United States Senate

Committee on the Judiciary

Subcommittee on Intellectual Property

Section 512 Hearing: Is the DMCA's Notice-and-Takedown System Working in the 21st Century?

June 2, 2020, 2:30 p.m.

Statement of

Douglas J. Preston

President

The Authors Guild, Inc.

I welcome the opportunity to submit these comments on behalf of the Authors Guild in connection with my testimony before the Senate Judiciary Committee, Subcommittee on Intellectual Property.

The Authors Guild is a national non-profit association of almost 10,000 professional writers, many of whom struggle daily to combat the unauthorized online distribution of their works. Founded in 1912, the Guild counts historians, biographers, academicians, journalists, and other writers of nonfiction and fiction as members. The Guild works to promote the rights and professional interests of authors in various areas, including copyright, freedom of expression, and taxation. The work of my fellow Authors Guild members covers important issues in history, biography, science, politics, medicine, business, and other areas; they are frequent contributors to the most influential and well-respected publications in every field. As an organization whose members earn their livelihoods through their writing, the Guild has a fundamental interest in ensuring that works of authorship and the rights of authors are protected online, and that the hard

work and talents of our nation's authors are rewarded so that they can keep writing, as intended by the Framers of the Constitution.

Is the DMCA's Notice-and-Takedown System Working in the 21st Century?

I appreciate the directness of the questions in the title and I will answer them in that same spirit. The notice-and-takedown system is not working—at least not for authors, other individual creators, and small creative businesses. This is because of the extremely narrow way in which the courts have construed the disqualifications for section 512's safe harbors, effectively eliminating several prerequisites. The courts did so in part because of section 512(m)'s express statement that safe harbor protection is not conditioned on a duty to monitor, as explained below. The duty to monitor is one of the provision's most in need of amendment because it causes internal inconsistencies within the statute.

Nor is the statute working as Congress intended. The drafters of the Digital Millennium Copyright Act not only recognized the economic promise of the digital revolution, but they also recognized its perils to rightsholders—particularly to individual creators such as authors, who lack the resources to combat digital theft on an industrial scale. In enacting the DMCA in 1998, Congress intended for section 512 to strike a balance between the needs of rightsholders and the needs of internet service providers ("ISPs"), by incentivizing ISPs to cooperate with rightsholders in combating internet piracy, while at the same time promoting the development of a robust internet economy. At the heart of section 512 is a bargain struck between copyright owners and service providers: in exchange for protection from financial liability for the infringement of their users, the ISPs were to cooperate with copyright owners in protecting against copyright infringement on their services.[1]

The second aspect of the bargain hasn't worked so well. Courts have barely held ISPs accountable. With the exception of recent cases that enforced section 512(i)'s requirement to

[1] Rep. Goodlatte underscored this two-pronged approach when deliberating the bill, saying that "[i]f America's creators do not believe that their works will be protected when they put them on-line, then the Internet will lack the creative content it needs to reach its true potential; and if America's service providers are subject to litigation for the acts of third parties at the drop of a hat, they will lack the incentive to provide quick and sufficient access to the Internet." 144 Cong. Rec. 18774 (1998) (statement of Rep. Goodlatte).

adopt and reasonably implement a repeat-infringer policy,[2] most decisions interpreting section 512—particularly those in the Second and Ninth Circuits, where the largest number of copyright cases are brought[3]—have done so in favor of the ISP and to the detriment of the rightsholder. This, we believe, is due not only to the courts' understandable fear of interfering with the progress of nascent internet technologies, but also due to a misunderstanding of the bargain Congress intended to enact because of some inconsistencies within the statute as applied to today's ISPs. As the United States Copyright Office concluded in its recent report, "Section 512 of Title 17" (hereafter "Copyright Office Report" or the "512 Report"), courts have interpreted ISPs' "obligations and limitations…quite narrowly, resulting in broader application of the safe harbors than Congress likely anticipated."[4] As such, we believe that legislative action is required to clarify some of the provisions and thereby reset the intended balance of section 512.

But first, to give you a sense of what it is like to operate under section 512 today, I will describe the Authors Guild's and its members' experiences in trying to combat digital piracy through notice-and-takedown, as well as our efforts to work with some of the major platforms on behalf of authors, including some of our successes. This should help elucidate what's working in section 512, and what's not. Then, I will address section 512's interpretation by the courts, discuss how the statute's internal inconsistencies may have led courts to frustrate Congressional intent, and describe the Authors Guild's proposed changes to the statute to encourage real cooperation between all ISPs and rightsholders, particularly individual authors and other creators.

I. The Piracy Landscape

---

[2] See, e.g., *BMG Rights Mgmt. (US) LLC v. Cox Commc'ns, Inc*., 881 F.3d 293 (4th Cir. 2018); *UMG Recordings, Inc. v. Grande Commc'ns Networks, Inc.*, 384 F. Supp. 3d 743 (W.D. Tex. 2019); *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 511-517 (S.D.N.Y. 2013).); *UMG Recordings, Inc. v. Veoh Networks Inc.*, 655 F. Supp. 2d 1099, 1118 (C.D. Cal. 2009), aff'd on other grounds sub nom *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013); *Io Group., Inc. v. Veoh Networks, Inc*., 586 F. Supp. 2d 1132 (N.D. Cal. 2008).

[3] United States Courts, "Just the Facts: Intellectual Property Cases—Patent, Copyright, and Trademark," figure 2, "U.S. District Courts—Intellectual Property Cases Filed, by type, 1996-2018," *available at* https://www.uscourts.gov/news/2020/02/13/just-facts-intellectual-property-cases-patent-copyright-and-trademark#figures_map.

[4] U.S. COPYRIGHT OFFICE, SECTION 512 OF TITLE 17: A REPORT OF THE REGISTER OF COPYRIGHTS 85-86 (2020), https://www.copyright.gov/policy/section512/section-512-full-report.pdf (hereafter "512 Report").

From the perspective of Authors Guild members and countless other small creators, section 512 is clearly failing at "protecting the legitimate interests of authors and other rightsholders against the threat of rampant, low-barrier infringement," one of the two goals Congress had in mind when enacting the DMCA.[5] Online piracy is flourishing by every measure, taking on forms beyond those contemplated by the drafters of section 512, and decimating legitimate markets for electronic books and other content in the process.

In the last decade, the number of piracy complaints handled by the Authors Guild has skyrocketed. A study by Nielsen and Digimarc in 2017 indicated that pirates were selling 315 million dollars of stolen ebooks a year of illegal downloads,[6] with pirated ebooks depressing legitimate book sales by as much as 14%.[7] Since then, based on the amount of ebook piracy reported to the Authors Guild, that number has probably doubled. Studies have shown that the vast majority of illegal book downloads occur because they are so easy to find and acquire, and that the users who acquire ebooks illegally would have acquired the book legally (by buying a legal ebook or print copy or checking one out from the library) if the "search costs" of pirated ebooks were higher—in the other words, if illegal ebooks were more than a few clicks away.[8] And a new issue has developed in the last couple of years with the rise of pirated commercial ebooks sold at low cost on the same platforms as legitimate copies: unknowing readers innocently buy the illegal copies thinking they are just getting a good deal.

There is a clear correlation between the growth in piracy and the decline in incomes of authors. In 2018, mean writing incomes for full-time professional authors went down to $20,300, a 42% reduction in real dollars from a decade prior. Richard Conniff, writing in *The New York Times*, starkly sums up the impact of piracy on authors:

---

[5] *Id.* at 1.
[6] NIELSEN AND DIGIMARC, INSIDE THE MIND OF A BOOK PIRATE 4 (2017), https://www.digimarc.com/docs/default-source/default-document-library/inside-the-mind-of-a-book-pirate.pdf. The study also found that "convenience" was the most common reason users gave for choosing an illegal download over acquisition of a legitimate copy. 69% of study participants said that they would have acquired the book legally (by buying a legal ebook or print copy or checking one out from the library) if pirated copies were not conveniently available.
[7] Imke Reimers, *Can Private Copyright Protection Be Effective? Evidence from Book Publishing* (2016), 59 J. L. & ECON. (2016): 411, 414, https://doi.org/10.1086/687521 ("While physical formats are not affected by piracy protection, closer substitutes for online piracy such as legally distributed ebooks see a mean differential protection-related increase in sales of at least 14 percent.").
[8] *Id.* at 11.

> Authors need to eat, too, and we get by (or not quite, these days), by showing up at our writing places at a designated time day after day and staying there till we have fretted out our quota of words, to be sent off, after a time, to a publisher, in the hope that, two or three years down the road, a few pennies may come trickling back under the ludicrously grandiose name of "royalties." These days, though, what comes trickling back are mostly email alerts about websites in brazen violation of copyright law, offering free downloads of books the authors have spent years of their lives producing. At the moment, I have about 400 such offers of my own books in an email folder labeled "Thieves."[9]

Last, section 512's failure to protect authors and small creators is perhaps most starkly—and absurdly—illustrated by pirates who build DMCA complaint forms into their websites, even though the site operators are uploading the books themselves.[10] (Indeed, some, such as the erstwhile "Ebook.bike," provide instructions to "members" on how to buy an ebook, strip the DRM, and upload the book to try to pass themselves off as a platform for user-posted content, so that they can point to section 512 as a defense when, in fact, they are not eligible.)[11]

A. Sources of Book Piracy

Book piracy today takes several forms.[12] These include:

---

[9] Richard Conniff, *Steal This Book? There's a Price*, N.Y. TIMES (Sept. 15, 2019), https://www.nytimes.com/2019/09/15/opinion/book-piracy.html.

[10] For example, Ebook.bike, a notorious now-defunct pirate website, featured an occasionally functional DMCA form. Kissly.net, another notorious pirate site which sells illegal downloads, notes that it is DMCA compliant and includes a takedown form.

[11] *See, e.g.*, Section 512 Study Roundtable, Tr. at 180:2–14 (Apr. 8, 2019) (Mary Rasenberger, The Authors Guild), https://www.copyright.gov/policy/section512/public-roundtable/transcript_04-08-2019.pdf (hereafter "April 8 Roundtable Tr."). *See also infra* Part I.A.1.a.

[12] Authors trying to enforce their rights face the added nuisance of wading through a veritable morass of phishing websites and links. These sites, which do not host illegal copies but rather bait users with free book ads into giving up personal information or downloading malicious software, provide cover to pirate sites by requiring copyright users and their proxies to distinguish between pirate and phishing sites. Despite the prevalence of phishing activities and scams in connection with book searches on the Internet (according to Digimarc 70% of malicious links they encounter in their piracy investigations link to phishing sites), Internet users can take few if any meaningful actions to protect themselves. We are grateful to Senator Tillis and other Senators who have been pushing for reforms to curb phishing and other illicit scams and the harm they cause the creative economy; and we hope to continue working with members of this Committee to find solutions. Letter from Sens. Thom Tillis, Mazie K. Hirono, Theodore E. Deutsch to Joseph Simmons, Chairman FTC (Dec. 10, 2019), https://www.ipwatchdog.com/wp-content/uploads/2019/12/TT-MH-TD-12.10-Ltr-to-FTC-re-Illict-Streaming1.pdf

1. Rogue websites dedicated to free or monetized distribution of pirated ebooks that are found through Google and other search engines;
2. Unauthorized copies of ebooks and audiobooks posted for sale (usually at a highly discounted price) on online marketplaces such as Google Shopping, Google Play, and eBay;
3. User-posted unauthorized ebooks and audiobooks on third-party social media platforms; and
4. Download lockers and peer-to-peer torrent transfer.

In each case, the internet service hosting or linking to the infringing material is potentially eligible for the safe harbors under sections 512(c) or (d). I will review our members' experiences with these various forms of piracy in turn.

1. Dedicated Piracy Sites

It is nearly impossible to estimate the number of active pirate sites at any given moment, but studies show that even the most robust and vigilant notice-and-takedown efforts lag behind the genesis of new sites and number of pirate posts on existing sites, resulting in an inexorable increase in the total number of pirate sites over time.[13] Sarina Bowen, a best-selling author, an Authors Guild member, and active campaigner against online piracy, describes, like so many others, her experience in sending takedown notices as playing "whack-a-mole all day long. You can take down a book on one site and it will pop up on another site or even on the same site the very next day because someone else has uploaded it."

The "whack-a-mole" metaphor in the context of online piracy captures the diffuse and ephemeral nature of pirate activities as well as to the absurd manner in which section 512 is applied today due to judicial decisions of the last 25 years that have expanded ISP safe harbors while reading burdensome requirements for rightsholders into the DMCA. As described in Part II of this statement, the decisions have taken the teeth out of section 512 and left us with a law that

[13] *See, e.g.*, Reimers, *supra* note 7, at 438; LUIS; AGUIAR ET AL., EUR. COMM'N, JRC TECHNICAL REPORT: ONLINE COPYRIGHT ENFORCEMENT, CONSUMER BEHAVIOR, AND MARKET STRUCTURE (2015), https://ec.europa.eu/jrc/sites/jrcsh/files/JRC93492_Online_Copyright.pdf

requires copyright owners to notify platforms of each individual infringing copy on the service by URL, which excuses the platforms from removing any other infringing copies at other URLs—including those inevitably reposted by the same infringers.

The vivid whack-a-mole metaphor in relation to online piracy isn't simply anecdotal; it is sustained by empirical studies suggesting that meaningful progress against online piracy is only possible through a coordinated approach that targets multiple channels of piracy, instead of selectively taking down one or two channels at a time.[14]

The Authors Guild tracks a number of the well-known pirate websites that authors frequently complain about. These sites, many of which earn money from advertising, are accessible through Google and other search engines and show up in search results for book-related queries. Google, which controls more than 90% of the search market,[15] will demote such sites in their search results after a certain number of takedown notices have been received for the site—usually, it appears, in the thousands or tens of thousands. They do not take the links down, however, or disable access, so that anyone who knows the name of the site can easily find it by typing that in (whereas the site will not show up in a search for a book by book title).

a. Ebook.bike

The recently defunct Ebook.bike was a highly popular ebook piracy site that gained notoriety after successful romance and other genre authors discovered that pirated copies of their books appeared on the site soon after their release. The Authors Guild conducted its own searches and found a vast offering of recent fiction books of all genres on the site. We helped rally authors to conduct a takedown campaign (to demote them in search results), in identifying the location of the site's server, and in sending complaints to the hosting providers.[16] Even after

[14] Brett Danaher et al., *The Effect of Piracy Website Blocking on Consumer Behavior* (Aug. 14 2019) (unpublished article), https://ssrn.com/abstract=2612063 ("[I]t remains entirely possible that any disrupted channels to source content will simply be replaced with new ones linking to the same content or that pirates will easily find other channels to the same source content when it has not been removed and so our study seeks to test the hypothesis that the number of channels disrupted (and thus the strength of the intervention) impacts the effectiveness of this type of supply side antipiracy enforcement.").
[15] Jeff Desjardins, *How Google Retains More Than 90% of Market Share*, BUS. INSIDER (Apr. 23, 2018), https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4.
[16] Call to Action: Get Google to Remove Ebook.bike Links from Search Results, https://www.authorsguild.org/industry-advocacy/call-to-action-get-google-to-remove-ebook-bike-links-from-search-results/.

many thousands of DMCA takedown complaints from publishers, authors, and others, the site continued to appear in book-related search results on Google.[17] In response to the takedown notices, Google removed links to individual infringing URLs on the site from its search index, but took no further action, such as de-indexing or even demoting the site from appearing in search queries.[18] After a conversation with Google's legal team, however, we were able to get the site demoted from search results, so it no longer showed up in common book-related search results.[19]

Ebook.bike—like many pirate sites nowadays—featured a takedown webform, which, to authors' endless frustration, was rarely functional. In spite of their user-upload pretensions, it was clear that site administrators were less than passive hosts of user-content; in fact, they were likely the ones uploading most of the pirate copies. They were also providing users explicit guidance on buying ebooks from Amazon, stripping DRM protections, and uploading pirate copies. Yet this did not stop Ebook.bike operator Travis McCrea from asserting a 512(c) safe harbor in his answer to a lawsuit brought in Texas last year by author John Van Stry.[20] McCrea lost the lawsuit and was slapped with a permanent injunction and statutory damages amounting to $9,000 plus costs and attorney's fees.[21] The site is now offline, though it's highly doubtful that McCrea—who resides in Canada—will pay anything towards Van Stry's $9,000 in damages, and the upwards of $80,000 it cost to fight the lawsuit. The Ebook.bike fiasco shows exactly how 512(c) can be misused by pirates, and while they may ultimately lose against a tenacious and financially capable author-plaintiff, the conceit extracts endless labor from authors who are forced to send takedowns in the dark to those who are not legally entitled to the safe harbor.

b. Libgen

Library Genesis, also known as Libgen, and its companion site Sci-Hub, have been around in some form since as far back as 2008.[22] Libgen/Sci-Hub is well-known in the

[17] A record of takedown notices received by Google is public accessible through the Lumen Database, https://www.lumendatabase.org/notices/search?utf8=%E2%9C%93&term=Ebook.bike&sort_by=date_received+desc.
[18] April 8 Roundtable Tr., *supra* note 11, at 405:16-22, 406:1-4.
[19] *See infra* Part I.A.2, Role of Search Engines.
[20] Def.'s Answer, p. 1. *Stry v. McCrea et al.*, No. 2:19-cv-00104-WCB (E.D. Tex. Apr. 20, 2020).
[21] *Id.*
[22] *See* Joe Karaganis, *Introduction, in* SHADOW LIBRARIES: ACCESS TO KNOWLEDGE IN GLOBAL HIGHER

publishing industry as the target of a highly publicized copyright infringement lawsuit that Elsevier brought against it in 2015. In 2017, Elsevier won[23] a $15,000,000 default judgment and permanent injunction against the site, but the site simply moved to new domains and remains active, ranking among the most visited pirate sites.[24] The site is sometimes called "The Pirate Bay of Science" for the sheer volume of pirated books and scientific articles it serves. University professors have reported with dismay that many of the students enrolled in their courses download assigned books from Libgen instead of acquiring legal copies. Just one of the site's active home URLs has received over 14,000 takedown notices, yet the site and its mirrors can be easily accessed by searching for "Libgen" or "Library Genesis" in Google.[25]

c. Epub.pub, Graycity.net, Kissly.net

Epub.pub, Graycity.net, and Kissly.net are some of the other infamous pirate sites. Both Epub.pub and Graycity.net allow visitors to the sites to read full books directly from the browser. Kissly.net sells illegal ebook downloads at prices much lower than authorized ebook sellers. Epub.pub even allows users to flip pages in a book—as if reading on an e-reader or a physical book. Kissly.net and Epub.pub both misrepresent themselves as legitimate sites. But unlike Kissly.net, Epub.pub does not charge for books, and instead is monetized through donations and ads, with options to pay with Bitcoin or Amazon gift cards for complete untraceability. Epub.pub calls itself "the world's largest distributor of indie ebooks.…[that makes] it fast, free and easy for any author or publisher, anywhere in the world, to publish and distribute ebooks to the major retailers."[26] The site is especially notorious for posting new self-published romance novels.

2. Role of Search Engines

EDUCATION 2 (Joe Karaganis, ed. 2018) ("Unauthorized digital copies of books and articles began to be aggregated into online collections in the early 2000s. In most cases, these collections were small—personal collections of scanned materials shared via listservs and social media accounts. In a few cases, these collections grew into larger, curated archives—the Russian-language Library Genesis site (usually called LibGen), the Spanish-language Hansi library, and the social theory archive Aaaaarg (yes, the pirate sound) were early examples."). *See also,* Balázs Bodó, *The Genesis of Library Genesis, in id.* at 25.

[23] *Elsevier Inc. v. Sci-Hub*, No. 1:15-cv-04282 (S.D.N.Y. June 21, 2017), *available at* https://copyrightalliance.org/wp-content/uploads/2017/12/Elsevier-v-Sci-Hub.pdf.

[24] Libgen.Is: Competitive Analysis, Marketing Mix and Traffic, https://www.alexa.com/siteinfo/libgen.is (last visited May 30, 2020) (at time of access the site ranked 2803 in global internet engagement during an average 90-day period).

[25] Lumen Database, https://www.lumendatabase.org/notices/search?utf8=%E2%9C%93&term=Libgen&sort_by=.

[26] About EpubPub, https://www.epub.pub/about.

Dedicated piracy sites are easily accessible through search engines, and do not require any special technical facility (e.g., downloading additional software). Locating these sites is as simple as typing in "free ebook," "download," or even "ebook" with the book's title or author in the Google search bar. The pirate results appear right alongside the legitimate ebook vendors, with no distinction made between them. Indeed, the results might include a bewildering variety of links to pirate sites that let users read whole books in their browsers, sites that let users download entire collections, and even sites that pretend to be online bookstores selling ebooks at cut-rate prices to purchasers who may not even know that what they're paying for is a pirate ebook copy.

Google makes it particularly easy to get to these pirate sites and unknowingly buy pirated copies. In response to a user's query for a book, Google's search engine results include a carousel of Google Shopping ads from various third-party sellers, which users can click to buy a desired copy. Those Google Shopping buy buttons include links to pirate sites and pirate eBay sellers[27] mixed in with legitimate vendors, sometimes even ranking above legitimate vendors in search results if the pirates have bought promotional placement on the page. And since there is no way to tell a licensed ebook copy apart from a pirated copy, users will usually choose the cheapest offer not knowing that these cheap ebooks are in fact pirated copies. As explained earlier, readers generally do not know that most publishers—certainly all of the major ones—only sell ebooks through a handful of authorized sellers. It should be fairly simple for Google to screen out unauthorized sellers from Google Shopping, for instance by obtaining information about licensed vendors from publishers, yet the internet giant has undertaken no such effort to prevent Google Shopping from becoming a conduit for pirates selling illegal copies to unsuspecting users.

The search giant is equally indifferent to linking to pirate sites in its search results. Google refuses to de-index infringing sites even after receiving many thousands of takedown notices and having knowledge, but will demote the site in search results in connection with commonplace search queries. The fact that Google de-indexes and filters out sites containing

[27] *See, e.g.*, Search Results for "John Grisham ebook," https://www.google.com/search?q=john+grisham+ebook&sxsrf=ALeKk00U99UasFWw2CjvO5C5z8eC9wb5Cg:1590871815086&source=lnms&tbm=shop&sa=X&ved=2ahUKEwiShK-ru9zpAhUPmXIEHYYdBroQ_AUoAXoECA0QAw&biw=1237&bih=632#spd=16494352253607140011.

child pornography and other types of illegal content from its search results proves that it has the ability to do the same for infringing content. The Authors Guild has asked Google in the past to de-index sites like Ebook.bike and Epub.pub from search results for books, but we were only successful in getting them demoted so they don't appear whenever a user searches for a book title on Google. Users can still find the sites if they know the URL or the site name close enough to the URL. For instance, a user can navigate to Libgen to download pirated books even if they don't know the current exact URL by searching for "Libgen" in Google. Google's policy, as we understand, is to never prevent access to an entire site—even if it is one devoted to piracy. It will only remove links to URL-specific infringing items. This inability to block sites that have no function other than to serve up pirated content in any manner is particularly frustrating as the operators and fileservers of most of these sites are based overseas in countries where service of process is difficult, and judgments almost impossible to enforce.

Studies on the online piracy ecosystem suggest that when pirated copies are harder to access and locate (when their search costs are high), users switch to legal sources for their content needs.[28] There is no reason for search engines and other legitimate platforms covered by the DMCA to continue linking to pirate sites—not when they clearly have abundant knowledge of the pirate nature of these sites. If the section 512(d) requirements were interpreted in accordance with its plain language—as we believe Congress intended—then Google would be required to do more to escape liability.

3. User-Driven Illegal Distribution Through Social Media Platforms and Online Marketplaces

In recent years, pirates have started using social media platforms and third-party online marketplaces to offer free or monetized illegal downloads of ebooks. Unlike freestanding pirate sites, illegal downloads through third-party platforms can be harder to identify and target since these listings may not be located on a static URL, allowing them to evade anti-piracy web-crawlers used by takedown services. Also, individual platforms have their own content moderation requirements and web-based forms for takedown complaints, meaning that as a

[28] *See e.g.*, Danaher et al., *supra* note 15, at 11 (finding that website blocks of major piracy streaming sites "caused meaningful decreases in total piracy as well as a 7-12% increase in usage of paid legal streaming sites among users affected by the blocks.").

practical matter, copyright owners expend considerable time and effort in understanding and meeting the requirements of each platform.[29] The differences between policies and processes also result in inconsistent and uneven enforcement so that while some platforms respond and remove pirated content expeditiously, others do not. Social media sites are commonly used by readers of pirated books who may use these platforms to request and trade pirate copies, whereas commercial level pirates are more likely to use online marketplaces where they can easily list their pirated offers alongside legitimate sellers and sell illegal content to unwitting readers.

a. Facebook

Last year, the Authors Guild escalated complaints pertaining to 12 Facebook user groups devoted to sharing unauthorized copies of ebooks to Facebook's content enforcement team. In such pirate communities, unauthorized copies posted by group admins or other users can be downloaded by any member of the group. Our intercession was triggered by Facebook's inaction to authors' complaints to take down the groups themselves. Some of the targeted groups had been hosting thousands of pirated books. Facebook did respond to rightsholder complaints by taking down individual posts pursuant to URL-specific notices, but it did not take action to close the groups or to terminate repeat-infringer accounts despite having notice that the groups were being used for piracy. As a result, authors were finding new pirated copies uploaded to the groups by other Facebook users almost immediately after one was taken down. The Authors Guild worked with Facebook's content enforcement team to target repeat infringers, close the groups in question, and terminate user accounts of its administrators. Still, new groups devoted to piracy continue to appear on the platform.

b. LinkedIn/SlideShare

[29] As the Copyright Office's 512 Report notes: "The proliferation of new web-based submission forms and ISP-imposed requirements for substantiation of takedown notices in order to ensure the efficiency of the process has had the effect of increasing the time and effort that smaller rightsholders must expend to send takedown notices. At the same time, some of the current notification standards set forth in section 512(c) could be on their way to becoming obsolete. The Copyright Office therefore recommends that Congress consider shifting the required minimum notice standards for a takedown notice to a regulatory process, enabling the Copyright Office to set more flexible rules and 'future-proof' the statute against changing communications methods." 512 Report, *supra* note 4, at 5.

This past year, the Authors Guild received complaints from many of its members who had found links for pirated copies of their books on LinkedIn's SlideShare platform. Some authors reported seeing dozens of separate accounts on the platform that were advertising pirate links to their books. The links led to phishing sites as well as "free" ebook sites, where users could download pirated copies. A single account might have hundreds of documents containing links for illegal downloads (or phishing sites). Once again, authors who tried to take down the links found themselves ensnared in an endless whack-a-mole game: LinkedIn's takedown process was slow at first, and new accounts with the same infringing copies would pop up almost immediately after one was taken down. Since our members were reporting their experiences with sending takedown notices and the results in real time on a discussion thread in our online members' forum, we had the benefit of seeing how fruitless the takedown process was in real time. One member reported that LinkedIn had indeed taken down an infringing copy from the URL he had identified only to have not one, but 12 new infringing copies pop up the next day.

The Authors Guild communicated the scope of the problem to LinkedIn's rights enforcement team, and they encouraged our members to keep sending takedown notices so that they could identify repeat infringers and apply their repeat-infringer policy, which they seemed to have done, judging by a temporary reduction in the number of pirated copies. The Guild also urged LinkedIn to use algorithmic solutions based on commonly used phrases to automatically identify and remove malicious accounts and to vet new accounts in order to prevent bots from infiltrating the platform. To their credit, LinkedIn's content moderation team welcomed our suggestions and implemented authentication procedures to eliminate the posting of pirated copies by bots, leading to some mitigation. That said, SlideShare is still far from being clean of malicious accounts and ebook piracy.

c. eBay

Listings for pirated ebooks abound on eBay. These pirated ebooks can be purchased for as little as $1.99, with the pirate seller emailing the illegal file to the buyer once the transaction is done. When the Authors Guild contacted eBay on behalf of its members, we were simply pointed back to eBay's notice-and-takedown program, and eBay disregarded our reminder that there should be no ebooks at all on eBay (except in the very rare instance of an author putting up a self-published ebook) since the resale of an ebook is never legal, and publishers license only a

handful of authorized, readily identifiable ebook vendors. In other words, it would be very simple to screen out illegal ebooks.

Pirated eBay copies are prevalent not just on the eBay service but, for some books, the majority of pirated copies that appear at the top of the Google Shopping results are listed by eBay sellers as well. As noted earlier, when searching for a book on Google's search engine, it will display a Google Shopping carousel above or alongside the search results with thumbnails of copies of books indicating where they are from. If you click on the link, you are taken to a longer list of copies available on Google Shopping, and often many of those links are for pirated copies on eBay.

d. Other Platforms

Academia.edu, Scribd, Google Play, and Google Drive are other platforms being used to advertise and distribute pirated ebooks. Among the big internet companies, Amazon has been the most receptive to our concerns about ebook piracy. Its content enforcement team has instituted strong identification practices and technical measures to both prevent pirate accounts from infiltrating its marketplaces and to pre-emptively filter uploads of pirated content on its self-publishing services. When the Authors Guild notifies Amazon of a particular pirated ebook that has slipped through, in our experience, they are quick to remove it. This shows that when a platform has the incentive to keep pirated books off their service, they can do a pretty good job of it. However, unrelated to section 512, Amazon has not been as successful at keeping sales of physical counterfeit books sold by third-party resellers out of the Amazon marketplace. Our comments in response to Department of Commerce's NOI on the "State of Counterfeit Goods and Pirated Goods Trafficking" discuss the third-party marketplaces for physical goods, like Amazon and eBay, in greater detail.[30]

B. Small Creators Are Disproportionately Excluded from Preferred Notice Provider Programs

[30] *See generally* Authors Guild, Inc., Comments Submitted in Response to the U.S. Department of Commerce's July. 10, 2019, Notice of Inquiry on the State of Counterfeit and Pirated Good Trafficking 3 (July 29, 2016), *available at* https://www.authorsguild.org/wp-content/uploads/2019/07/Authors-Guild-Comments.DOC-Counterfeiting-1.pdf.

Examples provided by internet companies to illustrate the successful operation of the DMCA's notice-and-takedown regime are almost entirely based on the experiences of large rightsholders who have the technical and financial wherewithal to engage anti-piracy and digital rights management services to send millions of takedown notices on their behalf. In addition, these large rightsholders also have access to preferred notice provider programs such as Google's Trusted Copyright Removal Program or YouTube's Content ID program, and may even have private agreements with platforms to police user-uploaded content for infringement.[31] These preferred enforcement options are only open to rightsholders at scale; authors and small creators who are already struggling against the tide of tech disruption of the creative industries are excluded. Even the Authors Guild, representing its 10,000 members and other authors from around the world, has a very limited ability to obtain cooperation from ISPs. The good actors work with us—to some extent—but those who do not wish to help our members do not. Why not? It is simple: they don't think they have to. Companies such as Google insist that their only obligation is to comply with takedown notices. But, as we have shown, many authors find that engaging in notice-and-takedown is so ineffective and so time consuming that it is simply not worth it. They give up.

The impact of piracy on many self-published authors is even greater. Without support from agents or publishers, self-published authors are left to fend for themselves in the outlaw digital world, and copyright pirates take advantage of this. As some genres like romance have migrated to an all-digital medium, the burden is increasingly falling on authors to discover and target pirated copies of their work. Authors report spending hours navigating the complicated takedown forms of various platforms where pirated versions of their books are available and locating website hosts obscured behind DNS masking services (and often based in foreign countries) for what ends up being a momentary pyrrhic victory against pirates. Because after all their time and effort, if one link is taken down, five more may appear instantly; if one site goes offline, hundreds more take its place in a short period of time. Would anyone ever intentionally design such an inefficient and expensive system for all parties? It is certainly not what Congress had in mind in enacting the DMCA.

[31] *See generally* 512 Report, *supra* note 4, pp. 42-46.

As the Copyright Office's 512 Report emphasizes: "a system that fails to provide adequate protection of creators' rights of all sizes ultimately fails to carry out congressional intent regarding section 512 as well as the overall purpose of copyright law."[32]

II. Issues with Courts' Interpretation of Section 512

I will now move on to discuss why and how we are left with this absurdist, Sisyphean notice-and-takedown system (and re-post and re-notice and re-takedown, and so on…) as the only way that a rightsholder can address pirated content. I will then discuss some of the Authors Guild's ideas for how section 512 might be amended to serve its original dual purpose. I will focus primarily on: (i) the courts' heightening and conflation of the statute's knowledge and awareness standards in sections 512(c)(1)(A) and 512(d)(1); (ii) the courts' effective elimination of the vicarious liability standard in sections 512(c)(1)(B) and 512(d)(2); and (iii) their strict interpretation of the required elements of notification, which ignores express language in the statute. I will also explain how internal conflicts in the statute within these provisions and with section 512(m) (which provides that the ability of an ISP to avail itself of the safe harbor is not conditioned on its monitoring its service or affirmatively seeking facts regarding infringing activity) understandably led the courts astray.

For a fuller discussion of other aspects of the statute, please see our First Round Comments and Additional Comments to the Copyright Office in response to its NOIs in connection with its section 512 study,[33] as well as our testimony at the Copyright Office's roundtables.[34]

---

[32] 512 Report, *supra* note 4, at 65.

[33] *See generally* Authors Guild, Inc., Comments Submitted in Response to the U.S. Copyright Office's Dec. 28, 2015 Notice of Inquiry on Section 512 Study (April 7, 2016), *available at* https://www.regulations.gov/document?D=COLC-2015-0013-90422; Authors Guild, Inc., Additional Comments Submitted in Response to the U.S. Copyright Office's Nov. 8, 2016 Notice of Inquiry on Section 512 Study (Feb. 23, 2017), *available at* https://www.regulations.gov/document?D=COLC-2015-0013-92463.

[34] Section 512 Study Roundtable, Tr. at 188-92, 254-56 (May 2, 2016), https://www.copyright.gov/policy/section512/public-roundtable/transcript_05-02-2016.pdf ; Section 512 Study Roundtable, Tr. at 110-14, 147-49 (May 3, 2016), https://www.copyright.gov/policy/section512/public-roundtable/transcript_05-03-2016.pdf ; Section 512 Study Roundtable, Tr. at 118-19, 145, 178-82, 192-93, 402-06. (Apr. 8, 2019), https://www.copyright.gov/policy/section512/public-roundtable/transcript_04-08-2019.pdf.

A. Conflation of Knowledge Standards

As the Copyright Office 512 Report demonstrates, one of the most difficult areas of the statute is the courts' interpretation of knowledge and awareness requirements in sections 512(c) and (d).

Under sections 512(c) and (d), to qualify for safe harbor protection, a service provider must make inaccessible or remove infringing content in each of *four separate* instances:

1. when it has "actual knowledge" of infringing material;
2. when it becomes "aware of facts and circumstances from which infringing activity is apparent"[35] (often referred to as "red flag" awareness);
3. when it receives a "financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and
4. when it receives a DMCA-compliant takedown notice."[36]

Yet for each of these purportedly distinct categories, courts have required *actual knowledge* of a *specific item* of infringing content at a *specific online location* (e.g., a URL). Under the courts' analysis, the only way an ISP would have such knowledge, as a practical matter, would be by receiving a compliant takedown notice.[37]

In a seminal case on this issue, *Viacom v. YouTube*, the district court held that both the "actual knowledge" and "awareness" of infringement standards required "knowledge of specific and identifiable infringements" to disqualify a service provider from the safe harbor.[38] The Second Circuit affirmed, explaining that the ISP must know specifically where the infringing item is in order to take it down, pointing to section 512's requirement that a service provider is

---

[35] 17 U.S.C.A. § 512 (c)(1)(A).
[36] 17 U.S.C.A. § 512 (c)(1)(B).
[37] *See, e.g.*, *Viacom Int'l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514, 523 (S.D.N.Y. 2010), aff'd in part, vacated in part, reversed in part, 676 F.3d 19 (2d Cir. 2012); *UMG Recordings, Inc. v. Veoh Networks Inc*., 665 F. Supp. 2d 1099 (C.D. Cal. 2009), aff'd on other grounds sub nom *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006 (9th Cir. 2013); *see also* our discussion of these cases in our First Round Comments, *supra* note 38, at 18-22.
[38] *Viacom v. YouTube*, 718 F. Supp. 2d 514, 523 (S.D.N.Y. 2010), *aff'd in part, vacated in part, reversed in part,* 676 F.3d 19 (2d Cir. 2012).

obliged to act expeditiously to remove the infringing material,[39] and reasoning that "expeditious removal is possible only if the service provider knows with particularity which items to remove."[40] Going far beyond the actual language in subsections 512(c)(1)(A)–(B) or (d)(1)–(2), the appeals court concluded that both the actual and awareness standards must mean location- and item-specific knowledge. It similarly concluded that sections 512(c)(1)(B) and 512(d)(2)—what we refer to as the vicarious liability prong, because it is identical to the common law vicarious liability standard)—must also require location-specific knowledge.[41] In each case, the ISP must also know that the content is infringing—not just that it is at a particular location. This happens to be the kind of knowledge that an ISP can only receive from a DMCA-compliant takedown notice.

Following in *Viacom*'s footsteps, the Ninth Circuit in *Veoh* similarly reasoned that "[r]equiring specific knowledge of particular infringing activity makes good sense…[because] [c]opyright holders know precisely what materials they own, and are thus better able to efficiently identify infringing copies than service providers."[42] While such reasoning might seem sensible at first blush, it ignores what Congress expressly provided in the statute, and as a practical matter it places an enormous and even impossible burden on rightsholders, particularly individual creators, who cannot afford to spend their days searching the internet for infringing copies and cannot afford to purchase services to do it for them. The service providers that enable and often profit from providing access to pirated works—and whose businesses are built around the very algorithms capable of identifying infringing works—would appear to be better positioned to identify infringements, particularly after they have been put on notice of the existence of infringing copies of a particular work.

The courts in these cases and their progeny emphasized that the question is not what a reasonable person would have deduced given all the circumstances, but whether the service provider deliberately proceeded in the face of blatant factors of which it was aware, and, as the legislative history has it, "turned a blind eye to 'red flags' of obvious infringement."[43] The standard might seem sound in theory, but they applied it to mean something that is identical in its

[39] *See* 17 U.S.C.A. § 512(c)(i)(A)(iii).
[40] *See Viacom v. YouTube*, 676 F.3d at 30 (2d Cir. 2012).
[41] *See id.*
[42] *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1021-22 (9th Cir. 2013).
[43] H.R. Rep. No. 105-551, pt. 2, at 42 (1998).

practical effect to a heightened actual knowledge standard.

In *Viacom*, for example, even where YouTube's own estimates during the discovery phase of the trial put the percentage of infringing copyrighted material on the service at 75–80%, where YouTube was aware that "significant quantities of material on the YouTube website were infringing," and where emails among the executives showed that they knew of specific instances of infringement and even debated how long to leave them up, the Second Circuit concluded that there was insufficient evidence of actual knowledge or red flag awareness to create a triable issue of fact.[44]

Why so high a standard, and why the logical somersaults to essentially negate the clear, separate requirements in the statute, when fundamental canons of statutory interpretation tell us we should presume that separate provisions in the same law mean different things?

It boils down to the understandable reluctance of courts to burden ISPs with the responsibility of locating and identifying infringing material on their services when a separate provision (subsection 512(m)) provides that ISPs have no duty to monitor their services to be eligible for the safe harbors.[45] So, even though the legislative history makes it crystal clear that red flag "awareness" requires *fact-seeking action*,[46] subsection 512(m)'s provision that there is no duty to "affirmatively [seek] facts"[47] suggests that is not the case. Further, courts questioned how an ISP would know if a particular copy is infringing if they stumble upon it.[48]

The *Veoh* and *Viacom* courts' conclusions that both actual knowledge and the red flag "awareness of circumstances or facts" standards must mean location-specific knowledge of each instance of infringement derives from an unwillingness to require the service providers to conduct any type of monitoring, searching for, or identifying content. Section 512(m)(1) states

---

[44] *Viacom v. YouTube*, 676 F.3d, at 30 (2d Cir. 2012).
[45] 17 U.S.C.A. § 512(m)(1).
[46] H.R. Rep. No. 105-551, pt. 2, at 53 ("[I]f the service provider becomes aware of a red flag from which infringing activity is apparent, *it will lose the limitation of liability if it takes no action*.") (emphasis added).
[47] 17 U.S.C.A. § 512(m)(1).
[48] *See Capitol Records, Inc. v. MP3tunes, LLC*, 48 F. Supp. 3d 703, 716 (S.D.N.Y. 2014), *aff'd in part, rev'd in part and remanded sub nom., EMI Christian Music Grp., Inc. v. MP3tunes, LLC*, 840 F.3d 69 (2d Cir. 2016), *withdrawn from bound volume, and aff'd in part, rev'd in part and remanded sub nom., EMI Christian Music Grp., Inc. v. MP3tunes, LLC*, 844 F.3d 79 (2d Cir. 2016); *UMG Recordings, Inc. v. Shelter Capital Partners LLC* 718 F.3d at 1023 (9th Cir. 2013).

that service providers should not be required to monitor their services or seek "facts indicating infringing activity, except to the extent consistent with standard technical measures."[49] Despite subsection 512(m) being titled "Protection of Privacy," the courts interpreted subsection 512(m) to mean that ISPs need never do anything to locate infringing activity on their services—meaning as a practical matter that they can and indeed even should "turn a blind eye" to infringement to remain shielded from liability. This is the inverse of what Congress intended, namely that when an ISP knows or should know about infringement on its service, it should act to take that infringement down, which may include doing a little looking. Instead, the courts ignored the legislative history, which clarifies that "[o]nce one becomes aware of such information…one may have an obligation to check further."[50] A service provider "must take down or disable access to infringing material residing on its system or network in cases where it has actual knowledge or that the criteria for the 'red flag' test are met—even if the copyright owner or its agent does not notify it of a claimed infringement."[51]

As a result, rightsholders are left with nothing but a takedown statute that is expensive for service providers and copyright owners alike to administer and which does extremely little to prevent rampant and growing piracy. Where the intent of section 512 was to create cooperation and balance, the Second and Ninth Circuits' decisions focused on only one side of the scale—protecting burgeoning internet services from liability and stripping any responsibility other than complying with takedown notices.

Far from encouraging cooperation, section 512 has been read to discourage service providers from monitoring their services for user-posted infringing content, because that knowledge could lead to liability.[52] This has created a perverse incentive for ISPs to adopt the type of "willful blindness" that Congress sought to prevent with section 512 and to steer clear of infringement-prevention technologies, such as filtering services, that might give rise to knowledge of specific acts of infringement.

The decisions also conflict with Congress's expressed intention that under the red flag

[49] 17 U.S.C.A. § 512(m)(1).
[50] H.R. Rep. No. 105-551 (part I),) at 26 (1998).
[51] H.R. Rep. No. 105-551 (part II),) at 54 (1998).
[52] *See* 17 U.S.C. § 512(c)(1)(A).

awareness standard, "[o]nce one becomes aware of such information…one may have an obligation to check further."[53] Basic rules of statutory interpretation, as well as the legislative history, make clear that a service's takedown obligation does not depend only on receiving a DMCA-compliant notice (or all of the information that should be contained in such a notice): "Section 512 does not require use of the notice and takedown procedure. A service provider wishing to benefit from the limitation on liability under subsection (c) must 'take down' or disable access to infringing material residing on its system or network of which it has actual knowledge or that meets the 'red flag' test, even if the copyright owner or its agent does not notify it of a claimed copyright infringement."[54]

In sum, the way that courts have interpreted the statute leaves rightsholders in the cold, especially individual creators, who lack the ability to strike deals with service providers and are unable to afford takedown services. All the while, it has allowed the major internet platforms to become some of the richest companies in the world by offering up others' content for free. We need to rethink this schema and ask, in 2020, who is better able to bear the burden of identifying infringing content on internet services?

As a general rule, internet platforms have the tools and are eminently capable of finding material on the services they administer. Certainly, it is easier for the service provider to search its own platform than it is for the copyright owner; today, fingerprinting and filtering software enable service providers to automate the identification of infringing copies. Moreover, ISPs can readily obtain the information to determine if a particular content is infringing. Most infringing content contains clear indicia of its infringing nature. But just as an ISP is better positioned to police its platform, the rightsholder is better positioned to identify those indicia; and an amended section 512 could provide a mechanism for them to do so.

Moreover, there are already ways for rightsholders—other than through DMCA takedown notices—to provide ISPs with information that will allow them to identify infringing content. This happens routinely on many services. Amazon, as we mentioned, fingerprints every ebook, and if it is uploaded by anyone other than the original provider of the ebook, it may not

[53] H.R. Rep. No. 105-551 (Part I), at 26 (1998).
[54] S. Rep. No. 105-190 at 45; H.R. Rep No. 105-551 (part I) at 54 (1998).

be posted.

Subsection 512(i) contemplated the development of such "standard technical measures" and required that ISPs not interfere with them.[55] This might have been helpful except that the section defines "standard technical measures" to require that there be broad consensus through a multi-industry process.[56] With the case law so staunchly in their favor, ISPs have no incentive to participate in processes or concede the need for standard technical measures.

A literal reading of the statute, on the other hand, tells us that Congress intended ISPs to take responsibility and remove infringing content if they have "actual knowledge"—under the common law understanding—that there is infringing material or activity on their service, or if they are not aware of facts or circumstances that makes the infringing activity apparent to a reasonable person. If the operators of a service know or are aware that the service is replete with infringing content, that should satisfy the "awareness" requirement, whether or not the operators of the service know the location of each infringing item. This is just common sense.

Neither actual knowledge nor awareness under section 512 means that the ISP is automatically liable; it simply means that the ISP must act. That was the bargain Congress struck in the DMCA. If an ISP knows or is aware that it hosts or links to infringing content, it has to take additional measures to control the piracy—it must cooperate.

How This Can Be Fixed

So, what can be done to fix this morass?

An amended section 512 would contain incentives for rightsholders to provide information about the indicia—or red flags—of infringement, as well as incentives for ISPs to identify and remove readily identifiable infringing material, and not to turn a blind eye. For instance, if publishers and authors were to provide platforms with a list of ebook sellers that are authorized and notice that ebooks from any other sellers are not, the ISP should be required to remove all books sold by unauthorized sellers—without item- and location-specific notice.

A few specific suggestions are:

1. Delete subsection 512(m)(1). Alternatively, subsection 512(m)(1) could be

[55] *See* 17 U.S.C.A. § 512(i)(1)(B).
[56] *See* 17 U.S.C.A. § 512(i)(2).

amended to apply only to ISPs that have received fewer than a fixed number of takedown notices in a fixed period of time (e.g., fewer than 100 or 1,000 over the course of a year). Once an ISP is on notice that there is a significant amount of infringing activity on its service, the burden switches to the ISP to take measures to remove infringing content from its service.

2. Congress should clarify that the knowledge and awareness provisions refer to the common law (and common sense) meanings of "actual knowledge" and "awareness," including general awareness. This could be done by expressly stating such in the legislative history and by amending sections 512(c)(1)(A)(ii) and 512(d)(1)(B) to clarify that an ISP is not eligible for the safe harbor if it has "a general awareness that there is pervasive infringing material on the system or network, whether or not it is aware of the specific location of the infringement or the specific infringing material." This is consistent with a plain reading of the statute, as noted in the Copyright Office's 512 Report, because the statute uses the definite article when describing actual knowledge but not when describing red flag knowledge, leading a group of copyright scholars to conclude that "[i]n Congress's view, the critical distinction between the two knowledge standards was this: actual knowledge turns on specifics, while red flag knowledge turns on generalities."[57]

3. Specifically, Congress could add a clarification to sections 512(c)(1)(A)(i) and (d)(1)(A) that "actual knowledge" of infringing activity on one's site does not require knowing the precise location.

4. Further, sections 512(c)(1)(A)(ii) and (d)(1)(B) should be amended to create a presumption of red flag awareness when an ISP knows its service is hosting or linking to a significant amount of infringing content. For instance, red flag awareness should be presumed if the service provider has received over a fixed number of takedown notices within a month or year. This could be the same amount as in the proposed section 512(m) limits above, or it could be different. Such awareness would not mean the ISP is automatically liable, but would trigger the obligation to take steps, such as filtering, to eliminate infringing content or links to it. The statute could also expressly

[57] 512 Report, *supra* note 4, at 118 (quoting Copyright Law Scholars Initial Comments at 3–5).

require ISPs that receive over the fixed number of notices and that have revenue of over, say, $10,000,000 per year to implement filtering, fingerprinting, and other "standard technical measures" (as redefined per the recommendation below) to screen out full-length, identical infringing copies. It is only fair that these ISPs that profit from infringement at the expense of copyright owners should bear the cost of weeding it out. A natural reading of the statute bears out that this is what Congress intended.

5. Further, sections 512(c)(1)(A)(ii) and (d)(1)(B) could be amended to add that the awareness is presumed if the rightsholder has provided the ISP with sufficiently detailed and clear indicia of infringing copies of their works so that the ISP can readily identify the infringement and remove or disable access to it. That would foster real cooperation—with all rightsholders, including individual creators. As the Copyright Office states in its 512 Report, "any method going forward to effectively address this issue depends on accurate and precise data shared through these cooperative channels."[58]

6. We also endorse the 512 Report's suggestion that Congress may want to direct courts to consider additional factors when determining whether as ISP qualifies for one of the safe harbors, such as an evaluation of intent and of the severity and frequency with which it ignored red flag awareness, because "a personal blog to which users occasionally paste the contents of a newspaper article in the comment section is not, and should not be treated, the same as a website whose business model is premised on distributing primarily infringing content."[59] Similarly, we agree with the Copyright Office that "a reasonableness standard that accounts for each ISP's relevant characteristics would be appropriate for right-sizing section 512, and necessary to continue section 512's promotion of a diverse internet ecosystem."[60]

7. The definition of "standard technical measures" in section 512(i)(1)(B) should be

[58] 512 Report, *supra* note 4, at 83.
[59] 512 Report, *supra* note 4, at 112, n. 593.
[60] Id. at 124.

amended to delete the requirement for a formal multi-industry standards process as explained above. In over 20 years, no standards process has yet been put in motion and there is no incentive for ISPs to participate in one. "Standard technical measures" could instead be defined to include all effective, contemporary standard technical measures that are generally accepted in the pertinent industry (i.e., that are commonly used and readily available), regardless of whether they are developed from a multi-industry standards-setting process.

B. Vicarious Liability Standard in Section 512

Sections 512(c)(1)(B) and 512(d)(2) were meant to impose a takedown obligation on ISPs that falls within the common law vicarious liability standard for secondary copyright liability. The language in these provisions is identical to the common law standard: An ISP is disqualified from the safe harbors if it receives a financial benefit from infringing activity, and has the right and ability to supervise or control that infringing activity,[61] and then fails to act expeditiously to remove or disable access to it.[62] Rules of statutory construction—and common sense—tell us that when there is an established legal meaning of a term or phrase, that is what Congress intended unless it otherwise defined the term or phrase in the same statute.

Nevertheless, some courts have interpreted 512(c)(1)(B)'s "ability to control" prong as requiring "something more" than having the ability to disable access to or remove infringing material, or discontinue service to an infringer, despite the fact that it is the usual understanding under the common law vicarious liability standard,[63] and despite the fact that it is precisely by blocking infringing content, taking it down, or discontinuing service to the infringer, that an ISP asserts control over online infringement—just as in traditional cases of vicarious liability that

[61] 17 U.S.C.A. § 512(c)(1)(B).
[62] 17 U.S.C.A. § 512(c)(1)(B).
[63] See, e.g., *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1026–31 (9th Cir. 2013) ("until [a service provider] becomes aware of specific unauthorized material, it cannot exercise its 'power of authority' over the specific infringing item."); *Viacom Int'l, Inc. v. YouTube, Inc*., 676 F.3d 19, 37–38 (2d Cir. 2012) (what must be shown is "something more than the ability to remove or block access to materials posted on a service provider's website."); *Capitol Records, LLC v. Vimeo, LLC*, 972 F. Supp. 2d 500, 530-35 (S.D.N.Y. 2013) (Vimeo lacked the "something more" where Vimeo employees responded to user questions by ignoring copyright infringement or posted infringing videos themselves.); CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004).

found that the owners of a music hall and swap meet had the ability to control infringing activities on their premises, and financially benefited from them.[64]

While the Second Circuit in *Viacom Int'l, Inc. v. YouTube, Inc.*[65] stated that section 512(c)(1)(B) requires "something more" than the ability to remove or block access to materials posted on an ISP's platform, it also admitted that "[t]he remaining—and more difficult—question is how to define the 'something more' that is required," advising only that the "something more" must exert "substantial influence" on the activities of the users.[66] In other words, no one has actually defined what "something more" might mean.

How did the courts come up with this nonsensical notion of what the standard meant? Courts reasoned that ISPs were obliged to take content down under the various provisions of section 512 and must have and implement repeat-infringer policies under section 512(i) that would eventually require disabling accounts. How could the ability to take down and disable infringement take an ISP out of section 512 then?

Another reason courts have taken this strained approach to the vicarious liability standard in section 512 is a perceived conflict with the general condition in 512(i) for service providers to implement a repeat-infringer policy, in addition to the requirements to take infringing material down once an ISP has actual knowledge or red flag awareness, or the vicarious liability standard applies under 512(c) and (d). Courts have found this hard to reconcile. In *Hendrickson v. eBay*, for example, the district court for the Central District of California reasoned that "Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA."[67] Because otherwise, they argued, section 512(c)(1)(B) would disqualify any service provider that in fact has the ability to do exactly what section 512(c) of the DMCA requires service providers to do in order to benefit from the safe harbors: to disable access to or remove material in response to notice, knowledge, or awareness of infringing activity.

But this overlooks the plain language of the provision—that if the ISP receives a financial

---

[64] *See id. See Shapiro, Bernstein & Co. v. H.L. Green Co.*, 316 F.2d 304, 307 (2d Cir. 1963); *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F. 3d 259 (9th Cir. 1996).
[65] 676 F.3d 19 (2d Cir. 2012).
[66] *Id*. at 36.
[67] *Hendrickson v. eBay, Inc.*, 165 F. Supp. 2d 1082, 1095 (C.D. Cal 2001).

benefit from infringing activity and it can control that activity, then it is ineligible. Since it is true that the requirement for the ISP to have the right and ability to take content down is duplicative, sections 512(c)(1)(B) and 512(d)(2) may as well simply read that an ISP is disqualified if it "does not receive a financial benefit directly attributable to the infringing activity," period. The problem with this interpretation is that it assumes that the statue was intended to protect user-generated-content services that are replete with infringing content. But the opposite is the case. What Congress must have intended—and remember that in 1996–98 when this legislation was being drafted, infringement was a one-off ordeal and nothing like the mass copying we've grown accustomed to since Napster—is just what the statute says: if an ISP is benefiting financially from the infringing activity and it has the ability and right to remove it, prevent access to it, etc., then it must take it down.

The Copyright Office concurs with this approach in its recent 512 Report, writing that "the Office is of the opinion that the right and ability prong should correctly be interpreted in accordance with the common law standard."[68] It further states that "a more appropriate test for financial benefit is to ask whether the existence of infringing material on the site is one of the primary draws for users, or whether the plaintiff's works were infringed by being performed or distributed through the site."[69] The Authors Guild would also echo that concern.

How This Can Be Fixed

Congress needs to address the lack of clarity surrounding the meaning of the "financial benefit" and "right and ability to control" standards under the section 512 safe harbors. Specifically, we believe that Congress should clarify that an ISP has the "right and ability to control" when (i) infringing material resides on its system, and (ii) the ISP retains the right and has the ability to remove or disable access to the infringing content. This could be done by adding at the end of the provision language such as, "including to prevent users of the system from posting or accessing the infringing material." The financial benefit prong should also be restored to its common law meaning.

Another qualification could be added to this provision so that it does not automatically disqualify all ISPs that are vicariously liable: the qualifier in subsections 512(c)(1)(A)(3) and

[68] 512 Report, *supra* note 4, at 135.
[69] 512 Report, *supra* note 4, at 134.

512(d)(1)(C) could be made to apply also to this vicarious liability standard in sections 512(c)(1)(B) and 512(d)(2). In other words, if an ISP met this vicarious liability standard, then, to be eligible for the safe harbor, it would have to remove or disable the infringing content. The duty could be triggered by the ISP's general knowledge of infringement on its service that it benefited from or from knowledge of a specific item. In the case of the former and more common scenario, it would likely mean employing technical measures to take infringing activity off its service.

Further, it should be clarified that "a financial benefit directly attributable to the infringing activity" does not mean that the ISP receives money for the content, nor does it even mean that ads were placed against that particular infringing content. That is not how most ISPs work. The real measure of value for internet companies is the number of clicks or eyeballs derived from the content which increases the ISPs' user base and in turn allows ISPs to extract greater advertising income.

C. The Required Elements of Notification

Section 512(c)(3) of the statute lists the requirements for a takedown notice. By its own terms, it does *not* require the identification of each infringing item, much less the location for each. Rather, subsection 512(c)(3)(A)(ii) allows the copyright owner to provide just a "representative list" of infringing copies of their works on the service.[70] Moreover, subsection 512(c)(3)(A)(iii) provides that the notice only need include "information reasonably sufficient to permit the service provider to locate the material"—not the URL for each infringing copy.[71]

The representative list language was intended as a safety valve to ease the burden on individuals and other rightsholders of having to track down and list the specific URL of each infringing copy on a platform containing multiple infringing works.[72] Moreover, the Senate Report makes clear that compliance with the DMCA takedown notice requirements should not be judged rigidly—that the standard to be applied is "one of substantial compliance."[73]

The language used in the Senate Report ("it is not necessary for a compliant notification

[70] 17 U.S.C.A. § 512(c)(3)(A)(ii).
[71] 17 U.S.C.A. § 512(c)(3)(A)(iii).
[72] *See* S. Rep. No. 105-190, at 46.
[73] *Id.*

to list every musical composition or sound recording that has been or could be infringed at that site"[74]) also underscores that Congress, even in the late 1990s, recognized the impracticality of requiring rightsholders to provide a complete list detailing every infringing copy of every work on platforms replete with infringement.

But courts have tended to ignore the representative list language and its purpose, insisting that ISPs need only take down content that is specifically identified by location, which requires listing out each work, assuming they are posted at different URLs, contrary to section 512(c)(3)(A)(ii). In *Perfect 10, Inc. v. CCBill LLC*, for example, the Ninth Circuit held that the burden of "identifying the potentially infringing material and adequately documenting infringement [falls] squarely on the owners of the copyright,"[75] a concept which has been followed in other decisions in the Ninth and Second circuits.[76]

To the contrary, the legislative history confirms that Congress recognized it would often be futile for rightsholders to provide an exhaustive list identifying every copyrighted work and every act of infringement, especially in cases involving massive infringement:

> Where multiple works at a single on-line site are covered by a single notification, a representative list of such works at that site should be sufficient. Thus, for example, where a party is operating an unauthorized Internet jukebox from a particular site, it is not necessary that the notification list every musical composition or sound recording that has been, may have been, or could be infringed at that site. Instead, it is sufficient for the copyright owner to provide the service provider with a representative list of those compositions or recordings in order that the service provider can understand the nature and scope of the infringement being claimed.[77]

The Fourth Circuit took a somewhat different, and arguably more balanced, approach

---

[74] *Id.*
[75] *Perfect 10, Inc. v. CCBill LLC*, 448 F.3d 1102, 1113 (9th Cir. 2007).
[76] See, e.g., Arista Records, Inc. v. MP3Board, Inc., No. 00 CIV. 4660, 2002 WL 1997918, at *15 (S.D.N.Y. Aug. 29, 2002) ("a bare list of musical artists whose songs were allegedly linked to did not constitute a representative list of works, or notice equivalent to a list of representative works that can be easily identified by the service provider.").
[77] H.R. Rep. No. 105-551 (Part II), at 55; S. Rep. No. 105-90, at 46.

than the Ninth Circuit in *ALS Scan v. RemarQ Communities*. It reversed a lower court's holding that a DMCA notice was deficient because it didn't identify every infringing work. The court clarified that the DMCA does not "seek to burden rightsholders with the responsibility of identifying every infringing work—or even most of them—when multiple works are involved. Instead, the requirements are written so as to reduce the burden on holders of multiple copyrights who face extensive infringements of their works."[78] It's worth noting that, as the Copyright Office points out in the 512 Report, this is only one of two cases not overturned on appeal where a court found the plaintiff's representative list to be sufficient.[79]

How This Can Be Fixed

The law should clarify what constitutes a "representative list" of "multiple copyrighted works at a single online site." A "representative list" could be defined and clarifying language could be added to the effect that "the copyright owner need not list every work that is infringed, nor its location." In addition, section 512(c)(3)(A)(iii) could be qualified to explain that the "information reasonably sufficient to permit the service provider to locate the material" in a takedown notice will depend on the circumstances and does not generally require notice of the URL of the infringing content, which, in many cases, the ISP is far better positioned to identify.

III. Conclusion

The courts' overbroad application of the safe harbors (and narrow application of the disqualifiers) has caused real, palpable damage to our creative sectors. The whack-a-mole system that the courts left us with is absurd and unworkable, particularly from the individual creators' perspective. A rightsholder should not have to send a takedown notice every single time an infringing copy appears at a new URL. After the first time, the ISP has been put on notice. It knows what to look for and it knows who the rightsholder is. If in certain circumstances it needs more information to identify recurring infringement, the rightsholder should provide it.

The fixes we have recommended in this statement would revert section 512 to what Congress intended: to encourage ISPs and rightsholders to take down and *keep* infringing content off their services. This is not a new idea. The statute that Congress enacted in 1998 was a

[78] *ALS Scan, Inc., v. RemarQ Communities, Inc.*, 239 F.3d 619, 625 (4th Cir. 2001).
[79] 512 Report, *supra* note 4, at 142.

staydown statute, not a whack-a-mole one. If clarified in the ways suggested in this statement, section 512 will operate as originally intended—as a "takedown and staydown" statute.

An alternative approach would be an express takedown and staydown regime. Rather than (or in addition to) the clarifications described in this statement, Congress could enact a new provision that provides that a takedown notice applies to every full-length, identical copy of the particular work. In other words, one notice does not result in one takedown, but in the removal of all current and infringing copies of that work.

Technology and practices have changed dramatically since the DMCA was adopted in 1998. We love our technology, and the internet sector has brought enormous value to the book industry, and indeed to our nation. But ISPs should not be allowed to profit from infringing content without any penalties or disincentives. The largest ISPs have gotten extraordinarily rich in recent years because they provide access to vast quantities of copyrighted content for free. The access they provide has transformed our world: information about almost anything is at our fingertips. It is nothing short of extraordinary. But the way that many courts have interpreted section 512 has allowed those for-profit companies to grow and prosper to an obscene measure and to drain wealth out of the creative community, leaving individual creators poorer than ever. We are a nation built on the inspiration and creative work of individual creators. That's why we need legislative reform to section 512.

On behalf of the almost 10,000 members of the Authors Guild, I thank you for your attention to this matter. The Authors Guild is available for further consultation.