

# COLUMBIA LAW REVIEW

## *SIDEBAR*

---

VOL. 112

APRIL 12, 2012

PAGES 83-107

---

### THE UNENDING SEARCH FOR THE OPTIMAL INFRINGEMENT FILTER

*Sonia K. Katyal\* and Jason M. Schultz\*\**

*Response to: Lital Helman & Gideon Parchomovsky, The Best Available  
Technology Standard, 111 Colum. L. Rev. 1194 (2011)*

Professor Edward Felten has observed, “[i]n technology policy debates, lawyers put too much faith in technical solutions, while technologists put too much faith in legal solutions.”<sup>1</sup> In their Article, *The Best Available Technology Standard*, Lital Helman and Professor Gideon Parchomovsky demonstrate the power and potential consequences of “Felten’s Law” as they consider whether the current “safe harbor” architecture of the Digital Millennium Copyright Act (“DMCA”) strikes the appropriate public policy balance concerning online copyright infringement and the open Internet, ultimately concluding that it cannot without the help of “the best filtering technology available” to guide and architect the contours of legally permissible behaviors online.<sup>2</sup>

The authors’ proposal would profoundly alter the legal and technical schemata of the Internet: offering immunity only for webhosts that employ the best available method for filtering content prior to publication. Like many technologies, the idea of an optimal infringement filter—described as a rule-based, machine-implemented algorithmic approach to identifying and preventing infringement versus the more standards-based approach of the human mind and judicial enforcement—provides an attractive yet deceptive solution to the authors’ copyright quandary.

---

\* Joseph M. McLaughlin Professor of Law, Fordham University School of Law.

\*\* Assistant Clinical Professor of Law, and Co-director, Samuelson Law, Technology & Public Policy Clinic at UC Berkeley School of Law. Many special thanks to Caitlin Dempsey and Joseph Galvin for their outstanding research assistance, and to Fred von Lohmann, Mehan Jayasuriya, and the faculty of Fordham Law School for their excellent comments and suggestions.

1. See Paul Ohm, *Breaking Felten’s Third Law: How Not to Fix the Internet*, 87 *Denv. U. L. Rev. Online* 50, 50 (2010) (quoting Felten).

2. Lital Helman & Gideon Parchomovsky, *The Best Available Technology Standard*, 111 *Colum. L. Rev.* 1194 (2011).

Online infringement is a hard problem, both quantitatively and qualitatively. Machines play a large role in creating its complexity and prevalence; therefore, it makes sense to conclude that they may play a role in its solution as well. Yet, the presumption that machines can help solve legal problems is a relatively unproven one.<sup>3</sup> While there is much to admire in the authors' provocative and imaginative Article, there are significant questions and concerns that they need to address in order to justify such a drastic alteration of the legal architecture that the DMCA originally put into place. These range from evidentiary questions regarding what constitutes a "best" filter to doctrinal and definitional problems with the determination of infringement to constitutional and social welfare queries concerning due process and the First Amendment. While the authors initially address some of these questions, they, like their proposed solution, eventually defer to the machines themselves for answers, inadvertently implicating the very points that Felten has made.

### I. THE AUTHORS' PROPOSAL: TO ERR IS HUMAN, TO FILTER IS DIVINE

Perhaps the greatest shift offered by Helman and Parchomovsky is their focus on rebalancing the division of labor in copyright infringement enforcement. At the heart of the matter lies a powerful argument made by the authors: A system that acts, *ex ante*, to prevent infringement by incentivizing webhosts to screen materials prior to posting them is more desirable—from an economic and legal point of view—than a system that reacts solely, *ex post*, via a notice and takedown system. Under their solution, the webhosts, rather than the content owners, would filter for protected content and would do so prior to posting, checking material against a massive copyright database containing metadata and digital "fingerprints" to identify each copyrighted work at issue. The authors argue that the *ex post* takedown regime should still be employed, but only in addition to the filtering solution.

Legally speaking, the solution the authors propose would mark a significant departure from the current architecture of the DMCA. From 1994 to 1998, Congress closely examined the problem of online copyright infringement, ultimately enacting a safe harbor that shields online service providers from monetary liability for user-posted content as long as they meet a specified list of statutory requirements, including, *inter alia*, having a policy for terminating repeat infringing users and adopting a system that responds expeditiously to copyright infringement notices.<sup>4</sup>

Currently, section 512 of the DMCA provides webhosts and ISPs

---

3. See, e.g., Lawrence Lessig, *Code: Version 2.0*, 227 (2006) (explaining "technologies standing alone . . . do nothing to solve the problem of privacy on the Net"); Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 *Tex. L. Rev.* 553, 555 (1998) (arguing that "the set of rules for information flows imposed by technology and communication networks form a 'Lex Informatica'").

4. 17 U.S.C. § 512(i) (2006). If the user who posted the material objects to the "take-down" notice, she can counternotify and, if no subsequent lawsuit is filed, the material is allowed to be restored within ten to fourteen business days. *Id.* § 512(g), (j).

(collectively treated as “Online Service Providers” in the statute (“OSPs”)) with immunity from damages as long as they satisfy certain safe harbor definitions. As many scholars have shown, this section was the product of a delicate compromise reached by Congress between the twin forces of innovation and copyright protection: In order for the Web to develop and innovate, Congress recognized that OSPs would need some immunity from liability for copyright infringement by end users.<sup>5</sup> At the time, the application of the doctrines of vicarious and contributory copyright infringement to the complex world of the Internet was a relatively new phenomenon. As a result, OSPs sought clarification on their potential liability for activities like providing connections, storing data, caching and indexing content, and the like.<sup>6</sup> The resulting safe harbors, therefore, were motivated out of the recognition that limiting OSP liability would ensure “that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will continue to expand.”<sup>7</sup> At the same time, however, Congress set forth some levels of responsibility for webhosts and OSPs to follow: They can lose protection, for example, if the webhost fails to remove infringing material expeditiously, fails to reasonably implement a termination policy, or receives a direct financial benefit from the infringement while having the right and ability to control infringing activity.<sup>8</sup>

As long as the provider meets these qualifications, they do not have to actively police their computer networks and servers for infringement; rather, they can simply wait until they receive a valid notice to act. This places the burden of discovering infringing content squarely on copyright holders or their agents. As one commentator explained, given the automated nature of providing many online services, among other variables, the DMCA “allocates primary responsibility for policing content on the party with the greatest interest in protecting copyrighted work: the right holders themselves.”<sup>9</sup> As a result of these guidelines, intellectual property owners have undertaken a program of locating and notifying service providers of infringing material, and ISPs have developed a response system that acts to “take down” allegedly infringing material in order to avoid allegations of contributory liability.

More than ten years after this system was designed and agreed to by both the large content owners and online service providers of the day, the

---

5. H.R. Rep. No. 105-551, pt. 2, at 21 (1998) (explaining need for legislation); *id.* at 49–65 (outlining provisions of DMCA); S. Rep. No. 105-190, at 8 (1998) (explaining need for legislation); see also Edward Lee, *Decoding the DMCA Safe Harbors*, 32 *Colum. J.L. & Arts* 233, 269 (2009) (“[T]he DMCA safe harbors have helped to foster tremendous growth in web applications.”).

6. See Lauren G. Gallo, Note, *The (Im)possibility of “Standard Technical Measures” for UGC Websites*, 34 *Colum. J.L. & Arts* 283, 286 (2011).

7. *Id.* at 286–87, (quoting S. Rep. No. 105-190, at 8).

8. Jonathan J. Darrow & Gerald R. Ferrera, *Social Networking Web Sites and the DMCA: A Safe-Harbor from Copyright Infringement Liability or the Perfect Storm?*, 6 *Nw. J. Tech. & Intell. Prop.* 1, 27 n.184 (2007).

9. Gallo, *supra* note 6, at 302.

debate over its effectiveness rages on. Many content owners complain that it costs far too much to search the Internet for infringing copies and that the scale of the problem forces them to spend far more than is reasonable—indeed, an entire industry has sprung up that searches through peer to peer content, websites, and chat rooms to find evidence of infringement.<sup>10</sup> Service providers, on the other hand, tout their neutral role in the notice-and-takedown system as one of the key reasons that sites like Google, YouTube, Flickr, and Twitter are able to grow as rapidly as they have and reach as many people as they do; any duty to police, they argue, would curb if not cripple this ability to grow and offer access to invaluable resources and opportunities to speak and share online.<sup>11</sup>

To Helman and Parchomovsky, this current system is broken and in dire need of redesign or repair. The authors argue that the current safe harbor design lacks an incentive for webhosts to participate in copyright enforcement, leading to wastefulness and inefficiency. Because webhosts are not required to monitor content in order to receive safe harbor protection, they can basically hide their heads in the sand, the authors lament, remaining passive, and thus abstain from taking any affirmative measures that are not required by law.<sup>12</sup> Knowledge of infringing activity as a general matter is not enough to spark an investigative requirement, the authors point out, and even website titles with terms like “stolen” and “illegal” are not enough.<sup>13</sup> To make matters worse, the authors explain, under the DMCA webhosts have a disincentive from monitoring content because the ability to filter may suggest a level of “knowledge” and “control” that may render a webhost ineligible for the safe harbor protection. For all these reasons, the authors argue that webhosts typically act only after they are notified of the presence of infringing content. And copyright infringement, they seem to suggest, runs rampant as a result.

Given this controversial legal landscape, one must salute the authors for their bravado and courage in being willing to question and essentially reverse the burden of responsibility. In their Article, the authors largely side with the content industry in this debate, asserting that the costs of enforcement on the Internet are far too high and must be reduced. Unfortunately, without evidence to support this assertion, either in terms of the actual cost of such searching and enforcement, or the actual

---

10. See Sonia K. Katyal, *Privacy vs. Piracy*, 7 *Yale J.L. & Tech.* 222, 224–25 (2007) (“[C]opyright owners maintain automated Web crawlers that regularly survey and record the Internet Protocol addresses of computers that trade files on peer-to-peer networks.”); Sonia K. Katyal, *The New Surveillance*, 54 *Case W. Res. L. Rev.* 297, 330 (2004) (“An entire industry has sprung up, seemingly overnight, that searches through individuals’ hard drives, Web sites, and chat rooms to find evidence of infringement.”).

11. Brief of Amici Curiae Ebay Inc., Facebook, Inc., Google Inc., Iac/Interactivecorp, and Yahoo! Inc. in Support of Appellee, *UMG Recordings, Inc., v. Veoh Networks, Inc.*, No. 09-56777, 2010 WL 3706523, at \*7 (9th Cir. July 26, 2010) (explaining “[w]ithout the protections of the safe harbors, the possibility of statutory damages—multiplied by thousands of works—could threaten innovation on the Internet”).

12. Helman & Parchomovsky, *supra* note 2, at 1201.

13. See *id.* (citing *Perfect 10, Inc. v. Amazon.com, Inc.*, 487 F.3d 701, 763–64 (9th Cir. 2007)).

numbers of DMCA notices that content owners have sent since 1998, it is difficult to conclude—as they presume—that these costs and numbers are higher than an optimal technology policy would merit.<sup>14</sup> Nonetheless, the authors propose that rather than webhosts risking their immunity by selecting content for publication (as they believe the current law does), their solution would instead have webhosts risking their immunity by *not* filtering.

Hence, from their first core assumption emerges a second—that mechanical filters installed on service provider networks would reduce these costs and produce scalable efficiencies that benefit society. The authors craft these two assumptions into a drastic revision of the DMCA's current burden-sharing arrangement, under which webhosts would have to employ the best available filtering technology at the time the infringement took place in order to receive their safe harbor. The Article then goes on to describe several variants for how such a filter would be identified and implemented, primarily relying on the United States Copyright Office as the authority to select the filter technologies that qualify as “best” and to host a massive database of copyright information and “digital fingerprints” of works for the filters to use in their infringement analysis. Copyright owners would submit their information and their fingerprints to the Copyright Office, and then a small number of these approved filter services would access this database of protected content so that matches with online files could be identified and removed *ex ante* by the webhost prior to publication.

The authors argue that this result is far more desirable than the current system for three main reasons: (1) mechanical filters will be more cost-efficient than humans at identifying and removing infringing works, especially before they are published online; (2) their solution will spur much more innovation among filtering technologies; and (3) their solution provides encouragement to webhosts to filter and will not significantly harm social welfare concerns such as free speech or fair use. Further, the authors assure us that the use of a safe harbor ameliorates the legal uncertainties that webhosts currently face. “If a copyright infringement suit is brought against a webhost, all it will have to do to defeat the lawsuit will be to show that it referred users’ content to a clearinghouse for filtering at the time of the infringement,” the authors explain.<sup>15</sup>

## II. FOUR PROVOCATIONS FOR THE OPTIMAL INFRINGEMENT FILTER

Despite our initial skepticism, the possibility of an optimal, or even efficient, infringement filter seems like a worthwhile pursuit. However,

---

14. While such information is not universally publicly available, some public sources do exist. See, e.g., Chilling Effects, <http://www.chillingeffects.org> (on file with the *Columbia Law Review*) (last visited Feb. 10, 2012); National Intellectual Property Rights Coordination Center, <http://www.iprcenter.gov> (on file with the *Columbia Law Review*) (last visited Feb. 10, 2012).

15. Helman & Parchomovsky, *supra* note 2, at 1227.

like many such proposals, Helman and Parchomovsky seem to raise more questions than they answer. One of the biggest threshold issues is the authors' promise of protecting innovation as a desirable spillover effect of their solution. "The technological safe harbor we envision," the authors write, "is a dynamic one; it will change with technological progress, creating opportunities for technology companies to develop superior filtering technologies and spurring websites to adopt them."<sup>16</sup> The more effective the technology, the authors reason, the more likely it will be adopted by a larger number of websites, particularly if the law requires it.

While we empathize with the desire to encourage innovation, we would respectfully suggest that the authors take into greater consideration the immense costs that their proposal might impose on webhosts upon being deputized to do the work that copyright owners are already doing. While it is true that their regime would provide an emergent, unproven industry with an added incentive to innovate, the web services and content dissemination industries—proven drivers of economic growth<sup>17</sup>—would unquestionably be hampered if not harmed by the heavy cost of mandatory adoption, implementation, and maintenance. These costs could undermine other incentives and dampen development of a variety of new communication and distribution technologies, essentially "picking a winner" in the contest for R&D resources instead of allowing the technologies and markets to interact in a truly dynamic fashion. Moreover, to the extent it encourages copyright enforcement innovation, it locks it into the single category of filtering, even though it is well known that network technologies often "route around" content filters and inhibitors as an architectural matter.<sup>18</sup> Thus, even if there were dynamism in filtering innovations, such technology may well become irrelevant to the overall network in the end.<sup>19</sup> It is hard to

---

16. *Id.* at 1197.

17. See, e.g., Mathew Le Merle et al., *Booz & Co., The Impact of U.S. Internet Copyright Regulations on Early-Stage Investment: A Quantitative Study 2* (2011), <http://www.booz.com/media/uploads/BoozCo-Impact-US-Internet-Copyright-Regulations-Early-Stage-Investment.pdf> (on file with the *Columbia Law Review*) ("New startup companies have long been an important driver of innovation and economic growth in the U.S., and few of them would have grown to maturity without the early-stage financing that allowed them to bring their ideas to the marketplace.").

18. See Philip Elmer-Dewitt et al., *First Nation in Cyberspace*, *Time*, Dec. 6, 1993, available at <http://www.chemie.fu-berlin.de/outerspace/internet-article.html> (on file with the *Columbia Law Review*) ("As Internet Pioneer John Gilmore puts it, 'The Net interprets censorship as damage and routes around it.'"); see also Mehan Jayasuriya et al., *Public Knowledge, Forcing the Net Through a Sieve: Why Copyright Filtering is Not a Viable Solution for U.S. ISPs 29–35* (March 22, 2012), available at <http://www.publicknowledge.org/pdf/pk-filtering-whitepaper-200907.pdf> (on file with the *Columbia Law Review*) ("Even if we could somehow design a filter that was 100 percent accurate, users would actively work to circumvent that filter, in order to access the content of their choice without exposing themselves to liability."); Timothy, *Beating Comcast's Sandvine on Linux with Iptables*, *Slashdot* (June 29, 2008, 11:20 PM), <http://tech.slashdot.org/story/08/06/30/0249249/beating-comcasts-sandvine-on-linux-with-iptables> (on file with the *Columbia Law Review*) (discussing user circumvention of Comcast reset packets (quoting HiroDeckard)).

19. For an example of this in the digital music context, see Wikipedia, *Secure Digital*

imagine how the benefits of the dynamism the authors promise could compare with those from more general dissemination technologies—under their solution, the birth of another YouTube might be impossible if filtering is required in order to receive section 512 DMCA protection.<sup>20</sup>

Even aside from the threshold questions about dynamism, efficiency, and innovation, there remain other questions about their proposal. Below we group these questions into four provocations that identify what we consider crucial inquiries for making a compelling case for online ex ante infringement filters as an appropriate legal solution.

*A. Provocation One: The Evidence Questions*

As noted above, Helman and Parchomovsky propose a solution that has great intuitive appeal for those that believe that the current system is not only challenging and costly for copyright owners but also potentially futile. For example, the authors assert that “expenditures involved in policing the Internet on a regular basis and issuing takedown requests may be prohibitive for many content owners, particularly individual authors, and independent studios and publishers” and “[c]ooperation with webhosts may be the only feasible way to enforce the rights of these content owners.”<sup>21</sup> The authors argue that active monitoring and enforcement by webhosts can complement the efforts of content owners, because webhosts are best situated to disrupt infringing activities and because they have a better ability to deploy automatic filters and block materials *before* they are posted. Since copyright owners cannot apply automatic filters ex ante, nor can they limit searches to newly uploaded content, they are forced to comb through every type of file, ex post, for infringing content, over and over again, which seems overly onerous and economically wasteful. The authors write, “[i]mposing th[is] duty on content owners makes very little sense as they have no access to the code of hosting sites, and website operators will rightly be reluctant to grant content owners access privileges to their proprietary code or otherwise intervene in the core operation of their business.”<sup>22</sup>

While we agree about the potentially duplicative costs of forcing copyright owners to continually search each and every website for a particular type of file, we are not convinced that their solution offers a more economical alternative when one considers all of the various costs and benefits that their solution might generate. First, from a copyright protection standpoint, it is not clear what the exact economic and societal benefits are from an ex ante regime that removes infringing content at the earliest possible opportunity. While the authors argue that the most profitable window for a copyrighted work occurs at the beginning of its

---

Music Initiative, [http://en.wikipedia.org/wiki/Secure\\_Digital\\_Music\\_Initiative#Demise](http://en.wikipedia.org/wiki/Secure_Digital_Music_Initiative#Demise) (on file with the *Columbia Law Review*) (last visited Mar. 27, 2012).

20. Our thanks to Mehan Jayasuriya for offering these observations.

21. Helman & Parchomovsky, *supra* note 2, at 1203; *id.* at 1204 (characterizing act of sending DMCA notices as “Sisyphian task”).

22. *Id.* at 1213.

lifetime,<sup>23</sup> the *ex ante* filter is not tied to the date of the work's creation; rather, it is tied to the date of the allegedly infringing publication, which could be days or months or years later, especially in the case of out-of-print or so-called "orphan works" that may lack significant economic value.<sup>24</sup> In addition, presumptions of economic harm in copyright cases have recently come under fire, forcing copyright owners to provide courts with strong evidence of irreparable economic harm before gaining the benefits of injunctive relief, a remedy akin to what the authors propose.<sup>25</sup> Therefore, while the case for an *ex ante* injunction for some works might surely be justified, the case for others might be quite weak. To apply such a strong singular economic presumption to all copyrighted works ever created—regardless of how old they are and what their current economic value might be—raises serious questions as to the benefits such an approach offers and the evidence to justify them.

The authors also fail to offer much evidence on whether or not the costs of copyright-owner enforcement are indeed prohibitive; their only citations in support are to a single law review article speculating as to the problem of enforcement cost and examples of the cost of filtering services, not to any direct evidence on the cost of enforcement. Yet the cost to hire humans to search online and send takedown notices is a critical piece of evidence in this debate. For instance, it could actually be quite low, depending on the labor costs involved, and whether the work is being done in the U.S. or abroad. Further, it might not be necessary to take down every infringing file in order to maintain profitability in specific copyright industries, but rather to remove only the files that come up most often in searches on the first few pages of results. Obscure files are likely less damaging to copyright-holder interests, since they would be downloaded less often. Which version of cost and benefit is true? Again, more evidence on this point is needed.<sup>26</sup>

Moreover, from an innovation standpoint, it also makes sense to contemplate precisely why webhosts should bear the costs of copyright

---

23. *Id.* at 1204.

24. See generally U.S. Copyright Office, Orphan Works, <http://copyright.gov/orphan> (on file with the *Columbia Law Review*) (last visited Feb. 10, 2012) (providing background information on orphan works problem).

25. See *infra* note 76 and accompanying text (discussing recent case law establishing injunctions are not automatic in infringement cases).

26. Another example is this series of statements:

The cost of the extant regime is exacerbated by the time-sensitive value of intellectual property. As a general rule, copyright content is most valuable immediately after its release. With the passage of time, the value of content diminishes. As a result, by the time offending content is finally removed, it may be virtually valueless.

Helman & Parchomovsky, *supra* note 2 at 1204. Yet the sole citation for these assertions is to *Nat'l Basketball Ass'n v. Motorola, Inc.*, 105 F.3d 841, 853 (2d Cir. 1997), a case about noncopyrightable "hot news" that has been heavily critiqued and is doctrinally inapplicable to copyrighted works. Moreover, there is strong evidence that many copyrighted works have "long tails" that allow them to produce both intrinsic and extrinsic value over time. See Chris Anderson, *The Long Tail: Why the Future of Business is Selling Less of More* 19–22 (2006) (describing "long tail" of album tracks).



enforcement when their role, since 1998, has been largely to publish without making content-based considerations. Indeed, their immunity—and often their profitability—has depended on it, and to shift the burden along the lines suggested would require a more precise examination of the effects on business models and paths towards innovation. For example, in calculating the “cheapest cost avoider,” the authors would have to calculate, or at least estimate, the effect of the substantial shift in information costs regarding copyrighted properties that would now be faced by webhosts due to the shift in filtering responsibilities.

Further, requiring webhosts to filter would substantially raise the cost of publication for webhosts without a predictive sense of how they will respond to this changing variable, namely, how the culture and speed of the Internet is likely to change with automated webhost filtering. The original design of the Internet is largely open and easy to build upon—a system that is designed to move content between hosts and clients as quickly, cheaply, and neutrally as possible, leaving other parties to make determinations about legality and appropriateness after they are posted. Yet content filtering by webhosts necessarily introduces an element of selection and delay into the posting of content, potentially changing the nature and speed of web publication generally.<sup>27</sup> How will webhosts respond? Consider, for example, Professor Tim Wu’s observations when confronted with the idea of ISP filtering by AT&T:

On the technical side, if I were an AT&T engineer asked to implement this plan, I would resign immediately and look for work at Verizon. AT&T’s engineers are already trying to manage the feat of getting trillions of packets around the world at light speed. To begin examining those packets for illegal pictures of Britney Spears would be a nuisance, at best, and a threat to the whole Internet, at worst. Imagine if FedEx were forced to examine every parcel for drug paraphernalia: Next-day delivery would soon go up in smoke. Even China’s Internet, whose performance suffers greatly from its filtering, doesn’t go as far as what AT&T is proposing.<sup>28</sup>

While Wu is definitively speaking about ISP filtering, as opposed to webhosts, we would respectfully suggest that his observations are salient in this context as well, particularly given that AT&T engages in both webhosting and more traditional ISP activity. Moreover, when one considers the slim margins in the web hosting market due to heavy competition—for example, YouTube offers free hosting for videos—and the predicted costs of filtering (which the authors acknowledge could be up to \$1 million per month per webhost in some instances), one must also

---

27. Jayasuriya et al., *supra* note 18, at 27 (“No matter how sophisticated filtering technologies eventually become, filtering will always slow the speed of traffic that travels over the network, so long as it is used to prevent unwanted or disfavored content from reaching users.”).

28. Tim Wu, *Has AT&T Lost its Mind?*, *Slate* (Jan. 16, 2008, 10:15 AM), [http://www.slate.com/articles/news\\_and\\_politics/jurisprudence/2008/01/has\\_att\\_lost\\_its\\_mind.html](http://www.slate.com/articles/news_and_politics/jurisprudence/2008/01/has_att_lost_its_mind.html) (on file with the *Columbia Law Review*).

question whether the benefits of preventing *ex ante* infringement would outweigh the costs to consumers, especially given that web hosts are likely to pass these costs onto the consumer regardless of whether they have ever uploaded infringing content or not.

Indeed, we note Wu's observations because they suggest the need for further scrutiny of a fascinating distinction that the authors make between actively distinguishing ISPs from webhosts. While they aggressively favor webhost filtering, curiously, the authors just as aggressively *oppose* filtering by ISPs. Ironically, they conclude—just as Wu does—that applying their system to ISPs would “yield considerably more harm than benefit,” namely, harm to innovation privacy, censorship, etc.<sup>29</sup> Moreover, since ISP filtering involves scrutinizing all internet traffic in real time, they observe, it would degrade the performance of the system. Indeed, the authors themselves even point out that the lack of ISP transparency and the significant costs of ISP filtering suggest that the costs of filtering are likely to be borne by the subscriber, further surrendering users' interests.

Despite these concerns, which they lay out in convincing fashion, the authors then take the opposite view—aggressively promoting filtering by webhosts. Yet for us, the most interesting question to examine is why the authors draw such a unilateral distinction between the two. There is very little discussion here of what evidence draws them to reach this distinction, and more information here would be helpful. Many ISPs also provide webhosting services (AT&T, for example)—and at the very least, some more discussion may be necessary to explain why the Article takes a unilateral stance against ISP filtering but would require it in the webhost context. For example, as the authors note, the performance costs that ISPs would incur attempting to filter traffic in real time are significant, yet video sites like YouTube receive over sixty hours of video every minute in real time.<sup>30</sup> The Article fails to explain why the impact of filtering on the performance of YouTube (or perhaps more importantly, smaller, less-resourced, sites) is any less of a concern.

The law, too, has at present failed to treat them differently as a policy matter, particularly where the all-important safe harbor is concerned, which suggests that Congress was just as concerned about innovation in the webhosting domain as it was in the ISP realm.<sup>31</sup> We note these

---

29. Helman & Parchomovsky, *supra* note 2, at 1241.

30. YouTube Blog, Holy Nyans! 60 Hours per Minute and 4 Billion Views a Day on YouTube, <http://youtube-global.blogspot.com/2012/01/holy-nyans-60-hours-per-minute-and-4.html> (Jan. 23, 2012) (on file with the *Columbia Law Review*).

31. Indeed, the DMCA and case law all too often conflate the two. See Darrow & Ferrera, *supra* note 8, at 13 n.90 (reaching this observation). Construing the term “service provider,” courts have consistently applied a very broad definition, encompassing webhosting entities and other activities like Aimster, eBay, and Amazon. *Id.* at 13 nn.89–93 (citing *In re Aimster Copyright Litig.*, 334 F.3d 643, 655 (7th Cir. 2003) (“[T]he definition of Internet service provider [contained in § 512(k)(1)(B)] is broad . . . and Aimster fits it.”); *ALS Scan, Inc. v. RemarQ Cmty., Inc.*, 239 F.3d 619, 623 (4th Cir. 2001) (noting DMCA defines “service provider” broadly); *Corbis Corp. v. Amazon.com, Inc.*, 351 F.Supp.2d 1090, 1100 (W.D. Wash. 2004) (holding “Amazon fits within the definition [of a ‘service provider’

evidentiary points, not just as a statutory matter, but because they suggest that the authors may be overlooking the kinds of concerns that led Congress to immunize webhosts (along with ISPs) in the DMCA. Innovation happens at many points and from many different entities, and we would respectfully suggest that the authors may wish to consider further the distributive costs that webhosts would face under their solution and how it might affect future business models.

In addition, the authors assert that there is a disincentive to filter or monitor outside the very narrow “red flag” bounds that the DMCA requires.<sup>32</sup> According to Helman and Parchomovsky, the current legal regime lacks sufficient predictability and certainty, leaving webhosts in an undecided gray area. Yet, examples of active filtering and monitoring abound in the form of YouTube’s Content ID and the existence of filter vendors such as Audible Magic. A recent study reported that “all” major copyright holders and user-generated content sites utilize filtering technology in some form, and one digital fingerprinting company, Audible Magic, offers its technology for free to smaller user-generated content sites.<sup>33</sup> If webhosts had disincentives to filter or monitor, then who is hiring these vendors? Further, what accounts for the range of voluntary extralegal measures that webhosts have willingly undertaken to address infringement, like the landmark User Generated Content Principles (UGC), which marshaled agreement from both the content industries and the web services industry?<sup>34</sup> The Principles clearly anticipate the use of content identification technology that eliminates infringing content, and also call for copyright owners to provide user-generated content web sites with copyright reference material in order to establish a match and instructions on how to treat matches when they occur. Under this system, user generated web sites will utilize the reference information, filter and scan for matches, and respond to those matches—all before posting the material online.<sup>35</sup> Similarly, in the ISP context, the development of graduated response and copyright alert measures, while such measures are admittedly imperfect, does suggest that much of the authors’ concerns are being addressed through the development of voluntary measures to curb infringement online. Consequently, it seems that the authors may overstate the law’s effect on social norms, without truly grappling with the variety of solutions—and incentives to filter—that are already firmly in

---

in the context of the § 512(c) safe harbor]”); *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1088 (C.D. Cal. 2001) (“eBay clearly meets the DMCA’s broad definition of online ‘service provider.’”).

32. Helman & Parchomovsky, *supra* note 2, at 1202.

33. See Gallo, *supra* note 6, at 312 & n.239.

34 The User Generated Content Principles were developed by “leading commercial copyright owners . . . and services providing user-uploaded and user-generated audio and video content . . . to foster an online environment that promotes the promises and benefits of UGC Services and protects the rights of Copyright Owners.” See User Generated Content Principles, <http://www.ugcprinciples.com/> (last visited April 8, 2012).

35. See Gallo, *supra* note 6 at 295 (“UGC’s are essentially required to participate in this matching process by using the reference material to ‘filter’ or scan user-uploaded content before that content is made available on its services.”).

place.

A related assumption is that competition in the marketplace for filter development is suboptimal.<sup>36</sup> Yet the authors provide little to no data on this issue; of course, more innovation may often be desirable, but without some empirical sense of the incentives—or disincentives—to innovate in this field, it is hard to say what an optimal level would be. (Indeed, from our end, antipiracy efforts seem to be rapidly growing and improving, not shrinking, under the watchful encouragement of the content industry.)<sup>37</sup> Some of these measures are far more creative and innovative than the authors' method would allow; for example, YouTube's Audio ID and Video ID operate by enabling a rights holder to choose whether to block, track, or monetize the posting, offering a wider menu of content management tools to the copyright owner than a filter alone would provide.<sup>38</sup>

A further, evidentiary point: While we are sympathetic to the idea that having copyright owners constantly troll the Internet for infringing material is costly, we remain less convinced that costs would be lowered by shifting the responsibility to webhosts instead. Both systems involve some duplication: Currently, the authors maintain that content owners have to scan each and every site for infringing material; and under their proposal, each and every webhost would have to scan each and every file prior to posting. The difference between the first and the second scenarios, however, is that there is arguably more collective action in the first instance, because more and more copyrighted works are becoming concentrated in the hands of fewer and fewer parties, and because rights holders face lower information costs than webhosts regarding their copyrighted works. This brings down the cost of monitoring because copyright holders' filtering strategies already bundle more and more works in their efforts.<sup>39</sup> Arguably, since there appear to be only a limited number of piracy surveillance vendors, the arguments about preserving competition are still true even in an ex post regime, making it unclear precisely how much would actually be saved by transferring these costs to

---

36. Helman & Parchomovsky, *supra* note 2, at 1203–04.

37. The Computer Crime and Intellectual Property Section of the United States Department of Justice provides much information on this topic. See, e.g., 2010 U.S. Intellectual Property Enforcement Coordinator Annual Report on Intellectual Property Enforcement 39 (2011), available at <http://www.cybercrime.gov//ipecreport2010.pdf> (on file with the *Columbia Law Review*) (“In FY 2010, cooperative efforts by CBP and ICE, including joint operations such as Operation Guardian, resulted in 19,959 seizures, an all time high.”). The Department of Justice also summarizes key prosecutions. U.S. Dep’t of Justice, Pro IP Act Annual Report FY2010 18–19 (2010), <http://www.cybercrime.gov//proipreport2010.pdf> (on file with the *Columbia Law Review*) (“In FY2010, the [online piracy] initiative resulted in a number of significant prosecutions, including” one involving website operators who “pled guilty to criminal copyright infringement and to conspiracy to commit criminal copyright infringement”).

38. See Gallo, *supra* note 6, at 296–97 & nn.108–114.

39. See Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 *Stan. L. Rev.* 1, 27 (2001) (explaining “[m]edia conglomerates can recycle and build upon their existing inventories at near-zero marginal cost. Others must purchase licenses at the supracompetitive price made possible by copyright law”).

webhosts. Further, the authors do not account for the possibility that much of the infringement that content owners care deeply about stems from a small number of websites (e.g., MegaUpload.com), which means that “trolling” the entire Internet may not be necessary at all. Comparatively, the startup costs of creating this new system would be significant, and shifting them to every single webhost seems inefficient without a deeper empirical showing of precisely how much would be saved, relative to the amount that has already been spent by copyright owners to solve the problem.

Even the issue of what would constitute the “best” filter poses questions of evidence and process. Arguing that a best available filter can be a determinable strategy is a bit like arguing that there is one best meal, best book, or best student out there. There are far too many variables—with too many types of copyrighted works and too many degrees of infringement—to presume that a singular standard can emerge and serve as a litmus test for safe harbor protection. For example, the authors’ argument rests on the presumption that false negatives (infringing posts that are not blocked) should be weighed equally with false positives (noninfringing posts that are blocked). We are not sure that the two are equal. While it is a difficult thing to weigh the costs of permitting one infringing file to exist versus the costs of censoring one noninfringing file, it is safe to say that the latter involves a potential chilling effect on speech broadly, whereas the former does not. Put differently, a single instance of censorship bears ripple effects that cause greater chilling of speech among noninfringing activity, and this is an externality that is worth considering.

A further question is institutional competence. Should we entrust this determination to an institutional body—the Copyright Office—that is at least arguably susceptible to capture and major public choice concerns?<sup>40</sup> Moreover, does the Copyright Office have the expertise to evaluate technological filters? One would imagine that this would require significant engineering, computer science, and informatics expertise, something the Copyright Office has not been delegated or funded to pursue. And what happens if the Office’s determination is contested? How many years and how much money will be spent litigating those issues? And what will happen to the safe harbor in the meanwhile?

Last, the information costs would be significant under the authors’ proposal due to the difficulty of identifying protected material. The authors acknowledge this, but then argue that a database that collects

---

40. See William M. Landes & Richard A. Posner, *The Political Economy of Intellectual Property Law* 25 (2004) (noting increase in legal protection of intellectual property since 1976 may be explained by political forces and ideological currents “abetted by interest-group pressures that favor originators of intellectual property over copiers”); Niva Elkin-Koren, *What Contracts Cannot Do: The Limits of Private Ordering in Facilitating a Creative Commons*, 74 *Fordham L. Rev.* 375, 375 (2005) (“The legislative process is captured by the content industries.”); Marci A. Hamilton, *Copyright Duration Extension and the Dark Heart of Copyright*, 14 *Cardozo Arts & Ent. L.J.* 655, 655 (1996) (“Again and again, Congress has been willingly captured by the publishing and motion picture industries.”).

copyrighted works and their metadata would solve this information deficit. Since the Copyright Office already has all of the necessary information about registered works, their reasoning goes, it makes sense to entrust them with the additional responsibility of hosting the “fingerprints” of the works themselves for identification during filtering. Copyright owners who do not utilize this formal process of registration should not be alienated from this regime, the authors explain, but should only be able to resort to notice and takedown procedures. Because of their failure to register their work in a central database, the authors explain, they would not lose value in their works, but only have access to an alternative system of enforcement.

Again, this observation forces us to ask the question of how much additional efficiency is being created by this system, in which a notice and takedown regime continues to remain in place, one that arguably manages to cover all protected works at the current time, and one that already incentivizes the copyright owner (the party with substantial informational advantages) to detect incidences of infringement. Or are the authors introducing more duplication with the creation of an *ex ante* and *ex post* regime? Furthermore, as Mark Lemley has written in the patent context, it may well be more efficient to use *ex post* regimes for IP enforcement due to the complex and expensive problem of predicting *ex ante* which rights will prove valuable enough to fight about over time.<sup>41</sup> Finally, at a time when U.S. federal deficits are skyrocketing, one must question how the Copyright Office would afford not only to store and make available in real time to any web host all *metadata* about every registered copyrighted work but also purchase and maintain storage for the millions if not billions of digital fingerprints the filters will need to check against uploaded files. Such databases and storage systems are not inexpensive and to the extent that they are privatized or outsourced in other ways, it would raise the costs of the authors’ solution significantly. At the very least, the question of marginal efficiency is an empirical question that—while difficult to investigate—makes sense to measure with a more holistic consideration of the variables involved.

#### B. *Provocation Two: The Infringement Questions*

Beyond the questions of evidence and metrics lies a core doctrinal concern: How will a machine, even a smart one, determine the legal question of infringement? The authors legitimately struggle with this, acknowledging that critical questions concerning fair use, tolerated use, and licensing pose significant challenges to the ability of filters to properly decide on which side of the infringement line any specific file should fall. However, in the end, they conclude that the tradeoff—more cost-efficient policing—is worth it and that so-called easy cases involving noninfringing

---

41. See Mark A. Lemley, *Rational Ignorance at the Patent Office*, 95 *Nw. U. L. Rev.* 1495, 1507–11 (2001) (noting only approximately 1.5% of patents issued are ever litigated, and concluding society should “deal with the problem [of a bad patent] *ex post*, if the patent is asserted in litigation”).

works and gray areas involving contested noninfringing works will be handled to the reader's satisfaction. To support this conclusion, they rely almost entirely on the presumption that the two most common file types to be filtered will be either the easy noninfringing works that have no matching content or entire "verbatim copies" of works are almost always infringing; thus, filters that detect these attributes will successfully determine the legal status of most files.<sup>42</sup>

In truth, however, the question of copyright infringement is far more complex than the authors give it credit. For example, in order to determine that a file is infringing, a mechanical filter would have to draw a sufficient legal conclusion concerning at least the following:

- Who is the owner of the copyrighted work?<sup>43</sup>
- Does the individual or entity that objects to the use of the work have standing under both Article III of the Constitution and Section 501(b) of the Copyright Act to enforce the copyright?<sup>44</sup>
- For works subject to the 1909 Copyright Act, were all applicable formalities satisfied?<sup>45</sup>
- Is the uploaded file substantially similar to the protectable expression of the original work of authorship, which excludes at a minimum unprotectable ideas, scènes-à-faire, expression that is merged with ideas, and standards within an industry?<sup>46</sup>

---

42. See Helman & Parchomovsky, *supra* note 2, at 1229–30 (describing categories of blatant copyright infringements, noninfringing posts, and some "hard cases").

43. See, e.g., Cmty. for Creative Non-Violence v. Reid, 490 U.S. 730, 749–50 (1989) (discussing importance of certain copyright ownership); Press Release, Elec. Frontier Found., Righthaven Copyright Troll Lawsuit Dismissed as Sham (June 14, 2011), <https://www.eff.org/press/archives/2011/06/14> (on file with the *Columbia Law Review*) (discussing dismissal of copyright lawsuit by organization that "never owned the copyright in the first place").

44. See, e.g., *Silvers v. Sony Pictures, Inc.*, 402 F.3d 881, 890 (9th Cir. 2005) (holding screenwriter who purchased right to sue for infringement still lacked standing without ownership of at least one exclusive right under 17 U.S.C. § 106); see also Elec. Frontier Found., *Diehl v. Crook*, available at <https://www.eff.org/cases/diehl-v-crook> (last visited Feb. 11, 2012) (on file with the *Columbia Law Review*) (describing settlement of case in which online journalist sued individual for sending "baseless [DMCA] takedown notices claiming to be the copyright holder of an image used in the story").

45. See, e.g., Elec. Frontier Found., *Jibjab Media v. Ludlow Music*, available at <https://www.eff.org/cases/jibjab-media-inc-v-ludlow-music-inc> (last visited Feb. 11, 2012) (on file with the *Columbia Law Review*) (describing settlement of challenge to copyright in "This Land Is Your Land" due to copyright owner's failure to renew registration under 1909 Act).

46. See, e.g., *Feist Publications, Inc. v. Rural Telephone Co.*, 499 U.S. 340, 350–51 (1991) ("Facts, whether alone or as part of a compilation, are not original and therefore may not be copyrighted."); *Lotus Dev. Corp. v. Borland Int'l Inc.*, 49 F.3d 807, 815 (1st Cir. 1995) (describing uncopyrightable "method of operation"), *aff'd per curiam* by an equally divided court, 516 U.S. 233 (1996); *Morrissey v. Procter & Gamble Co.*, 379 F.2d 675, 678–79 (1st Cir. 1967) (holding subject matter with limited forms of expression uncopyrightable).

- Has the work been licensed, either explicitly or implicitly, in any way that might authorize the use of it in the file?<sup>47</sup>
- Does the user who posted the file qualify for any of the statutory copyright defenses under 17 U.S.C §§ 107–127, including but not limited to fair use?<sup>48</sup>
- Has the copyright owner or the complainant engaged in any conduct that might constitute laches, estoppel, acquiescence, copyright misuse, or unclean hands?<sup>49</sup>

For example, consider the 1991 Supreme Court case *Feist Publications, Inc. v. Rural Telephone, Co.* There, a local telephone company sued a regional publisher for selling telephone directories that contained wholesale verbatim copies of its listings, including entirely fictional listings that were inserted in order to detect such alleged malfeasance. Despite thousands of acts of wholesale verbatim copying, the Supreme Court held that this behavior was noninfringing because telephone listings were not original works of authorship sufficient to earn copyright protection.<sup>50</sup> Yet, under the authors' "verbatim copy" test for accuracy, Rural could submit its phone book to the Copyright Office for filtering and we would expect every single website in the country to detect and ban Feist's publications as infringing.

Other examples of noninfringing uses involving 100% verbatim copies abound, especially in the fair use case law, where the amount of the work taken is only relevant to one of the four fair use factors.<sup>51</sup> One of the

47. See, e.g., *Field v. Google Inc.*, 412 F. Supp. 2d 1106, 1115–16 (D. Nev. 2006) (finding implicit license); see also Jayasuriya et al., *supra* note 18, at 9 (noting complexity of some mechanical licenses that might only authorize limited number of reproductions or limit distribution to certain geographies or time frames).

48. See, e.g., 17 U.S.C. § 121 (2006) (allowing full reproduction and distribution of works for blind or other people with disabilities).

49. See *Alcatel USA, Inc. v. DGI Techs., Inc.*, 166 F.3d 772, 792–95 (5th Cir. 1999) (finding copyright misuse); *Practice Mgmt. Info. Corp. v. Am. Med. Ass'n*, 121 F.3d 516, 520 (9th Cir. 1997) (holding AMA engaged in copyright misuse); *Lasercomb Am., Inc. v. Reynolds*, 911 F.2d 970, 972–77 (4th Cir. 1990) (tracing history of "misuse of copyright" defense).

50. 499 U.S. at 362–64.

51. See, e.g., *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 454–55 (1984) (100% copying of work verbatim for time-shifting is a fair use); *A.V. v. iParadigms, LLC*, 562 F.3d 630, 642 (4th Cir. 2009) (100% use of student papers protected by fair use); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1165 (9th Cir. 2007) (100% use of photo protected by fair use); *Bill Graham Archives v. Dorling Kindersley Ltd.*, 448 F.3d 605, 615 (2d Cir. 2006) (100% use of poster protected by fair use); *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 820–22 (9th Cir. 2003) (100% use of series of photos was fair use); *Bond v. Blum*, 317 F.3d 385, 393 (4th Cir. 2003) (use of entire book protected by fair use); *Nuñez v. Caribbean Int'l News Corp.*, 235 F.3d 18, 24 (1st Cir. 2000) (use of entire photograph "of little consequence to our [fair use] analysis"); *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 599 (9th Cir. 2000) (copying entire work multiple times for purposes of reverse engineering was fair use); *Sega Enters. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1527–28 (9th Cir. 1992) (same); *Triangle Publ'ns, Inc. v. Knight-Ridder Newspapers, Inc.*, 626 F.2d 1171, 1177 n.15 (5th Cir. 1980) ("[T]he idea that the copying of an entire copyrighted work can never be fair use 'is an overbroad generalization, unsupported by the decisions and



most prominent is *Sony Corp. of Am. v. Universal City Studios, Inc.* In *Sony*, the Supreme Court held that entire verbatim copies of plaintiffs' movies and television programs were fair use when they were copied for the purposes of personal noncommercial time-shifting.<sup>52</sup> This is another instance where the authors' "best available technology" filters would likely fail to produce the proper result.

This is not news to the authors, who attempt to mitigate the concern that fair use will suffer under a filter regime by claiming that the "best" filters will actually be able to detect other relevant factors such as whether or not the work has been published (an element of the second fair use factor) and even potentially whether the use is "commercial" or "transformative" under the first fair use factor.<sup>53</sup> However, again, the authors fail to provide any citations or evidence to suggest how the machines will provide such answers. There are no citations to the current literature on artificial intelligence, natural language processing, or computational linguistics to suggest that we are anywhere near the type of machine intelligence needed for such a task.<sup>54</sup> There are also, of course, substantial distributive consequences to this proposal: The authors admit that underrepresented groups may lose more than others (in a footnote, the authors note that "mash-up artists or other creators that rely on fair use, as well as the public's diffuse interests in preserving fair uses, might continue to be underrepresented compared to the narrowly focused interests of content industries, causing the latter to prevail despite representing the less socially optimal outcome").<sup>55</sup> The authors respond by suggesting the machines employ and develop a taxonomy of infringements—ranging from the most blatant types of piracy to the hardest cases—and then confidently predict that over time, the amount of human oversight needed over such cases is likely to decrease. Once again, this leaves us with little more than faith that the machines will provide what law and humans cannot.<sup>56</sup>

---

rejected by years of accepted practice." (quoting *Williams & Wilkins Co. v. United States*, 487 F.2d 1345, 1353 (Ct. Cl. 1973)); *Field v. Google Inc.*, 412 F.Supp. 2d at 1109 (fair use protected Google's commercial copying of 51 copyrighted writings in their entirety).

52. *Sony*, 464 U.S. at 442.

53. Helman & Parchomovsky, *supra* note 2, at 1230–31.

54. In fact, the Supreme Court and others have expressly rejected bright-line rule-based approaches to fair use. See *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 577 (1994) ("The task is not to be simplified with bright-line rules, for the statute, like the doctrine it recognizes, calls for case-by-case analysis."); *Sony*, 464 U.S. at 448 (the fair use doctrine "enable[s] a court to apply an equitable rule of reason" to copyright infringement claims (internal quotations and citations omitted)); *Perfect 10*, 508 F.3d at 1163 ("We must be flexible in applying a fair use analysis . . .").

55. Helman & Parchomovsky, *supra* note 2, at 1225 n.167.

56. At one point, the authors acknowledge that filters will not be "error-proof" but counter that "human review [of fair use] is not a silver bullet either." *Id.* at 1230. However, as they reference in a prior footnote, see *id.* at 1229 n.184, the notion that fair use case law is an unruly "wild west" without any discernable pattern or doctrinal consistency has been largely disproven empirically. See Barton Beebe, *An Empirical Study of U.S. Copyright Fair Use Opinions, 1978–2005*, 156 U. Pa. L. Rev. 548, 575 (2008) ("Overall, these data support the unexpected, if also somewhat uninspiring, finding that our fair use case law . . . has not

Finally, the authors do not sufficiently address how the filters would handle the critical fourth fair use factor, potential harm to the market for the original work, which must be balanced with the public benefit in access.<sup>57</sup> Such determinations are often vexing, even to lawyers and economists, and contested in almost every fair use case.<sup>58</sup> In response to this question, among the other complex legal issues raised by fair use, the authors propose that some human review will be necessary—again raising questions concerning how their solution will be any more efficient than the current one—and the idea that somehow, in the future, machines may surprise us with their ability to solve these complex problems.<sup>59</sup> While we share the authors' aspirations for improvements in machine learning and understanding of the law, the lack of evidence to suggest this will happen any time soon counsels against the adoption of their proposal rather than in favor of it.

Another problem area is how these filters will control for and anticipate potential defenses. Consider, for example, the defense of 17 U.S.C. § 117(a)(2), archival copying of computer programs. Under this exception, the owner of a computer program may make an entire verbatim copy of that program for archival purposes.<sup>60</sup> Given the emergence of cloud computing storage and backup services such as Dropbox, it would not be unreasonable to assume that numerous consumers would look to store archival copies of their computer programs online. Section 117(a)(2) would render these archival copies legal, yet even the “best” filter technology would flag them as verbatim copies that are infringing. This would also likely occur for consumers who attempt to store personal copies of digital music, movies, books, and other media that they purchase. Even though § 117(a)(2) does not cover works other than computer programs, most scholars and commentators believe such personal uses are likely noninfringing as well.<sup>61</sup>

---

been marked by especially high reversal, dissent, or appeal rates.”); Paula Samuelson, *Unbundling Fair Uses*, 77 *Fordham L. Rev.* 2357, 2541 (2009) (arguing fair use doctrine is “more coherent and more predictable than many commentators have perceived”); Matthew Sag, *Predicting Fair Use* 41 (July 6, 2003) (unpublished manuscript), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1769130](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1769130) (on file with the *Columbia Law Review*) (finding “considerable evidence against the oft-repeated assertion that fair use adjudication is blighted by unpredictability and doctrinal incoherence”).

57. See *MCA, Inc. v. Wilson*, 677 F.2d 180, 183 (2d Cir. 1981) (“[W]here a claim of fair use is made, a balance must sometimes be struck between the benefit the public will derive if the use is permitted and the personal gain the copyright owner will receive if the use is denied.”).

58. See, e.g., Mark A. Lemley, *Should a Licensing Market Require Licensing?*, 70 *Law & Contemp. Probs.* 185, 189–91 (2007) (describing and criticizing courts' new approach to evaluating fourth fair use factor).

59. Helman & Parchomovsky, *supra* note 2, at 1232–33.

60. See, e.g., *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255, 267 (5th Cir. 1988) (describing archival use exception for computer programs).

61. See Jessica Litman, *Lawful Personal Use*, 85 *Tex. L. Rev.* 1871, 1873–74 (2007) (noting even recording industry concedes “it is lawful for twenty-two million iPod owners to use them to listen to music they've copied from recordings they have purchased”); Aaron Perzanowski & Jason Schultz, *Copyright Exhaustion and the Personal Use Dilemma*, 96

Moreover, even the suggestion that filters will somehow “know” enough to make other legal determinations—such as whether or not a work has been published—is suspect. The authors suggest that the filters will be able to rely on the Copyright Office records for such information, or on information submitted by the copyright owners themselves. Yet there is no evidence that these records are accurate enough to presume their validity. The Copyright Office does not verify their accuracy, instead assuming that if publication is contested, it will be resolved in court. Thus, the incentives for copyright owners, even of unpublished works, would be to lie and always say that something is published, as it would directly benefit them in terms of filtering. As Jason Mazzone has shown, copyfraud continues to be a serious problem.<sup>62</sup> Ownership of a work can also be highly contested and illegitimate or multiple claims easy to make.<sup>63</sup>

These complex questions of infringement are exactly the reason Congress places service providers in a neutral role under the DMCA. While the providers do have important technical information about the file itself, they lack numerous facts that determine its legal status. Maintaining the copyright owner or her agent as the policing party is one way to allocate responsibility more closely to those most likely to know or discover these facts. Until and unless filters can somehow outperform copyright owners, it seems ill advised to us to shift this responsibility.

---

Minn. L. Rev. (forthcoming 2012) (manuscript at 3), available at <http://ssrn.com/abstract=1925059> (on file with the *Columbia Law Review*) (“Public opinion has generally embraced the notion that consumers are entitled to make personal use of their copies, particularly when that use is non-commercial.”).

62. See generally Jason Mazzone, *Copyfraud and Other Abuses of Intellectual Property Law* (2011). For examples of misguided attempts to assert copyright in publications that were not published or not copyrightable, see *Doe v. Geller*, 533 F. Supp. 2d 996, 1000–01 (N.D. Cal. 2008) (dismissing for lack of personal jurisdiction plaintiff’s claim that defendant “knowingly misrepresented to YouTube . . . that one of plaintiff’s video postings infringed defendants’ copyrights”); *Diehl v. Crook*, No. C 06-6800 SBA, slip op. at 1 (N.D. Cal. dismissed Mar. 16, 2007) (requiring plaintiff to email every person or entity to which he sent cease-and-desist notice and/or request relating to his appearance on Fox News withdrawing notice and/or request); *Online Policy Grp. v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1203 (N.D. Cal. 2004) (holding Diebold’s email archive was not subject to copyright because it “identified no specific commercial purpose or interest affected by publication of the email archive, and there is no evidence that such publication actually had or may have any affect on the putative market value, if any, of Diebold’s allegedly copyrighted material”). For more information about these cases, see Elec. Frontier Found., <https://www.eff.org/cases/sapient-v-geller>, <https://www.eff.org/cases/diehl-v-crook>, <https://www.eff.org/cases/online-policy-group-v-diebold>, and <https://www.eff.org/cases/electric-slide-litigation> (last visited Feb. 10, 2012) (on file with the *Columbia Law Review*).

63. See *Cnty. for Creative Non-Violence v. Reid*, 490 U.S. 730, 732 (1989) (involving dispute over ownership); Ernesto, *Music Royalty Collectors Accused of Copyfraud*, *TorrentFreak* (Oct. 2, 2011), <http://torrentfreak.com/music-royalty-collectors-accused-of-copyfraud-111002/> (on file with the *Columbia Law Review*) (discussing case of German musical collecting agency mistakenly demanding money from nonprofit organization for publishing licensed tracks).

*C. Provocation Three: The Due Process Questions*

Procedural due process has been the subject of several articles that are critical of the current safe harbor regime's notice-and-takedown provisions.<sup>64</sup> Thus, it is worth considering whether the authors' solution would provide more or less process. In his seminal article on procedural due process, *Some Kind of Hearing*, Judge Henry Friendly lays out eleven elements of a fair hearing. These include an unbiased tribunal; notice of the proposed action and the grounds for it; an opportunity to present reasons why the proposed actions should not be taken; the right to call witnesses; the right to know the evidence against one; the right to have a decision based only on the evidence presented; the right to counsel; the making of a record; a written statement of reasons; public attendance; and judicial review.<sup>65</sup> While Judge Friendly goes on to argue that not every one of these criteria is required for every hearing, they provide a useful framework for evaluating the impact of an optimal filter on due process concerns. Under these criteria, the authors' proposal does not appear to fare well. While one might argue that a mechanical filter is an unbiased tribunal and will only make a decision based on the evidence presented, there appears to be little in the authors' proposal to account for the other nine elements.

The best available technology standard also appears to lack any accountability for mistakes or knowing misrepresentations, either substantive or procedural. Who is responsible for violations of Judge Friendly's list? Who is responsible for suppressing the noninfringing creative expressions that might be flagged as false positives by this best filter? Under the current DMCA regime, Congress saw fit to include a counterbalancing mechanism for false and fraudulent takedowns, § 512(f), which allows suits by users or service providers against those who knowingly send notices with material misrepresentations in them.<sup>66</sup> And

---

64. E.g., Katyal, *supra* note 10, at 345 (arguing that "by clarifying the scope and entitlement of fair use, and by precluding extrajudicial determinations, we can come to a greater balance between privacy, property, and protection of expression"); Jennifer M. Urban & 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, 688-92 (2006) (calling for reform and suggesting changes that will "retain[] essential benefits for complainants, while increasing protections for targets"); see also Joseph M. Miller, *Fair Use Through the Lenz of § 512(c) of the DMCA: A Preemptive Defense to a Premature Remedy?*, 95 *Iowa L. Rev.* 1697, 1707-10 (2010) (critiquing current regime because copyright holders can receive "expeditious" takedown regardless of merits of claim, takedown takes effect before Internet user can object, and procedures ultimately harm Internet users); Benjamin Wilson, *Notice, Takedown, and the Good Faith Standard: How to Protect Internet Users from Bad-Faith Removal of Web Content*, 29 *St. Louis U. Pub. L. Rev.* 613, 628 (2010) (stressing that "proving copyright owners' subjective bad faith is extremely challenging" under current procedures).

65. Henry J. Friendly, *Some Kind of Hearing*, 123 *U. Pa. L. Rev.* 1267, 1279-95 (1975).

66. See 17 U.S.C. § 512(f) (2006); *Lenz v. Universal Music Corp.*, 572 F. Supp. 2d 1150, 1156-57 (N.D. Cal. 2008) (denying motion to dismiss when plaintiff user sued copyright owner for sending improper takedown notice); *Online Policy Grp. v. Diebold, Inc.*, 337 F. Supp. 2d 1195, 1206 (N.D. Cal. 2004) (holding copyright claimant violated DMCA by sending improper takedown notice); *First Amended Answer, Affirmative Defenses and Counterclaim*

while there has been some contest about what level of knowledge is required for liability, there is a clear answer as to who is held accountable—the sender of the notice. The Article is silent on this point, and as cases such as *Diebold* show us, it is far from an insignificant concern. Instead, once again, it is left to the ghost in the machine and the presumption of rational actors and competitive markets to sort it out.

And then there is the problem of the technology itself. Filtering technology is notoriously prone to mistakes and shortcomings and constantly risks being both over- and under-inclusive at the same time. It would be helpful for the authors to address some of these technologies more specifically, particularly given the authors' allegiance to their problem-solving potential. Filters employ varying methods of detection, which variously focus on: (a) the type of traffic involved, (b) the type of content, and (c) the end user's device.<sup>67</sup> We know, for example, that relying on types of protocol or traffic (like BitTorrent) to filter content is necessarily over-inclusive, blocking both legal and illegal content. But content filtering, too, can be subject to similar types of claims, mostly due to the complexity of determining the boundaries of fair use. Traffic inspection, for example, addresses the nature of the traffic but has been subject to FCC involvement from time to time because it casts a wide net that presumes that all types of content that flows through certain protocols are automatically less desirable and/or illegal. Comcast, for example, faced a reprimand by the FCC when it attempted to degrade traffic that utilized peer-to-peer protocols.<sup>68</sup>

Given these complexities, it might seem that filters that engage in a specific analysis of content are more desirable, because they draw on the metadata that accompanies a specific type of content—like the name of an artist or album, for example. However, even the metadata is highly prone to manipulation and mislabeling. Consider Public Knowledge on this point:

Take, for example, a song entitled "Happy Birthday." Given only this title, a filter would be unable to determine whether the work in question is the copyrighted song "Happy Birthday," a different song of the same name or something else entirely that has been mislabeled. If the filter attempts to identify the song based on its listed performer, it will run into a similar set of problems. Does the artist listed perform the song in question or is it an amateur cover of a song by that performer? Or, is the file in question simply a song performed in the style of that performer? . . . . Given that none of the data will be certifiably reliable, however, the filter will never be able to identify a piece of content based solely on its metadata with any degree of certainty. You might

---

to Defendant Hotfile Corporation to Plaintiffs' Complaint, *Disney Enters., Inc. v. Hotfile Corp.*, 798 F. Supp. 2d 1303 (S.D. Fla. 2011) (No. 11-20427-WILLIAMS), available at <http://www.scribd.com/doc/64860927/Disney-v-Hotfile-Answer-Counterclaim> (on file with the *Columbia Law Review*).

67. See Jayasuriya et al., *supra* note 18, at 12 (dividing filter performance into "traffic inspection, content analysis and instrumentation of the end-user's device"); Gallo, *supra* note 6 at 296–98 nn. 110–134 and accompanying text (describing fingerprinting).

68. See Jayasuriya et al., *supra* note 18, at 12 (citing complaint).

say that the filter would have trouble judging a book by its cover.<sup>69</sup>

Using watermarks, too, can be subject to difficulties because works that are not watermarked can automatically escape detection, creating the risk of under-inclusivity. Digital fingerprinting, another popular technique, utilizes a technique that generates a unique fingerprint for a particular file and then draws upon a search method to locate examples of the fingerprint.<sup>70</sup> While some critics argue that fingerprinting will slow Internet traffic (since it requires the file to download a significant portion of the filter), the authors do not address whether the same concern extends to webhosts.<sup>71</sup> Still, a file that uses a portion of clips or transforms them in some way might be subject to the filter's potential for over-inclusivity. Some fingerprinting technologies, such as Vobile's VideoDNA, allegedly do not even consider fair use when sending automated takedown notices.<sup>72</sup>

#### D. *Provocation Four: The Speech Questions*

As our case law has dramatically shown for years, the complicated dynamic between protection of speech and filtering technologies is nothing new. Large bodies of literature—domestically and internationally—have exposed substantial social welfare concerns when filters are employed.<sup>73</sup> These questions are not mere byproducts or externalities but central to the question of filtering itself and its relationship to copyright and constitutional doctrine. On this point, much more needs to be addressed.

The Supreme Court has told us in *Eldred v. Ashcroft* that the fair use doctrine and the idea/expression dichotomy are meant as safeguards for

---

69. See *id.* at 15. In fact, the question of whether “Happy Birthday” remains under copyright itself is contested. Robert Brauneis, Copyright and the World’s Most Popular Song 23 (Geo. Wash. U. Legal Studies Research Paper No. 111624, Oct. 14, 2010), available at [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=111624](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=111624) (on file with the *Columbia Law Review*) (discussing “three principal weaknesses in the claim that ‘Happy Birthday to You’ is still under copyright”).

70. Jayasuriya et al., *supra* note 18, at 21.

71. For a discussion of this point, see *id.* at 16–17.

72. *Id.* at 23.

73. See, e.g., *United States v. Am. Library Ass’n*, 539 U.S. 194, 208–09 (2002) (discussing concerns that filtering technology “erroneously block[s] access to constitutionally protected speech that falls outside the categories that software users intend to block”); Jayasuriya et al., *supra* note 18, at 1 (arguing “[c]opyright filtering . . . poses a number of dangers to Internet users, legitimate businesses and U.S. federal government initiatives to increase the speed, affordability and utilization of broadband Internet services”); Maira Sutton, Indian Authorities Try (And Fail) to Make Tech Companies Block Politically Offensive Content, Elec. Frontier Found. (Dec. 7, 2011), <https://www.eff.org/deeplinks/2011/12/indian-authorities-try-and-fail-make-tech-companies-block-politically-offensive> (on file with the *Columbia Law Review*) (discussing possibility that Indian “laws are used to monitor and block content with little or no oversight”).

First Amendment principles in copyright law.<sup>74</sup> Yet there is no evidence that any filter, let alone the best available, is currently capable of detecting when these principles should come into play. The authors presume that the “best filtering technology” will actually work in most instances. But if it doesn’t, for some reason (for example, due to countermeasures taken to evade filtering), then the law has effectively made a decision to grant a subsidy to companies that adopt suboptimal and perhaps even counterproductive technologies. It is hard to see how this system ensures more efficiency given this risk.<sup>75</sup> Moreover, recent case law regarding intellectual property infringement and injunctions has established that injunctions, both preliminary and permanent, are not automatic in either patent or copyright cases even when infringement has been found.<sup>76</sup> Yet one of the main benefits proposed by the authors of filtering is that the machines will block publication *ex ante*—a remedy that appears increasingly difficult to achieve in federal court these days. In light of these concerns, it is surprising that the authors insist so vehemently on *ex ante* filtering instead of *ex post* compensation. Given the strength of these precedents, monetary compensation would be the likely outcome from a federal court action and thus, potentially a better model for any technological approximation of law instead of blocking or banning content prior to publication. In fact, this appears to be how YouTube’s Content ID has increasingly approached the filtering issue.<sup>77</sup>

Without a compelling justification for explaining why *ex ante* filtering is preferable to *ex post* takedowns, the authors’ argument seems to seriously overlook the substantial prior restraint risks of their proposal. Given that *ex ante* prevention of publication is the quintessential example of a First Amendment prior restraint, there are additional strong reasons to resist this approach. Among them is the question of timeliness of

---

74. 537 U.S. 186, 220 (2003).

75. Thanks to Mark Patterson for this trenchant observation.

76. See *eBay, Inc. v. MercExchange, LLC*, 547 U.S. 388, 392–93 (2006) (“[T]his Court has consistently rejected invitations to replace traditional equitable considerations with a rule that an injunction automatically follows a determination that a copyright has been infringed.”); *Perfect 10, Inc. v. Google, Inc.*, 653 F.3d 976, 980–81 (9th Cir. 2011) (“[T]he propriety of injunctive relief in cases arising under the Copyright Act must be evaluated on a case-by-case basis in accord with traditional equitable principles and without the aid of presumptions or a ‘thumb on the scale’ in favor of issuing such relief.”); *Salinger v. Colting*, 607 F.3d 68, 77–79 (2d Cir. 2010) (holding preliminary injunctions are not automatic in copyright infringement cases); see also *Bethesda Softworks, LLC v. Interplay Entm’t Corp.*, No. 11-1860, 2011 U.S. App. LEXIS 21711, at \*5–\*6 (4th Cir. Oct. 26, 2011) (“At one time, federal courts, including this circuit, presumed irreparable harm in copyright cases once the plaintiff established probable likelihood of success on the merits. . . . In 2006, the Supreme Court declared such presumptions inappropriate.”); *Flexible Lifeline Sys., Inc. v. Precision Lift, Inc.*, 654 F.3d 989, 996 (9th Cir. 2011) (concluding “eBay applies with equal force to preliminary injunction cases as it does to permanent injunction cases”); *Christopher Phelps & Assocs., LLC v. Galloway*, 492 F.3d 532, 546 (4th Cir. 2007) (holding “any relief granted in equity is at the discretion of the district court, and a petitioner cannot claim that it was *entitled* to injunctive relief”).

77. *Impact of YouTube’s Royalty Agreement and Content ID, The Royalty Exchange* (Aug. 23, 2011), <http://www.theroyaltyexchange.com/wp/?p=42> (on file with the *Columbia Law Review*).

publication. The authors acknowledge that their filter model may be imperfect and there may be cases where mistakes are made. However, they argue, users should be able to counternotify and raise objections to being filtered and thus, be able to exercise their First Amendment rights at some future time if they are truly noninfringing.

However, our First Amendment cases show that the doctrine is quite time-sensitive, raising questions about the utility of counternotification.<sup>78</sup> Given that so many online political commentaries depend on reuse and remix of original video, government-mandated filters would almost certainly raise serious concerns.<sup>79</sup> Imagine, for example, that Fox News regularly submits each segment of the O'Reilly Factor as a separate copyrighted work to all of the best available filters immediately upon airing. The night before the 2012 Presidential Election, Mr. O'Reilly misrepresents the position of Barack Obama on a critical policy issue. In response, The Colbert Report and The Daily Show attack O'Reilly's misrepresentation by showing a clip of his program followed by other video clips that disprove his assertion. Under current copyright law, this type of commentary and criticism is classic fair use and nothing short of an eleventh hour temporary restraining order—which would likely be denied—would prevent it from airing on cable and satellite networks all over the country. However, for the online versions of shows, even the best filter would most likely block the clips *ex ante* from being published online because they used wholesale verbatim copies of the O'Reilly segment, an outcome explicitly prohibited by the *Arizona* decision. Any subsequent counternotification or appeal could take days if not weeks to resolve, rendering the critiques irrelevant in terms of influencing voters in the election.

At the very least, rewriting the DMCA to require content filtering from webhosts, without a prior showing of infringement would surely invoke the kind of constitutional scrutiny that the law originally sought to avoid. Again, while the authors spend some pages discussing this issue and acknowledging it as a concern, they ultimately delegate the tough questions and their consequences to the technology itself to resolve.

### CONCLUSION

Given the questions we raise about evidence, infringement, due process, and about the impact on social welfare from such filters, especially in the arena of free speech and the First Amendment, the Helman and Parchomovsky proposal seems premature and potentially ill-

---

78. See, e.g., *Ariz. Right to Life Political Action Comm. v. Bayless*, 320 F.3d 1002, 1004 (9th Cir. 2003) (holding regulation which required 24-hour waiting period on political advertisement within ten days of election was "severe burden on political speech" and violated First Amendment).

79. For some examples of political remix videos, see, e.g., *Synchronized Presidential Debating*, YouTube (Oct. 28, 2008) [http://www.youtube.com/watch?v=wfd5g8Y\\_Jqo](http://www.youtube.com/watch?v=wfd5g8Y_Jqo); *Vote Different*, YouTube (Mar. 5 2007), <http://www.youtube.com/watch?v=6h3G-IMZxjo;23/6.com>.



suites for solving the problems of online copyright infringement. Perhaps the machines will yet surprise us, but until they do, the current division of labor for enforcement seems more appropriate from the position of sound copyright policy.

Moreover, their proposal runs the risk of moving us backward instead of forward in terms of solving the online copyright conundrum. After all, technology changes over time; as filters develop, so do the means of circumventing them. For example, even as Comcast attempted to block BitTorrent traffic from operating, Slashdot reported on how users figured out ways to work around the blockage.<sup>80</sup> Were their proposal to become law, it may risk fomenting an arms race between the filters and filter circumvention technologies, one that may well be difficult to win.

---

Preferred Citation: Sonia K. Katyal & Jason M. Schultz, *The Unending Search for the Optimal Infringement Filter*, 112 COLUM. L. REV. SIDEBAR 83 (2012), [http://www.columbialawreview.org/assets/sidebar/volume/112/83\\_Katyal.pdf](http://www.columbialawreview.org/assets/sidebar/volume/112/83_Katyal.pdf)

---

80. Jayasuriya et al., *supra* note 18, at 30; Timothy, *Beating Comcast's Sandvine on Linux with Iptables*, Slashdot (June 29, 2008, 11:20 PM), <http://tech.slashdot.org/story/08/06/30/0249249/ beating-comcasts-sandvine-on-linux-with-iptables> (on file with the *Columbia Law Review*).