Before the

Federal Trade Commission

Request for Public Comment Regarding Reducing Anti-Competitive Regulatory Barriers

Docket No. FTC-2025-0028

Comments of Authors Alliance and Electronic Frontier Foundation

May 27, 2025

Submitted by:

David Hansen
Authors Alliance
2108 N ST # 8898
Sacramento, CA 95816
Telephone: (510) 480-8302
dave@authorsalliance.org

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

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis and advocacy, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

Authors Alliance is a nonprofit organization founded in 2014 to advance the interests of authors who want to serve the public good by sharing their creations broadly. We host educational resources to help creators understand and enjoy their rights and promote policies that make knowledge and culture available and discoverable. We also advocate on our members' behalf before Congress, the courts, and other government entities.

Authors Alliance and EFF submit these comments to call the FTC's attention to an overlooked but highly influential set of anti-competitive regulations: the rules the Library of Congress issues every three years pursuant to Section 1201 of the Digital Millennium Copyright Act. While often well-intentioned, these rules, and the process by which they are adopted, undermine the fundamental purpose of copyright laws as envisioned by the Constitution: to promote the progress of science and the useful arts.

Copyright grants exclusive rights to creators, but only as a means to serve the broader public interest. Fair use plays a critical role in maintaining the balance—ensuring that the public can engage in commentary, research, education, innovation, and repair without unjustified restriction. As explained below, Section 1201 effectively forbids fair uses where those uses require circumventing a software lock (a.k.a. technological protection measures) on a copyrighted work.

Congress realized that Section 1201 had this effect, so it adopted a safety valve—a triennial process by which the Library of Congress could grant exemptions. Under the current rulemaking framework, however, this intended safety valve functions more like a chokepoint. Individuals and organizations seeking an exemption to engage in lawful fair use must navigate a burdensome, time-consuming administrative maze. The existing procedural and regulatory barriers ensure that the rulemaking process—and Section 1201 itself—thwarts, rather than serves, the public interest.

The FTC does not, of course, control Congress or the Library of Congress. But we hope its investigation and any resulting report on anti-competitive regulations will recognize the negative effects of Section 1201 and that the triennial rulemaking process has failed to be the safety valve Congress intended. Indeed, we urge the FTC to recommend that Congress repeal or reform Section 1201. At a minimum, the FTC should advocate for fundamental revisions to the Library of Congress's next triennial rulemaking process, set for 2026, so that copyright law can once again fulfill its purpose: to support—rather than thwart—competitive and independent innovation.

Section 1201 Gives Some Rightsholders a Default Veto Right on Competitive Innovation

Before Section 1201 was adopted, it was a long-standing American tradition and copyright principle that once a consumer purchased a product, she was free to use, modify, or customize it as she saw fit. Consumers who lawfully acquired their electronic goods were free to customize their products to better fit their needs; just as car enthusiasts might wish to modify or enhance their engines, consumers may wish to write their own software for their robot pet, install a larger hard drive on their computer, etc. Consumers have traditionally been free to choose competitive add-on or alternative technologies that interoperated with the goods they bought, and innovators

were able to develop and distribute such technologies that promoted competition in the market.

With the help of Section 1201, manufacturers can now easily shut down consumer-driven competition and innovation simply by embedding copyrighted software or technological protection measures (TPMs) in their products.

Section 1201 was ostensibly intended to stop copyright infringers from bypassing anti-piracy technological protections by creating a legal backstop for TPMs[1]—the software that restricts how people interact with content like music, movies, and ebooks. But as software has become embedded in everything from tractors[2] to light bulbs to kitty litter boxes, the prohibition has become best known for its unintended consequences.[3] Instead of a tool for fighting piracy, Section 1201 has become a weapon that rightsholders can wield against the American traditions of tinkering, repair, and innovation—undermining our freedom to make use of our own property while stifling technological progress for the entire country.

The case of DVDs will serve to illustrate the anti-competitive and innovation-stifling effect of Section 1201. The encryption on DVDs was broken almost immediately, and subsequent versions were quickly bypassed as well. Yet movie studios continued to use encryption on every commercial DVD release, because the movie studios (acting through their agent, DVD-CCA) could use that encryption as a gatekeeping tool—requiring innovators to sign restrictive licensing agreements before they could build any software capable of decrypting a DVD.

This gave the movie studios unprecedented power to influence the pace and nature of innovation in the world of DVDs. Any new feature—like copying to a hard drive—had to pass muster in a 3-way "inter-industry" negotiation: movie studios, incumbent consumer electronic companies, and big computer companies must all agree before innovation or "competition" happened. In other words, a new market entrant had to get permission from their adversaries and competitors before the newcomer could innovate.

The result: DVD technologies changed very little from 1995 to 2025.

DVDs are far from the only example of rightsholders using TPMs to block competition rather than prevent piracy. Most modern products contain some element of copyrightable software

[1] For an explanation on DRM, see https://www.eff.org/issues/drm
[2] Farmers are locked out of their own tractors: https://reason.com/2024/01/08/how-john-deere-hijacked-copyright-law-to-keep-you-from-tinkering-with-your-tractor/
[3] For a discussion of the negative consequences, see https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca

code.[4] In order for replacement parts and compatible accessories to function, the parts must "access" the computer code inside the product. If unauthorized access involves circumvention of a TPM and is therefore prohibited, the manufacturer can easily leverage Section 1201 to assert exclusive control over the market for those goods and accessories.

The detrimental effects on the market are well documented. For instance, cell phone manufacturers sell phones with TPMs that lock consumers to a particular service provider, forcing them to pay artificially inflated service charges and crippling the market for used phones.[5] Until Congress specifically intervened,[6] consumers had little legal choice than to do what the TPMs demanded.

Unfortunately, the narrow intervention for cell phones did little to protect consumers using other types of devices. For example, some camera manufacturers have embedded TPMs that make image files unreadable by competing photo-editing programs. This prevents consumers from editing their own photos with the software of their choice and artificially suppresses competition in the photo-editing market—not by offering a better product, but by locking rivals out through legal barriers.[7]

Even beyond the usual domain of copyright, companies have used the DMCA Section 1201 to block aftermarket competition in laser printer toner cartridges, garage door openers, video game console accessories, and computer maintenance services, just to name a few. Though ostensibly a copyright law, Section 1201 can easily be leveraged by market incumbents to regulate competition for uncopyrightable products, because the cost, complexity, and uncertainty of legal battles create a powerful deterrent for newcomers. Innovators and competitors may avoid entering the market altogether, fearing expensive litigation. This "chilling effect" limits competition before it can even begin. Worse still, it is unclear if Section 1201 lawsuits can always be defeated if rightsholders sufficiently merge TPM-restricted copyrightable software into their products.

Lexmark, the second-largest laser printer maker in the U.S., wanted to use Section 1201 to eliminate the secondary market for refilled laser toner cartridges. Lexmark had added

---

[4] *See*, e.g., David Chartier, *Microsoft's New Vision: A Computer in Every ... Coffee Maker?,* Ars Technica, Jan. 12, 2009, http://arstechnica.com/microsoft/ news/2009/01/microsofts-new-vision-a-computer-in-every-coffee-maker.ar.

[5] David Kravitz, *Apple v. EFF: The iPhone Jailbreaking Showdown*, Wired, May 2, 2009, http://www.wired.com/threatlevel/2009/05/apple-v-eff-the-iphone-jailbreaking-showdown/.

[6] https://en.wikipedia.org/wiki/Unlocking_Consumer_Choice_and_Wireless_Competition_Act

[7] Declan McCullagh, *Nikon's Photo Encryption Reported Broken*, CNET, Apr. 21, 2005, http://news.cnet.com/Nikons-photo-encryption-reported-broken/2100-1030_3-5679848.html.

authentication routines between its printers and cartridges explicitly to hinder aftermarket toner vendors. Static Control Components (SCC) reverse-engineered these measures and sold "Smartek" chips that enabled refilled cartridges to work in Lexmark printers. Thanks to the anti-competitive power granted to Lexmark by Section 1201 was able to obtain an injunction banning SCC from selling its chips to cartridge remanufacturers. SCC ultimately succeeded in getting the injunction overturned on appeal, but only after 19 months of expensive litigation while its product was held off the market. The prolonged litigation alone—not dismissed at an early stage as it should have been—sent a chilling message to those in the secondary market for Lexmark cartridges.[8]

Garage door opener manufacturer Chamberlain Group also invoked Section 1201 against competitor Skylink Technologies after several major U.S. retailers dropped Chamberlain's remote openers in favor of the less expensive Skylink universal "clickers." Chamberlain claimed that Skylink had violated Section 1201 because its clickers bypassed an "authentication regime" between the Chamberlain remote opener and the mounted garage door receiver unit. Skylink ultimately defeated Chamberlain both at the district court and court of appeals, but again only after many months of expensive litigation. In the words of the court of appeals, Chamberlain's use of Section 1201 was nothing less than an "attempt to leverage its sales into aftermarket monopolies."[9]

Microsoft used Section 1201 to try to shut down competition for gaming accessories. Datel, Inc. produced third-party accessories for every major video game console, including Microsoft's Xbox 360.[10] As with all third-party manufacturers, Datel must engineer its accessories so that they would be compatible with the chosen first-party console; this frequently required reverse engineering or other work-arounds. In 2009, Microsoft issued a mandatory firmware update for all Xbox 360 consoles connected to the Internet: this update had no effect on Microsoft's own memory cards, but rendered Datel's less-expensive memory cards completely unusable. When Datel sued Microsoft for antitrust violations, Microsoft counterclaimed by accusing Datel of violating Section 1201. In a nutshell, Microsoft forced consumers to purchase its own memory cards and then used the DMCA to attack legitimate competitors.

---

[8] Declan McCullagh, *Lexmark Invokes DMCA in Toner Suit*, CNET News (Jan. 8, 2003), http://news.com.com/2100-1023-979791.html; Lexmark v. Static Control Components, 387 F.3d 522 (6th Cir. 2004).

[9] Steve Seidenberg, *Suits Test Limits of Digital Copyright Act*, NAT'L L. J. (Feb. 7, 2003), http://www.law.com/jsp/article.jsp?id=1044059435217; Chamberlain Group v. Skylink Technologies, 381 F.3d 1178 (Fed.Cir. 2004), *available at* http://scholar.google.com/scholar_case?case=16927618869037195909).

[10] Mike Masnick, *Microsoft Still Claiming That It Can Use The DMCA To Block Competing Xbox Accessories*, TechDirt, Jun. 21, 2011, http://www.techdirt.com/articles/20110620/10505614766/microsoft-still-claiming-that-it-can-use-dmca-to-block-competing-xbox-accessories.shtml.

Moreover, manufacturers of ordinary consumer products have sought to extend the DMCA to police any consumer behavior or innovation that is contrary to their preferences. For example, calculator manufacturers have brought Section 1201 claims against hobbyists who reverse-engineered their personal graphing calculators to develop alternative operating systems for personal use.[11]

And these Section 1201 legal threats re-appear with every wave of technological innovation. For example, a Czech software development company threatened a computer scientist for offering a gateway to the Interplanetary File System network—one of the decentralized web technologies that have the potential to make the internet more robust and efficient, supporting a new wave of innovation. EFF pushed back on the scientist's behalf.[12] And EFF has recently counseled independent researchers who have been threatened for doing nothing more than unlocking diagnostic codes which would make it easier for independent repair shops to survive and for owners to repair their own cars. But not everyone has access to pro bono legal services.

An Expensive Regulatory Groundhog Day — the Triennial Rulemaking Process

In theory, these anti-competitive consequences should be alleviated by the triennial rulemaking, which authorizes the Librarian of Congress (via a process conducted by the Copyright Office) to authorize exemptions for lawful secondary uses. The hope is that users can engage in lawful uses despite Section 1201's categorical ban on circumvention of TPMs. But in practice, the triennial rulemaking process is slow, complex, limited and places an undue burden on users to repeatedly justify lawful uses. Even to gain—or retain—the right to use their own devices or conduct lawful research is an uphill battle.

As Professor Blake Reid explained in testimony before the U.S. Senate, the Copyright Office's conduct of the triennial rulemaking—much of which is not required by Section 1201's delegation of authority—undermines the purpose of the rulemaking itself. Rather than receiving public comments and engaging in independent fact-finding, as many administrative agencies do, the Copyright Office has instead long laid a heavy burden on the shoulders of those wishing to make lawful uses by circumventing TPMs[13]: "[P]roponents must show by a preponderance of the

---

[11] Dan Goodin, *Texas Instruments Aims Lawyers at Calculator Hackers*, The Register, Sept. 23, 2009, http://www.theregister.co.uk/2009/09/23/texas_instruments_ calculator_hacking.

[12] Kit Walsh, Defending Access to the Decentralized Web, EFF, Feb 20, 2024, https://www.eff.org/deeplinks/2024/02/defending-access-decentralized-web.

[13] Testimony of Prof. Blake E. Reid, Are Reforms to Section 1201 Needed and Warranted?, U.S. Senate Committee on the Judiciary, Subcommittee on Intellectual Property (Sept. 16, 2020), https://www.judiciary.senate.gov/download/reid-testimony.

evidence that there has been or is likely to be a substantial adverse effect on noninfringing uses by users of copyrighted works."[14] Meeting that standard—a standard not found in the DMCA's text—generally requires extensive work from specialized copyright attorneys, technical experts, researchers, and industry analysts. Without expert assistance, individuals cannot reasonably gather the evidence and devote the time necessary to participate meaningfully in the DMCA Section 1201 triennial rulemaking process. And even if she does succeed, she must be prepared to make the case again, three years later.

Exemption proponents must wait for a window that opens just once every three years. Assuming they can wait that long, they must then hire specialized legal assistance. Developing the case for a single exemption can take more than 500 hours of legal work across a single instance of the triennial rulemaking. At the prevailing market rate, advocacy for a single exemption under the triennial rulemaking may cost an individual proponent or advocate more than $120,000 even if performed entirely by law clerks, or potentially more than $450,000 if performed by a senior attorney—a prohibitive cost for many non-profit organizations and individuals. There's no alternative for these exemption-seeking organizations or individuals though; their lawful activities are chilled by Section 1201 absent an applicable exemption.

If a proponent cannot afford counsel, they might be lucky enough to retain one of the small number of pro bono law clinics with expertise in the triennial rulemaking process. The limited capacity of clinics to provide pro bono services for the triennial rulemaking means that some would-be exemption proponents likely never have the opportunity to present their case at all. While Section 1201 permits the Office to investigate exemptions sua sponte, as an agency might typically do in the context of a notice-and-comment rulemaking, the Office has chosen not to do so for as long as the rulemaking process existed.

Even when a proponent manages to obtain legal help, a lengthy task awaits. A proponent must work with counsel to compile dozens of pages of detailed justifications across numerous filings, usually over the course of a full year if not more. In many cases, proponents must undergo intensive questioning about the legitimacy of their work and personal activities from government officials in hours-long hearings. Specifically, proponents in the 2021 rulemaking were required to prepare:

- A petition to renew an existing exemption;
- A separate petition to request expansion of an existing exemption;

[14] Recommendation of the Register of Copyrights at 10, Oct. 27. 2003, https://cdn.loc.gov/copyright/1201/docs/registers-recommendation.pdf.

- Detailed long-form comments;
- Detailed long-form reply comments;
- Hearing testimony across several weeks of hearings,

As a part of the rulemaking process, exemption proponents also must undergo opposition and questioning from professional lobbyists and corporate attorneys representing opponents who in some cases impugn the proponents' character and reflexively criticize their proposals, often without seriously reviewing or even attempting to understand the proposed exemptions.

In some cases, the Copyright Office poses additional questions or asks proponents to engage in protracted negotiations with rightsholders to develop specific regulatory language or settle substantive disputes.

As a result, the Office routinely recommends exemptions riddled with vague and ambiguous language and caveats. These limits can have dangerous as well as anti-competitive consequences. For example, security researchers had sought a Section 1201 exemption in 2003 in order to facilitate research on dangerous TPM systems like the Sony-BMG rootkit, but the Librarian of Congress denied their request.[15] In 2006, the Librarian granted an exemption to Section 1201 for researchers examining copy protection software on compact discs.[16] However, this exemption did not protect researchers studying other TPM systems. In 2009, security researchers again sought an exemption for computer security research relating to TPM systems, including the protection mechanisms used on the Electronic Arts video game, Spore, which has been the subject of class action lawsuits alleging security vulnerabilities.[17] A narrow version of this exemption was granted in 2010. However, the exemption was not renewed in 2012, leaving this field of research vulnerable to legal action.[18]

Case Study: Independent Repair

The repair community has extensive experience with the triennial rulemaking process. Today, a vast array of devices, from vehicles to televisions to refrigerators contain copyrightable software

[15] Recommendation of the Register of Copyrights in RM 2002-4, Oct. 27, 2003, 87-89, http://www.copyright.gov/1201/docs/registers-recommendation.pdf.

[16] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,477 (Nov. 27, 2006), http://www.copyright.gov/fedreg/2006/71fr68472.pdf.

[17] Comments of Prof. J. Alex Halderman, http://www.copyright.gov/1201/2008/comments/halderman-reid.pdf.

[18] See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 77 Fed. Reg. 208 (Oct. 26, 2012) (to be codified at 37 C.F.R. pt. 201), http://www.copyright.gov/fedreg/2012/77fr65260.pdf.

that is locked under TPMs so that only the original manufacturer can access and control the product. Members of the repair community have repeatedly appeared before the Office to seek exemptions necessary to diagnose, maintain, and repair vehicles, consumer devices, and medical equipment.

Opponents have offered some absurd counterarguments.[19] For example, opponents of exemptions for cars and tractors repair have claimed that giving owners the freedom to inspect and modify the software code in the vehicles they own would lead to all kinds of other illegal activity. They said people shouldn't be allowed to repair their own car because some might not do it right. They claimed people shouldn't be allowed to modify the software code in their car because some might defraud a used car purchaser by changing the car's mileage. They say no one should be allowed to even *look* at the code without the manufacturer's permission because letting the public learn how cars work could help malicious hackers, "third-party software developers," and competitors. During one rulemaking process, John Deere even argued that letting people modify car computer systems would result in them *pirating music* through the on-board entertainment system—as if users didn't have many easier ways to play music in their cars.

But the vast majority of manufacturers' concerns have nothing to do with copyright law. And, as they themselves noted, vehicles are subject to regulation by other government agencies with subject matter expertise. The Copyright Office and the Library of Congress are ill-suited to regulate vehicle repair.

From the initial petition for an exemption on vehicle repair, to the repair exemptions' later expansion to encompass consumer devices and medical equipment, to the rejection of proposals to encompass video game consoles and commercial and industrial equipment,[20] the Office has recognized that the functional nature of repair often entails lawful fair use.[21] It has further found that the other statutory factors it is required to consider favors an exemption.

Despite consistently recognizing repair as fair use, the Office has repeatedly denied or narrowed requested exemptions for repair. In 2015, for example, the Office narrowed the proposed exemption for vehicle repair by excluding circumvention of in-vehicle entertainment and telematics systems even though accessing these systems is necessary for repair because they often are inextricably linked with other vehicle systems used in remote repair diagnostics.

---

[19] See EFF's discussion on this issue: https://www.eff.org/deeplinks/2015/04/automakers-say-you-dont-really-own-your-car

[20] 2021 Recommendation at 197–98.

[21] 2015 Recommendation at 234; 2018 Recommendation at 202-05; 2021 Recommendation at 201-04.

Similarly, the Office also narrowed the exemption to exclude circumvention by independent mechanics undertaking repair on behalf of a vehicle's owner, again for reasons unrelated to fair use. In both 2018 and 2021, despite finding that the expanded proposals were likely to entail fair use, the Office declined to expand the exemption to explicitly allow for third-party assistance. Even though the Office reversed course on some of its previous repair restrictions in 2021, it substantially limited proposals for commercial and industrial equipment.

The Office's ongoing inability or unwillingness to broadly permit fair repair uses via the triennial rulemaking prevents consumers from repairing their devices independently and stifles the development of a competitive market for independent repair services.

Case Study: Jailbreaking

Another classic example of how Section 1201 and the triennial rulemaking process impede innovation and competition involves "jailbreaking." Users of smartphones, tablets and other all-purpose mobile computing devices depend on the ability to jailbreak their devices, because it allows them to add and remove software, and to enable interoperability with other software and hardware. But these mobile devices include TPMs that give smartphone manufacturers, such as Apple, the ability to decide what software they will allow on the phones they sell. Jailbreaking restores to users control over their own devices, but it requires circumventing those TPMs.

EFF led the first successful effort to demand an exemption for jailbreaking, but opponents, principally Apple, fought hard against it. Others have taken up the jailbreaking mantle, and manufacturers continue to resist efforts to expand existing exemption to match technological developments. Users and their representatives must still go hat in hand to the Copyright Office every three years to ask for existing exemptions to be renewed.

EFF has spoken to many device users who currently rely on jailbreaking for a variety of reasons.

Some examples include:

- *Alternative Operating Systems:* Many device owners use an alternate operating system for their devices, such as the operating system LineageOS. In order to install these alternate operating systems, iOS devices and many Android devices must first be jailbroken or rooted (the Android equivalent of jailbreaking). Users jailbreak their devices to control the device itself and add or remove software, often driven by their concerns about privacy, avoiding data collection by hardware and software providers, and the desire to customize the functionality of their devices. One device owner reported that they jailbreak their device to stop apps from reporting to Google when the owner installs and opens them, while another mentioned implementing security controls at the device

level to block and filter internet traffic to and from entities they don't want their traffic going to. Multiple device owners use an alternate operating system because certain features and bug fixes come sooner to alternate operating systems compared to the official one.

- *Making Older Devices Functional*: Other users rely on jailbreaking to keep their older devices functional. As devices become older, companies stop maintaining them or issue updates that can slow or degrade functionality. By jailbreaking their devices, users are able to keep their older devices secure, improve their functioning, and prevent these devices that they paid hundreds of dollars for from becoming obsolete.

- *Customization:* Device owners also greatly value jailbreaking in order to develop custom app functionality that would not be approved by the manufacturer, or where approval would be unreasonably costly for the desired use. One example of this is creating an app to interface with a home security system made by a manufacturer who had been out of business for years and would never provide an official app. Users greatly value the ability to customize their devices to their specific needs but can be prevented from doing so by access controls and the official app approval process. Additionally, many users included that they prefer using open source applications that are peer reviewed, both due to their desire to support open source technologies and because some apps that make it through the official audit process have malware. While some of these apps are available on official app stores, other open source apps are only available outside official channels for a variety of reasons, such as to avoid paying high fees to Apple and Google or because the app has not been approved for official app stores. As Apple uses access controls to restrict app distribution to its official app store, iOS users rely on jailbreaking their devices to access these apps.

These firsthand accounts of jailbreaking show how it empowers users to extend the lifespan, security, and utility of the devices they legally own, yet the legal framework treats this as suspect—forcing users and advocates to beg for temporary, narrowly drawn exemptions every three years. This only serves to benefit incumbent manufacturers at the public's expense. The FTC should recognize that Section 1201, as currently implemented, has become a powerful tool for entrenching market dominance and blocking independent innovation, far beyond its original anti-piracy intent. Jailbreaking is just one of many areas where reform is urgently needed to ensure that copyright law supports, rather than stifles, competition and user freedom.

Case Study: Text and Data Mining

The Office has also used Section 1201 to grant media cartels what amounts to an administrative

subpoena to scrutinize users' security practices. Such a right is nowhere found in the Copyright Act and substantially chills reuses of copyrighted works that are entirely lawful.

In this case, the Office created the right in the context of an exemption for academic researchers engaged in text and data mining.[22] Text and data mining has been an important research technique across a wide variety of fields, from history and literature to chemistry and biology, to assess patterns and trends across large corpora of texts—due to its transformative and noncommercial nature, a practice clearly permissible under existing fair use case law such as *Authors Guild v. Google*[23] and *Authors Guild v. HathiTrust.*[24] The fair use case of text and data mining is strong, because copyrighted works are used only for analytical and search purposes and where the underlying copies are appropriately secured from infringing downstream uses.[25]

The Office has consistently agreed that text and data mining is fair use, and approved a limited exemption for researchers to engage in this important research activity. The original petition for the text and data mining exemption was for a simple two-line exemption that allowed researchers to circumvent TPMs on any lawfully acquired literary works and motion pictures for purposes of use with text and data mining techniques.[26] Through the triennial process, that original two-line exemption morphed into a multi-page, 800-word-long set of rules with voluminous limitations on researchers.

One such limit was that researchers must employ "adequate security measures" on the corpus they create. In and of itself, this requirement was a minor inconvenience, though unnecessary—since fair use caselaw already indicated that appropriate security measures would be part of any fair use analysis. For the Office this clarity of law was not enough: in the 2021 rulemaking, the Office requires that in order for researchers to comply, they must do one of two things: 1) seek a privately negotiated agreement with rightsholders on what security practices were adequate, or 2) subject themselves to capricious auditing requests from rightsholders or their representatives to provide information about the research institution's internal security

---

[22] Authors Alliance, along with the American Association of University Professors and the Library Copyright Alliance, brought the petition. Authors Alliance et al., Petition for New Exemption under 17 U.S.C. § 1201, Sept. 8, 2020, https://www.copyright.gov/1201/2021/petitions/proposed/New%20Pet.%20-%20Authors%20Alliance%20et%20al.pdf

[23] Authors Guild v. Google, Inc., 804 F. 3d 202 (2d Cir. 2015).

[24] Authors Guild, Inc. v. HathiTrust, 755 F. 3d 87 (2d Cir. 2014).

[25] *HathiTrust,* 755 F. 3d at 100-101 ("Next, the Authors assert that the HDL creates the risk of a security breach which might impose irreparable damage on the Authors and their works. . . . This showing of the security measures taken by the Libraries is essentially unrebutted. Consequently, we see no basis in the record on which to conclude that a security breach is likely to occur, much less one that would result in the public release of the specific copyrighted works belonging to any of the plaintiffs in this case.")

[26] Authors Alliance, *supra* note 20.

practices.[27]

No part of the Copyright Act nor any relevant cases grants a copyright holder a right to issue demand letters to users of copyrighted works to investigate whether they are storing copies in a secure environment. Yet the Office concluded that it had the power to create such a right here.

The result was predictable: rightsholders abused the new right single-handedly conjured up by the Office. In the 2024 triennial rulemaking process three years later, the proponents of this exemption sought renewal and a modest expansion that was well within the bounds of fair use. In accordance with the Office's rules, the proponents offered evidence from users of the existing exemption to show that the exemption is warranted. In response, the American Association of Publishers and the Motion Picture Association issued unreasonable and intimidating demand letters to the very academic researchers who had volunteered their perspective, propounding a lengthy list of questions about their security practices.[28] These trade organizations did so under the auspices of their members (though with questionable authority—e.g., the AAP claimed to

[27] 37 C.F.R. 201.40(b)(4)(i)(D)&(b)(5)(i)(D).

[28] See, Association of American Publishers, Comments in Opposition to Proposed Class 3(b): Literary Works – Text and Data Mining, Feb. 20, 2024, https://www.copyright.gov/1201/2024/comments/opposition/Class%203(b)%20-%20Opp'n%20-%20Association%20of%20American%20Publishers.pdf

The letters demanded:

1. An overview of the policies and protocols in place at your institution concerning the security measures that apply to your institution's own highly confidential information ("HCI").
2. Written policies and protocols concerning the security measures that apply to your institution's HCI, including but not limited to:
    a. Written agreements with and/or registration of persons seeking to engage with HCI
    b. Password, two-factor and/or other identification protocols
    c. Training of personnel with respect to handling of HCI
    d. Physical security to protect HCI storage facilities, including cameras and locks
    e. System intrusion protections and alarms
    f. "Choking" or other mechanisms to prevent downloading or reproduction of HC
3. An explanation of how applicable security measures are communicated to and enforced with respect to researchers and other institutional actors engaged in circumvention activities under the Exemption.
4. Written guidance and/or instructional materials concerning security that is provided to researchers and other institutional actors engaged in TDM activities under the Exemption.
5. Efforts by you or the institution to monitor and ensure compliance with applicable security measures by researchers and others engaged in circumvention activities under the Exemption.

represent its membership broadly, which included publishers who are subsidiaries of the very institutions targeted by their letters). The net effect was to intimidate researchers who had offered their perspective in good faith, chilling their willingness to participate in the rulemaking process in the future or to exercise the rights they already have under fair use and existing exemptions.

So what did the Office do? As these attempts came to light in the rulemaking process, the Office's response was not to admonish the trade associations or to revise its rules to prevent further abuses. Instead, the Office *broadened* the security demand provision, which in the now-revised rule explicitly allows trade associations to issue such demands on behalf of rightsholders, emboldening them to be even more aggressive in the future.[29]

Neither Section 1201 nor any other law gives the Copyright Office authority to create new rights for copyright owners. If a rightsholder believes that their work has been infringed or that TPMs have been circumvented in a way that exceeds the law, the appropriate solution is to litigate in court and to go through the well-established discovery process.

But thanks to the new "right" invented by the Office, rightsholders have the ability to do prophylactic security audits of those suspected of using their works. By effectively granting rightsholders unchecked power to demand detailed information about internal security practices, the Office incentivizes copyright holders to use these demands as a strategic tool to intimidate and burden law-abiding users, undermining the original constitutional purpose of fostering creativity and progress. This stifles competition by discouraging research, innovation, and the fair use of copyrighted material at research institutions who are vulnerable to these coercive tactics and least able to absorb the cost and disruption of such unwarranted audits.

Recommendations

We believe the best outcome would be for Congress to overturn Section 1201 altogether. Short of that, it should be scaled back to ensure that its applicability is limited to the situations it was intended to target—combating piracy. Using or distributing tools for circumvention should not be a violation of Section 1201 unless the use or distribution is intended to facilitate copyright infringement. Not only would this bring the law back in line with its intent, but it would dramatically reduce the enormous costs of the triennial rulemaking process that are currently shared by the government, the public, and rightsholders.

In the meantime, we urge the FTC to recommend that the triennial rulemaking process be reformed. Such reforms should include:

[29] The Office did clarify that such requests must be "reasonable" and based on a "reasonable belief" of use of the subject copyrighted work as a limiting factor, which we appreciate.

- *Independent Fact-Finding*. As part of the triennial rulemaking, the Copyright Office should actively solicit input from users and undertake independent fact-finding to determine whether lawful uses of copyrighted works are being impaired by TPMs.

- *Reduce Complexity and Re-assign Burdens of Proof.* The complexity and burden now imposed on consumers should be replaced with a regime that imposes the burden of proof on those best positioned to shoulder it. Accordingly, once a petitioner comes forward with a concern regarding a lawful use that appears to be impaired by TPMs, the burden should then shift to the copyright owner to (1) describe how the TPM functions and how widely it is deployed; and (2) demonstrate by a preponderance of the evidence that continuing DMCA protection for the TPM in question is necessary to the market viability of the work.

- *Leave Fair Use to the Courts.* Where a petitioner comes forward with a use, otherwise impeded by TPM restrictions, that might plausibly be viewed by a court as a fair use, the Copyright Office should presume that the use in question is a fair use for purposes of considering whether an exemption should be granted.

- *Authorize Exemptions to Include Distribution of Circumvention Tools*. As noted above, consumers must have access to circumvention tools if they are to be able to take advantage of any DMCA exemptions granted in the rulemaking. Congress should expand the scope of the rulemaking proceedings to expressly authorize the Librarian to grant exemptions to the DMCA's prohibitions on trafficking in circumvention tools to the extent necessary to permit technically unsophisticated consumers take advantage of any exemptions to the DMCA's circumvention prohibition granted in the rulemaking.