notices under instructions from various agencies of the Ecuadorian government, for alleged infringements that are trivial or *de minimis* at best—for example, the use of a government logo or a photograph of the President in an unfavorable blog post or tweet. This campaign of DMCA abuse first came to light in 2013,[32] and in September 2014, both Facebook and YouTube removed a

---

(2014) (testimony of Paul Sieminski, General Counsel, Automattic Inc.), https://judiciary.house.gov/wp-content/uploads/2016/02/113-86-87151.pdf ("[W]e have recently seen a troubling rise in the misuse of the DMCA takedown process. The most egregious cases we have seen are notices from those who fraudulently misrepresent that they own a copyright at all in order to strike content from the Internet that they simply don't agree with. Other examples include DMCA notices sent by companies to remove articles that are critical of their products or copyright holders who send overly broad blanket DMCA notices to take down content even though it is being legally and fairly used."); Reddit, Inc., *Transparency Report 2015* ("In 2015, we received a large number of requests for removal of content under the DMCA, which either did not comply with the requirements of a takedown notice under the DMCA, were requests for removal under our content policy or requests for removal of content that we did not host on our servers".), https://www.reddit.com/wiki/transparency/2015; Parker Higgins, *New Company Transparency Reports Help Quantify DMCA Abuse*, Deeplinks (Sep. 17, 2014), https://www.eff.org/deeplinks/2014/09/new-company-transparencyreports-help-quantify-dmca-abuse.

[30] Yes Men Brief at 16-17 (citing Mike Masnick, *NRA Trademark Complaint Over Yes Men Parody Takes Down 38,000 Websites*, Techdirt (June 30, 2016), https://www.techdirt.com/articles/20160629/23462634866/nra-trademark-complaint-over-yes-men-parody-takes-down-38000-websites.shtml; Sarah Jeong, *NRA Complaint Takes Down 38,000 Websites,* Motherboard (June 29, 2016), http://motherboard.vice.com/read/nra-complaint-takes- down-38000-websites).

[31] Maira Sutton, *State Censorship by Copyright? Spanish Firm Abuses DMCA to Silence Critics of Ecuador's Government*, Deeplinks (May 15, 2014) https://www.eff.org/deeplinks/2014/05/state-censorship-copyright-spanish-firm-abuses-DMCA.

[32] *See* Rosie Gray, *Under Pressure, Scribd Yanks Ecuadorian Spy Documents,* BuzzFeed News (Jun. 28, 2013, 11:36 AM), https://www.buzzfeed.com/rosiegray/under-pressure-

video called “Lo que Correa no quieres que veas” (“What Correa doesn’t want you to see”), which included images of police repression during student protests that month interposed with statements by President Correa praising the police.[33] More recently, the Ecuadorian government has also started to issue some of its own removal requests directly.[34] In 2016, an app called Mashi Machine was released which enabled users to produce parody videos of President Correa for upload to social media sites. The Mashi Machine app and its creators received a DMCA takedown notice for the alleged use of copyrighted images of the President, and 25 Twitter accounts were downgraded for DMCA complaints for the use of the app.[35] DMCA complaints have also been levied against bloggers, digital magazines such as FOCUS Ecuador[36] and PlanV,[37] and NGOs such as Fundamedios.[38] Similar allegations of DMCA abuse have also emerged from Mexico and Brazil.[39]

---

scribd-yanks-ecuadorian-spy-documents; Adam Steinbaugh, *Spanish Firm Abusing Copyright to Censor Spying Documents Has Ties to Ecuador’s Government,* (Jun. 28, 2013), http://adamsteinbaugh.com/2013/06/28/spanish-firm-abusing-copyright-to-censor-spying-documents-has-ties-to-ecuadors-government; Freedom House, *Freedom on the Net 2014, Ecuador*, https://freedomhouse.org/report/freedom-net/2014/ecuador.

[33] Freedom House, *Freedom on the Net 2016, Ecuador,* https://freedomhouse.org/report/freedom-net/2016/ecuador; José Miguel Vivanco and Eduardo Bertoni, *La censura en Ecuador llegó a Internet,* Juicio Crudo (Dec. 15, 2014), http://www.juiciocrudo.com/articulo/la-censura-en-ecuador-llego-a-internet/1373.

[34] Freedom House, *Freedom on the Net 2015, Ecuador* https://freedomhouse.org/report/freedom-net/2015/ecuador.

[35] Usuarios Digitales, *#Internet2016EC Amenazas al libre ejercicio de los derechos en Internet: Resumen 2016 (Dec. 28, 2016)*, http://www.usuariosdigitales.org/2016/12/28/amenazas-al-libre-ejercicio-los-derechos-internet-resumen-2016.

[36] Usuarios Digitales, *#AlertaDigitalEC Portal Focus sale del aire por reclamación de Secretaría de Comunicación* (Dec. 8, 2016), http://www.usuariosdigitales.org/2016/12/08/alertadigitalec-portal-focus-sale-del-aire-reclamacion-secom-derechos-autor.

[37] Usuarios Digitales, *#AlertaDigitalEC PlanV fuera del aire por petición de SECOM ante servidor Digital Ocean* (Dec. 5, 2016), http://www.usuariosdigitales.org/2016/12/05/alertadigitalec-planv-del-aire-peticion-secom-ante-servidor-digital-ocean.

[38] Alexandra Ellerbeck, *How U.S. copyright law is being used to take down Correa's critics in Ecuador,* Committee to Protect Journalists Blog (Jan. 21, 2016 3:41 PM), https://cpj.org/blog/2016/01/how-us-copyright-law-is-being-used-to-take-down-co.php

[39] Claudio Ruiz, *Copyright as a Tool to Censor Political Dissent in Latin America*, Creative Commons (Jan. 20, 2017), https://creativecommons.org/2017/01/20/copyright-tool-censor-political-dissent-latin-america; Taisa Sganzerla, *Brazilian Bloggers Claim Presidential Candidate is Censoring His Critics on YouTube,* Global Voices advox (Oct.

Interpreted correctly, section 512(f) (along with the notice requirements in section 512(c) and the counter notice provisions of section 512(g)) can provide both an effective remedy for users and a deterrent against abusive takedown notices. As the Court of Appeals for the Ninth Circuit recently confirmed in *Lenz*, section 512(f) requires notice senders to consider whether their targeted use is a lawful fair use before sending the notice.[40] That rule, however, provides little remedy if a notice sender can escape liability by asserting a subjective belief that the use was not fair, no matter how unreasonable that belief. As we explained in our prior comments, the Ninth Circuit's subjective standard is both inconsistent with the language of the act, and would render the misrepresentation claim superfluous.[41] The Supreme Court is currently deciding whether to weigh in on this question.

Question 8: For ISPs acting as conduits under 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*?*

Section 512(i)(1)(A) conditions eligibility for the safe harbors on ISPs adopting and "reasonably" implementing a policy for "termination in appropriate circumstances of subscribers and account holders . . . who are repeat infringers."[42] The language of that provision accommodates different approaches to termination for different classes of intermediaries and different types of Internet services. The "appropriate circumstances" for termination of a subscriber's Internet access by a conduit ISP are far narrower than the appropriate circumstances for terminating users' access to a caching, hosting, or indexing service. More broadly, appropriate circumstances and reasonable implementation will vary across different ISPs that perform different functions, and will change as these services and uses of the Internet evolve. The law is deliberately flexible enough to account for these differences.

Conduit ISPs serve as the bridge between their subscribers and the entire Internet. Terminating a subscriber's Internet access account imposes a far more significant penalty that merely cutting off access to a single Internet service. In today's world, terminating a subscriber's account often will mean than an entire household looses access to services necessary to find and perform their jobs,[43] to complete their homework[44] and access

---

23, 2014), https://advox.globalvoices.org/2014/10/23/brazilian-bloggers-claim-presidential-candidate-is-censoring-his-critics-on-youtube.

[40] *See Lenz v. Universal Music Corp.*, 815 F.3d 1145, 1148 (9th Cir. 2016).

[41] EFF Comments at 24-25.

[42] 17 U.S.C. §512(i)(1)(A).

[43] A recent study from the Pew Research Center highlighted the important role the Internet plays for job seekers. According to that study, "[t]he [I]nternet is an essential resource for many of today's job seekers," where "[a]mong Americans who have looked for work in the last two years, 79% utilized online resources in their most recent job search and 34% say these online resources were the *most* important tool available to

educational resources, and to access healthcare,[45] government information and services and even essential emergency information and services.[46] Indeed, as former President Obama stated, Internet access today is "not a luxury, it's a necessity."[47]

---

them." Aaron Smith, *Searching for Work in the Digital Era*, Pew. Res. Center (Nov. 19, 2015), http://www.pewinternet.org/2015/11/19/searching-for-work-in-the-digital-era. Jobseekers that lack reliable Internet access are at a severe disadvantage. *See* Cecilia Kang, *Unemployed Detroit Residents Are Trapped by a Digital Divide*, N.Y. Times, May 22, 2016, https://www.nytimes.com/2016/05/23/technology/unemployed-detroit-residents-are-trapped-by-a-digital-divide.html?_r=0.

[44] *See* Hispanic Heritage Found. et al., *Taking the Pulse of High School Student Experiences in America* 9, 11 (2015) ("Nearly all students say they are required to use the internet to complete homework assignments outside of school (96.5%)" and "42% of students have received a lower grade on an assignment because they did not have access to the [I]nternet.").

[45] A 2009 report from the Pew Research Center found that "83% of internet users, or 61% of U.S. adults, have looked online for [health] information." Susannah Fox and Sydney Jones, *The Social Life of Health Information,* Pew Internet an American Life Project 8 (June 2009), http://www.pewinternet.org/files/old-media//Files/Reports/2009/PIP_Health_2009.pdf. And health care providers themselves are increasingly offering online services to their patients. Matthew Perrone, *Online Doctor Visits Can Save Time and Money, But Mostly for Basic Health Problems*, USNews, Nov. 4, 2015, http://www.usnews.com/news/business/articles/2015/11/04/virtual-doctor-visits-offer-convenience-lower-costs. Internet access also makes it far easier for those seeking insurance coverage under the Affordable Care Act's federal health exchanges to determine eligibility for federal assistance and choose their insurance plans. *See* Jeffrey Young, *Seven Alternatives To HealthCare.gov, Obamacare's Glitchy Website*, The Huffington Post (Oct. 16, 2013), http://www.huffingtonpost.com/2013/10/16/alternatives-healthcare-gov-obamacare-website_n_4109749.html.

[46] As copper telephone lines throughout the country are replaced with fiber-optic cables, phone services are increasingly dependent on Internet connections. That means even the most fundamental emergency service—the ability to call 911—will, for many, necessitate an active Internet connection. *See* New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283, sec. 6, § 6(b), 122 Stat. 2620 (requiring Voice-over-Internet Protocol services to provide 911 service); *see also* Bob Fernandez, *Verizon's Quiet Plan to Change Copper Phone Lines to FiOS*, Phila. Inquirer, Apr. 10, 2016, http://www.philly.com/philly/business/20160410_Verizon_s_quiet_plan_to_change_copper_phone_lines_to_FIOS.html.

[47] Remarks During the ConnectHome Initiative at Durant High School in Durant, Oklahoma, Daily Comp. Pres. Doc. No. 497 (July 15, 2015) https://www.gpo.gov/fdsys/pkg/DCPD-201500497/pdf/DCPD-201500497.pdf.

Disconnection also severs subscribers from today's most powerful platform for free speech and association. As a report from the Center for Democracy and Technology acknowledged, "[i]nteractive platforms have become vital not only to democratic participation but also to the ability of users to forge communities, access information, and discuss issues of public and private concern."[48] The freedom to engage in public discourse, to speak and associate freely, and to have access to the ideas and information of others is foundational to our democratic system.[49] Those constitutional values must guide the Copyright Office's approach to section 512(i)(1)(A).

In light of the severe consequences of terminating Internet access, the Office should endorse a reading of 512(a)(1)(A) that allows ISPs to limit terminations to egregious instances of repeat infringement, without forfeiting the protection of the safe harbor. The Copyright Office's report should reflect that appropriate circumstances and reasonable implementation of this provision should be determined on a case-by-case basis, taking into account both the consequences of loss of Internet access as well as the volume and egregiousness of the alleged infringements. ISPs should have the flexibility to attempt to persuade customers to cease infringement, and to take other steps prior to termination.

The U.S. District Court for the Eastern District of Virginia's recent ruling in *BMG Rights Management v. Cox Communications*[50] adopted an inappropriately rigid construction of 512(i), disregarding critical differences between access to a single online service and access to the Internet as a whole. That court appeared to base its ruling on prior precedents that dealt solely with termination from a single Internet service or website, and did not address the "appropriate circumstances" in which a subscriber's basic Internet connection could be disconnected.[51] We believe that the decision was in error. The case is currently on appeal to the 4th Circuit.

---

[48] Center for Democracy and Technology, *Shielding the Messengers: Protecting Platforms for Expression and Innovation* (2012), https://cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf.

[49] *See New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964) (noting "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open"); *see also NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449, 460 (1958) (stating that "it is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Constitution").

[50] *BMG Rights Mgmt. (US) LLC v. Cox Communs.*, Inc., 149 F. Supp. 3d 634 (E.D. Va. 2015).

[51] *Id.* at 653-55; Brief of Public Knowledge, The Electronic Frontier Foundation, and the Center for Democracy and Technology as *Amici Curiae* in Support of Neither Party, *BMG Rights Mgmt. v. Cox Communs., Inc.*, U.S. Court of Appeals for the Fourth Circuit, No. 16-1972, https://www.eff.org/document/eff-pk-cdt-amicus-brief-bmg-v-cox.

Question 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?

While copyright enforcement agreements among private entities can sometimes be adopted more quickly than laws or regulations, they are no panacea. Such agreements are often written without sufficient input from the public whose actions will ultimately be regulated. Without transparent and accountable policy-making processes, these agreements tend to favor the interests of the parties who drafted them—typically major media and entertainment companies and specific groups of Internet intermediaries. And such agreements tend to lack procedural safeguards for average Internet users. As Professor Annemarie Bridy describes, "[t]he 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."[52]

Private copyright enforcement agreements can also be a means of avoiding government accountability for unpopular or unfair policies. For example, using the penalty of domain name suspension, which renders an entire website, or multiple websites, difficult or impossible to access, was the most unpopular part of the Stop Online Piracy Act (SOPA), a bill that was set aside following widespread protests. Yet several domain name registry operators, along with major media and entertainment companies, are now proposing to institute a similar policy through contracts of adhesion with website owners.[53] While this proposal suffers from many of the same flaws as SOPA, the ability of Internet users to influence its design and operation is less clear. This lack of accountability threatens public confidence in the integrity of the domain name system, a key component of the Internet.

No private copyright enforcement agreement can fairly be called "voluntary" if it is "incentivized" by the government. Any participation by government raises the express or implied threat of binding regulations or new laws, or the withholding of benefits, if the "voluntary" agreement does not pass muster. Therefore, if the Copyright Office and other government entities continue to encourage private enforcement agreements, they must ensure that such agreements, and the processes by which they are created, meet the same procedural and substantive standards as laws or regulations. Specifically, they must be developed in a transparent process that gathers and integrates the input of all affected stakeholders. And, the resulting enforcement mechanisms must protect freedom of speech and provide due process for those accused of infringement.

---

[52] *See* Bridy & Keller Comments at 27.

[53] Press Release, Domain Name Association, *The Domain Name Association Launches Healthy Domains Initiative as Industry-Led Effort to Evolve Internet Naming Ecosystem* (Feb. 16, 2016), http://www.thedna.org/the-dna-launches-hdi-press-release-2-16-2016.

Question 11: Should industry-wide or sub-industry-specific standard technical measures be adopted? If so, is there a role for government to help encourage the adoption of standard technical measures? Is legislative or other change required?

We are aware of no current or proposed measure that could meet the statutory definition of a "standard technical measure" laid out in section 512(i)(2). As defined in that section, a "standard technical measure" must:

> "(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process; (B) be available to any person on reasonable and nondiscriminatory terms; and (C) do not impose substantial costs on service providers or substantial burdens on their systems or networks."[54]

While *some* service providers and content owners have proposed and/or implemented *some* technical measures, none of those measures comes close to meeting the requirements of section 512(i).

That fact is not particularly surprising, nor is it a problem. The statute's drafters purposefully declined to establish a government-ordered technological mandate for service providers, and ensured that any standards that might be adopted would be confined to those resulting from "open, fair, [and] voluntary" processes.[55] That choice helped guard against locking in technological standards that could impede valuable innovations, and prevented a powerful few players from effectively creating requirements that would affect the health of the Internet as a whole. The result is that service providers have the flexibility to experiment with solutions that make sense for their resources, their relationship to their users, and the services they provide.

Moreover, the diversity of Internet services today makes adoption of an industry-wide or even sub-industry-wide technical measure difficult to imagine. The measures that work for OSPs would not likely work for conduit ISPs, and those that worked for larger, well-resourced providers would likely not work for smaller, start-up, or nonprofit ones. Even if a measure were to succeed in meeting section 512(j)(2)'s definition, it would soon be outpaced by rapidly developing technologies, and undoubtedly leave many rights holders unsatisfied.

---

[54] 17 U.S.C. 512(i)(2).
[55] S. Rep. 105-190, at 52.

As for the role of government, we must be clear that any government mandated standard technological measure (or measures) would contravene the plain language of the statue, which calls for the development of the measure "pursuant to a broad consensus" between copyright owners and service providers, in an open, fair, and voluntary process.[56]

Nor does the statute appear even to contemplate a role for government in "encouraging" such a process. Government "encouragement" is often perceived as government pressure. Any such pressure would fatally undermine the "voluntary" requirement.

As a final note, standard setting, even among similarly situated entities, can be a complex and difficult process that is best led by technologists in consultation with all affected parties, including users, rather than lawyers or government officials.

Question 12: Several study participants have proposed some version of a notice-and-stay-down 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 a system have for future online innovation and content creation?

In the interest of clarity, so-called "notice-and-stay-down" proposals should be identified for what they are: proposals to require service providers otherwise in compliance with the DMCA to proactively filter the Internet on the basis of allegations of copyright infringement.

EFF opposes any such requirement, for several reasons. First, there is no way to implement these proposals without monitoring Internet users' behavior and running afoul of section 512(m). Second, by shifting the burden and cost of enforcement away from copyright holders and onto service providers, these proposals would stifle competition for Internet services, exacerbate current problems with the notice and takedown system, and increase the risk that valuable, lawful speech will be silenced.[57] Third, filters are and will remain imprecise.[58] Filtering tools are unable to account for the complexities of fair use, licensing arrangements, or the possibility of claims targeting material in the public domain, and no filter has yet been shown to be completely successful at detecting and preventing infringement.[59] Filtering tools would also need to constantly adapt to keep

---

[56] 17 U.S.C. 512(i)(2)(A).
[57] Elliot Harmon, *"Notice-and-Stay-Down" is Really "Filter-Everything"*, Deeplinks (January 21, 2016), https://www.eff.org/deeplinks/2016/01/notice-and-stay-down-really-filter-everything.
[58] *See, e.g.*, Fred von Lohmann, *Testing YouTube's Audio Content ID System*, Deeplinks (April 23, 2009), https://www.eff.org/deeplinks/2009/04/testing-youtubes-aud.
[59] *See* Jayasuriya, et. al., *Forcing the Net Through a Sieve: Why Copyright Filtering is Not a Solution for U.S. ISPs* 4 (2009), https://www.publicknowledge.org/pdf/pk-filtering-whitepaper-200907.pdf (explaining that "filters will be underinclusive because their

pace both with evolving infringer practices and with increasing rights holder demands.[60] Fourth, a filtering mandate would distort the market for Internet services by privileging those service providers with sufficient resources to develop and/or implement costly filtering systems, reduce investment in new services, and impair incentives to innovate.[61] And finally, a filtering mandate that cannot adequately preserve access to non-infringing content raises serious constitutional questions.

A filtering mandate would not be the minor change to existing law that the anodyne phrase "notice-and-stay-down" suggests, but would rather dismantle the careful balance reflected in the DMCA.

Question 15: What approaches have jurisdictions outside the United States taken to address the question of ISP liability and the problem of copyright infringement on the Internet? To what extent have these approaches worked well, or created problems for consumers, content creators, ISPs, or other stakeholders?

In 2015, EFF joined over one hundred other organizations in endorsing the Manila Principles on Intermediary Liability,[62] a set of best practices for intermediary liability frameworks.[63]

---

technology is not advanced enough—and will likely never be advanced enough—to identify every instance of prohibited content on the network. Filters will also be overinclusive; as a filter will never be able to distinguish between fair, legal uses of content and illegal uses of content with 100 percent accuracy.").

[60] *Id*. at 5 ("Furthermore, as history attests, users will work to actively circumvent the filter, thereby luring the architects of the filter into a fruitless technological arms race.").

[61] Matthew Le Merle, et. al., *The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment: A Quantitative Study*, Booz & Co. 6 (2011), http://www.strategyand.pwc.com/media/uploads/Strategyand-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf (finding that increasing liability for online service providers that host content, for example by requiring those intermediaries to filter content, would "have a significantly negative impact on investment.").

[62] Press Release, Electronic Frontier Foundation, *International Coalition Launches 'Manila Principles' to Protect Freedom of Expression Worldwide* (March 24, 2015), https://www.eff.org/press/releases/international-coalition-launches-manila-principles-protect-freedom-expression.

[63] At a high level, the Manila Principles consists of six basic principles: (1) "[i]ntermediaries should be shielded by law from liability for third-party content," (2) "[c]ontent must not be required to be restricted without an order by a judicial authority," (3) "[r]equests for restrictions of content must be clear, be unambiguous, and follow due process," (4) "[l]aws and content restriction policies and practices must comply with the tests of necessity and proportionality," (5) "[l]aws and content restriction policies must respect due process," (6) "[t]ransparency and accountability must be built into laws and

Many jurisdictions, including the United States, have opted for "conditional-liability" frameworks, creating safe harbors for online service providers that comply with certain statutory requirements.[64] Some of those jurisdictions also include, like the DMCA's section 512(m), a prohibition against requiring intermediaries to engage in monitoring or filtering of their users' online activities.[65]

However, not all jurisdictions employing a conditional-liability framework have adopted the DMCA's notice-and-takedown style system, and some have opted to afford greater protection for users' online speech.

Notice-and-notice systems, which do not require the intermediary to block or remove access to content on receipt of a notice of infringement, provide the strongest protections for users' free expression and are more consistent with the Manila Principles.[66] Because the intermediary is not obliged to remove or block content, erroneous or abusive removals are less likely. Any content removal requests are evaluated by the user, and if necessary, by a court. Canada currently employs just such a system.[67] Under Canada's framework, once intermediaries receive a notice of alleged infringement from a rights holder, they must either forward that notice on to the subscriber or user, or provide the

---

content restriction policies and practices." Manila Principles, https://www.manilaprinciples.org.

[64] *See* Center for Democracy and Technology, *Shielding the Messengers*, supra note 48, at 6-7 (listing the European Union, the United States, and potentially India as jurisdictions employing conditional liability frameworks). This study also identified 11 countries whose bi-lateral trade agreements with the United States contain conditional liability frameworks "modeled on [the] DMCA safe harbor." *Id.* at 7. The study also notes "a recent survey commissioned by the World Intellectual property Organization identified the conditional-safe-harbor approach as the most widely adopted approach to copyright liability for intermediaries." *Id.*

[65] For example, the European Union Art. 15 of the E-Commerce Directive 2000/31/EC includes such a provision, as does, South Africa's Electronic Communications and Transactions Act of 2002 (No. 25 of 2002), *available at* http://www.gov.za/sites/www.gov.za/files/a25-02.pdf.

[66] *See The Manila Principles on Intermediary Liability Background Paper* ("Background Paper") 33 (May 30, 2015), https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf ("Such a mechanism ensures that the intermediary is not placed in a quasi judicial position—making determinations regarding the legality or illegality of content.").

[67] *See* Copyright Modernization Act, S.C. 2012, c. 20, Canada. Sec. 41.25-41.26, http://laws-lois.justice.gc.ca/eng/AnnualStatutes/2012_20/page-17.html#docCont; s*ee also* Jyoti Panday, et al., *Jurisdictional Analysis: Comparative Study Of Intermediary Liability Regimes Chile, Canada, India, South Korea, UK and USA in support of the Manila Principles On Intermediary Liability* 26 (July 1, 2015), https://www.eff.org/files/2015/07/08/manila_principles_jurisdictional_analysis.pdf; Background Paper at 33.

notice-sender with an explanation as to why they are unable to do so.[68] The intermediary is not obliged to take any action to remove or block access to the content, nor to terminate or suspend the subscriber's account. Following receipt of the notice, the subscriber herself determines whether to remove the content, or risk the content owner seeking a court order for removal.

While notice-and-notice systems provide greater protection than notice-and-takedown systems that require intermediaries to remove infringing content, they can benefit from additional safeguards. Without such safeguards, unscrupulous rightsholders may exert undue pressure on users.[69] For example, Rightscorp, a U.S.-based company, has abused Canada's notice-and-notice system to send misleading and threatening notices to Canadian users in an effort to extort settlement payments.[70] EFF joined Canadian user advocate groups in proposing additional safeguards against these abuses.[71]

Chile's approach to notice-and-takedown,[72] which requires a court order before an intermediary can be required to remove or block access to content, also provides more protection against unjustified content removals than notice-and-takedown systems that don't entail independent judicial review.[73] Users are also given the opportunity to seek judicial review or appeal the removal orders.[74] India uses a similar system for alleged

---

[68] Panday, *supra* note 67, at 27.
[69] *See* Jeremy Malcolm, *Canada Must Fix Abuse of Its Copyright Notice System,* Deeplinks (April 23, 2015), https://www.eff.org/deeplinks/2015/04/call-canada-fix-rightsholder-abuse-its-copyright-notice-system.
[70] *See id.*; *see also* Jeremy Malcolm, *New Tool to Help Notify Users When Their Content is Taken Offline*, Deeplinks (July 29, 2016) https://www.eff.org/deeplinks/2016/07/new-tool-help-notify-users-when-their-content-taken-offline (reporting that Rightscorp was "falsely threatening Canadian users with penalties that are not even applicable under Canadian law.); *see also* Michael Geist, *Rightscorp and BMG Exploiting Copyright Notice-and-Notice System: Citing False Legal Information in Payment Demands* (January 8, 2015), http://www.michaelgeist.ca/2015/01/rightscorp-bmg-exploiting-copyright-notice-notice-system-citing-false-legal-information-payment-demands ("Many Canadians may be frightened into a settlement payment since they will be unaware that some of the legal information in the notice is inaccurate.").
[71] *See* Jeremy Malcolm, *Upload Filtering Mandate Would Shred European Copyright Safe Harbor,* Deeplinks (Oct, 12, 2016), https://www.eff.org/deeplinks/2016/10/upload-filtering-mandate-would-shred-european-copyright-safe-harbor.
[72] *See* Background Paper at 27; Panday, *supra* note 67, at 13.
[73] *See* Background Paper at 27.
[74] *See* Center for Democracy and Technology, *Chile's Notice and Takedown System for Copyright Protection: An Alternative Approach* 8 (August, 2012), https://cdt.org/files/pdfs/Chile-notice-takedown.pdf.

infringing content, where intermediaries are not required to remove or block content unless they receive a court or administrative order to do so.[75]

Both notice-and-notice and judicial notice-and-takedown provide users with a greater degree of protection against both inadvertent and intentional censorship than extrajudicial notice-and-takedown frameworks. While EFF does not currently recommend changes to section 512, it is worth noting that some jurisdictions have designed frameworks governing intermediary liability that fall more on the user-protective end of the spectrum.

In contrast to these approaches, some jurisdictions have begun imposing obligations on ISPs to block access to specific websites, and others have imposed or are considering mandatory filtering obligations. These frameworks introduce dangerous mechanisms for Internet censorship, interfere with users' fundamental rights, and, often, prove ineffective in solving the problem of online copyright infringement.

Site-blocking often has broader impacts on lawful online speech than intended. When entire domains are blocked, every other page hosted by those domains are subject to the block, regardless of whether they contain infringing content.[76] Site-blocking is also largely ineffective at stemming online copyright infringement. Many sites are able to relaunch at new URLs, and users are often able to circumvent blocks using VPNs and the

---

[75] *See* Jeremy Malcolm, *Indian Victory Bears Out the Need for the Manila Principles*, Deeplinks (Mar. 24, 2015), https://www.eff.org/deeplinks/2015/03/indian-victory-bears-out-need-manila-principles (discussing a recent ruling by the Supreme Court of India on section 79 of India's Information Technology Act). The ruling is available at http://supremecourtofindia.nic.in/FileServer/2015-03-24_1427183283.pdf

[76] Christina Angelopoulos, et. al., *Filtering the Internet for Copyrighted Content in Europe* (Amsterdam Law School Research Paper No. 2012-04, Institute for Information Law Research Paper No. 2012-04, 2012), https://ssrn.com/abstract=1983866. Likewise, when sites are blocked based on an IP-address, it can inadvertently effect a large number of sites. Ben Grub, *How ASIC's Attempt to Block one Website Took Down 250,000*, The Sunday Morning Herald, June 5, 2013, http://www.smh.com.au/technology/technology-news/how-asics-attempt-to-block-one-website-took-down-250000-20130605-2np6v.html; *see also* Angelopoulos, et al. at 7.

Tor browser.[77] Marginal improvements to the effectiveness of site-blocking come at the cost of user privacy, requiring intrusive monitoring of user requests.[78]

Lastly, implementing site-blocking for copyright infringement also increases the risk that governments less hospitable to free speech and political dissent will employ those same mechanism to overtly censor information online.[79]

Government-mandated copyright filtering obligations pose perhaps the greatest danger to freedom of expression online. Currently, the Council of Europe and the European Commission are considering a proposal from the European Commission that would require ISPs to enter agreements with rightsholders to scan and filter user uploads for copyright infringing content.[80] Article 13 of the proposed Directive of the European Parliament and the Council on Copyright in the Digital Single Market would require online platforms that host "large amounts" of user-generated content to reach agreements with rights holders to "prevent the availability on their services of content identified by rights holders."[81] This means that any service provider hosting user-generated content,

---

[77] Paula Dootson, Kyle Pappalardo & Nicolas Suzor, *Blocking Access to Illegal File-Share Websites Won't Stop Illegal Downloading,* The Conversation (Dec. 15, 2016), https://theconversation.com/blocking-access-to-illegal-file-share-websites-wont-stop-illegal-downloading-70473 ("The experience from overseas shows how easy it is for a site such as The Pirate Bay to change its address faster than courts can keep up. Consumers can also easily use VPNs and proxies to access the sites through private and secure connections.").

[78] Angelopoulos, et al., Institute for Information Law, *Study of fundamental rights limitations for online enforcement through self-regulation* 30, http://www.ivir.nl/publicaties/download/1796 (noting "a clear distinction between blocking and filtering cannot be made, given that even cases of targeted and therefore 'specific' blocking, will often necessitate the 'filtering' of identifying data that help locate the content and differentiate it from other material may be required, if not the processing of the content itself. So, for instance, URL-based blocking which compares the website requested by the user with a pre-determined 'blacklist' of URLs of objectionable websites will result in the indiscriminate processing of all URLs passing through the filter, even if only few of these are subsequently blocked.").

[79] Jeremy Malcolm, *Censoring the Web Isn't the Solution to Terrorism or Counterfeiting. It's the Problem*, Deeplinks (Nov. 25, 2014), https://www.eff.org/deeplinks/2014/11/censoring-web-isnt-solution-terrorism-or-counterfeiting-its-problem.

[80] Malcolm, *supra* note 71.

[81] Article 13, Proposal for a Directive of the European Parliament and of the Council on Copyright in the Digital Single Market, https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-593-EN-F1-1.PDF

including non-commercial entities, would need to implement automated technologies to scan user uploads, and either block that content or pay royalties for its use.[82]

Academic experts,[83] civil society organizations,[84] and members of the EU's startup community[85] have all denounced the proposal. They have pointed out that the proposed filtering law would potentially conflict both with a significant provision in the EU's e-commerce directive[86] that prohibits EU Member States from imposing "general monitoring obligations" on ISPs and with case law from the Court of Justice of the European Union.[87] Further, following two landmark rulings from the Court of Justice of the European Union that connected that prohibition with the fundamental rights to free expression, access to information, and privacy of personal information,[88] the proposed Article 13 could also conflict with EU Member States' obligations to protect those fundamental rights.[89]

In the same vein, graduated response liability frameworks for conduit ISPs also pose serious threats to users' fundamental rights, with little evident impact on copyright infringement. Those schemes provide for imposition of progressive penalties against users' accused of infringement by their ISPs, often culminating in suspension or

---

[82] *See* Malcolm, supra note 71.
[83]Stalla-Bourdillon, et al., *Open Letter to the European Commission – On the Importance of Preserving the Consistency and Integrity of the EU Aquis Relating to Content Monitoring within the Information Society* ("Academics Letter") (September 30, 2016), https://ssrn.com/abstract=2850483.
[84] *See, e.g.*, Joe McNamee, *EU Copyright Directive – Privatised Censorship and Filtering of Free Speech*, European Digital Rights Initiative (Nov. 10, 2016), https://edri.org/eu-copyright-directive-privatised-censorship-and-filtering-of-free-speech; Press Release, Open Rights Group, *Copyright Reform Fails EU Citizens in Favor of Industry* (2016), https://www.openrightsgroup.org/press/releases/2016/copyright-reform-fails-eu-citizens-in-favour-of-industry.
[85] Silicon Allee, *EU Copyright Reform is Coming. Is Your Startup Ready?*, Medium (Feb. 8, 2017), https://medium.com/silicon-allee/eu-copyright-reform-is-coming-is-your-startup-ready-4be81a5fabf7#.mv053764j.
[86] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN
[87] *See* Sophi Stalla-Bourdillon, et al., *A Brief Exegesis of the Proposed Copyright Directive* 7-8 (Nov. 24, 2016), https://ssrn.com/abstract=2875296.
[88] *See* Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 November 2011; Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, 16 February 2012; *see also* Angelopolous, et al., *supra* note 78, at 27-28, for a discussion of the two cases.
[89] *See* Sophi Stalla-Bourdillon, et al., *supra* note 87, at 2; *see also* Academics Letter at 1-2.

termination of users' Internet access accounts. Graduated response laws have been challenged around the world for their potential to curtail users' fundamental rights. The UN's Special Rapporteur on Freedom of Expression, in 2011, expressed serious concerns with these programs.[90] They have also proven largely ineffective: South Korea's graduated response scheme, the first of its kind,[91] led to wide-spread termination of subscriber accounts for minor infringements, and seemingly had no impact on online infringement.[92] Korea's National Human Rights Commission recommended that the law be re-examined, and Korean lawmakers have proposed to repeal it.[93]

France's 2009 HADOPI law,[94] which created a government agency with the power to terminate Internet subscribers' connections, met a similar fate. Criticized as both expensive and ineffective, [95] the law faced constitutional hurdles from the beginning.[96] It was held partly unconstitutional by the French Constitutional Council, [97] who determined that Internet access termination under HADOPI violated the French constitution's guarantee of "free communications of ideas and opinions."[98] A subsequent version of the

---

[90] Frank La Rue*, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression* ¶ 49 (May 16, 2011), http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[91] Article 133(2), Copyright Law, Law No. 14432, amended as at December 20, 2016, *available at* http://www.law.go.kr/LSW/LsiJoLinkP.do?docType=JO&lsNm=%EC%A0%80%EC%9E%91%EA%B6%8C%EB%B2%95&joNo=013300000&languageType=KO&paras=1#.
[92] Danny O'Brien and Maira Sutton, *Korean Lawmakers and Human Rights Experts Challenge Three Strikes Law*, Deeplinks (Mar. 29, 2013), https://www.eff.org/deeplinks/2013/03/korea-stands-against-three-strikes.
[93] *Id*.
[94] Loi 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet, 135 Journal Officiel de la République Franćaise [J.O.] [Official Gazette of France], June 13, 2009, p. 9666.
[95] Rainey Reitman, *French Anti-Piracy Law Claims First Victim, Convicted of Failing to Secure His Internet Connection,* Deeplinks (Sept. 13, 2012), https://www.eff.org/deeplinks/2012/09/french-anti-piracy-law-claims-first-victim-convicted-failing-secure-his-internet.
[96] Danny O'Brien, *France Declares Three Strikes Unconstitutional*, Deeplinks (June 10, 2009), https://www.eff.org/deeplinks/2009/06/three-strikes-dead-in-france; Conseil constitutionnel, decision n° 2009-580 DC, 10 June 2009 reported in JO, 13 June 2009, 9675.
[97] Conseil constitutionnel, decision n° 2009-580 DC, 10 June 2009 at pt.16, *available at* http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf
[98] *Id.*

law[99] was later overturned and replaced, and its replacement[100] excluded the possibility of termination as a punishment.[101]

In summary, international approaches to ISP liability illustrate the importance of safeguarding freedom of expression by protecting intermediaries against liability and providing adequate safeguards against abuse. They also demonstrate that blocking and filtering mandates, and draconian disconnection penalties are controversial, unpopular, and often ineffective at stemming online infringement.

Respectfully submitted,

Corynne McSherry
Mitch Stoltz
Kerry Sheehan
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
corynne@eff.org

[99] Loi 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet arts. 6 and 7, 251 J.O., Oct. 29, 2009, p. 18290.
[100] Décret n° 2013-596 du 8 juillet 2013, J.O. Jul. 9, 2013.
[101] Siraj Datoo, *France Drops Controversial 'Hadopi law' After Spending Millions*, The Guardian, July 9, 2013, https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy.