ELECTRONIC FRONTIER FOUNDATION

House Committee on the Judiciary Subcommittee on Courts, Intellectual Property and the Internet

Hearing:
"Chapter 12 of Title 17"

Testimony of Corynne McSherry
Intellectual Property Director
Electronic Frontier Foundation

September 17, 2014

Chairman Goodlatte, Ranking Member Conyers; Chairman Coble, Ranking Member Nadler, and Members of the Committee, thank you for the opportunity to speak today on Section 1201 of the Digital Millennium Copyright Act. My name is Corynne McSherry, and I am Intellectual Property Director for the Electronic Frontier Foundation, a nonprofit civil liberties organization dedicated to protecting consumer interests, innovation, and free expression in the digital world.

For almost 25 years, EFF has represented the interests of technology users in both court cases and in broader policy debates regarding the application of law in the digital age, including the "anti-circumvention" provisions of the Digital Millennium Copyright Act. As counsel and as friends of the court, we have been involved in most of the leading court cases interpreting Section 1201. Today, we regularly counsel security researchers, innovators and ordinary Internet users regarding the pitfalls of Section 1201 as part of our Coders' Right Project. We also have extensive experience with the 1201 exemption process, having sought and obtain a variety of exemptions (and failed to obtain others).

Based on this experience, we have seen that Section 1201 has not been used as Congress envisioned. Indeed, the past year has seen an object lesson in the profound flaws of Section 1201, as consumers discovered, to their dismay, that merely unlocking their phones might violate the DMCA. They also discovered that the DMCA puts an unelected official in charge of regulating their personal devices. And they were not happy. Thousands spoke out, the White House weighed in, and Congress passed a law temporarily restoring the ability of consumers to unlock their phones.

We are grateful that Congress passed that law, but we should all be profoundly disturbed that it was necessary to do in the first place.

Section 1201 of the Copyright Act was ostensibly intended to stop copyright infringers from defeating anti-piracy protections added to copyrighted works. In practice, however, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities. We have collected many examples of such misuses in our whitepaper, *Unintended Consequences: 16 Years Under the DMCA*.[1] I am submitting that document in addition to this statement for the Committee's reference, but I will offer here just a few examples.

1. Section 1201 Impedes Competition and Innovation.

Traditionally, once a consumer has purchased a product, she has been free to use it however she sees fit. Legitimate consumers of electronic goods have been free to customize their products to better fit their needs; just as car enthusiasts might wish to soup up 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 also been free to

[1] *See* https://www.eff.org/pages/unintended-consequences

choose competitive add-on or alternative technologies that interoperate with the goods they buy, because innovators were able to develop and distribute such technologies. But in its current form, the DMCA threatens those freedoms.[2]

The anti-competitive effect of Section 1201 became evident early on with respect to DVDs. The encryption on DVDs was broken almost immediately, as were updated versions. Despite early lawsuits, easy-to-use DVD copying software has been available for free from many online sources for many years. Yet movie studios continued to embrace encryption, using it on every commercial DVD release. Why? We believe that one reason is that the movie studios (acting through their agent, DVD-CCA) could force innovators to sign a license agreement for that encryption software before they built anything that can decrypt a DVD movie.

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) must first pass muster in the 3-way "inter-industry" negotiation (movie studios, incumbent consumer electronic companies, and big computer companies) that is DVD-CCA In other words, you must get permission (from your adversaries and competitors!) before you innovate. If these had been the rules in the past, there would never have been a Betamax, much less an iPod.

But the problem does not stop with DVD technologies. Most modern durable goods—including household appliances, power tools, calculators, cameras, stereos, printer cartridges, garage door openers, as well as video game controllers, headsets, and memory cards—contain some element of copyrightable software code.[3] In order for replacement parts and compatible accessories to function, they must "access" the code inside. If unauthorized access amounts to circumvention of a TPM and is therefore prohibited, the manufacturer can use the DMCA to assert exclusive control over the market for those goods and accessories.

The detrimental effects on consumers are well documented. For instance, cell phone manufacturers sell phones equipped with technological protection measures that lock consumers to a particular service provider, forcing them to pay artificially inflated service charges and crippling the market for used phones.[4] According to the claims of major U.S. wireless carriers, unlocking a phone without your carrier's permission violates the DMCA. But a prohibition on unlocking has nothing to do with preventing infringement. Camera makers have similarly installed technological protection measures

---

[2] *See* Dan L. Burk, *Anticircumvention Misuse*, 50 UCLA L. REV. 1095, 1139 (2003)

[3] 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.

[4] 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/.

that render pictures unreadable in competitors' photo-editing programs, preventing consumers from editing their own pictures with their preferred software.[5]

Similarly, Apple has relied on the DMCA to "lock" iPhone owners into purchasing software exclusively from Apple's own App Store.[6] Apple uses technical measures backed by the DMCA to try to lock iPhone owners into obtaining software ("apps") exclusively from Apple's own iTunes App Store, where Apple must approve every app and retains 30% of revenues generated by app sales. This business practice has had significant consequences for both competition and speech, as Apple regularly rejects apps that might compete with Apple's own offerings or that are deemed "potentially offensive."[7]

Despite Apple's efforts, millions of iPhone owners, took steps to "jailbreak" their iPhones to use the carriers and apps of their choice. They did so under a legal cloud, however; Apple contended that these activities violated the DMCA. Responding to intensive efforts, the Librarian of Congress granted an exemption for jailbreaking, but that exemption is both narrow and temporary.

And that's just the beginning: the DMCA has been used to block aftermarket competition in laser printer toner cartridges, garage door openers, videogame console accessories, and computer maintenance services. For example, StorageTek sells data storage hardware to large enterprise clients. It also sells maintenance services for its products. Custom Hardware is an independent business that repairs StorageTek hardware. In an effort to eliminate this competitor in the maintenance services market, StorageTek sued under the DMCA, arguing that Custom Hardware had circumvented certain passwords designed to block independent service providers from using maintenance software included in the StorageTek hardware systems. In other words, StorageTek was using the DMCA to ensure that its customers had only one place to turn for repair services.[8]

---

[5] 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.

[6] David Kravets, *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/.

[7] See e.g., Jason Kincaid, *Apple is Growing Rotten to the Core: Official Google Voice App. Blocked from App Store*, TechCrunch, Jul. 27, 2009), http://techcrunch.com/2009/07/27/apple-is-growing-rotten-to-the-core-and-its-likely-atts-fault/; Fred von Lohmann, *Another iPhone App Banned: Apple Deems South Park App 'Potentially Offensive*, EFF Deep Links, Feb. 17, 2009, http://www.eff.org/deeplinks/2009/02/south-park-iphone-app-denied.

[8] Fred von Lohmann, *DMCA Used to Stymie Competition . . . Again*, EFF Deep Links blog (Nov. 4, 2005), https://www.eff.org/deeplinks/2005/11/dmca-used-stymie-

The infamous Lexmark litigation is another case in point. Lexmark, the second-largest laser printer maker in the U.S., has long tried to eliminate the secondary market in refilled laser toner cartridges. Lexmark had added 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. Lexmark then used the DMCA 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 litigation alone sent a chilling message to those in the secondary market for Lexmark cartridges.[9]

Garage door opener manufacturer Chamberlain Group also invoked the DMCA 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 the DMCA because its clicker bypassed an "authentication regime" between the Chamberlain remote opener and the mounted garage door receiver unit. On Chamberlain's logic, consumers would be locked into a sole source not only for replacement garage door clickers, but virtually any remote control device. Like SCC, Skylink ultimately defeated Chamberlain both at the district court and court of appeals, but only after many months of expensive litigation. In the words of the court of appeals, Chamberlain's use of the DMCA was nothing less than an "attempt to leverage its sales into aftermarket monopolies."[10]

More recently, Microsoft used the DMCA to try to shut down competition for gaming accessories. Datel, Inc. produces third-party accessories for every major videogame console, including Microsoft's Xbox 360.[11] As with all third-party manufacturers, Datel must engineer its accessories so that they will be compatible with the chosen first-party console; this frequently requires 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

---

competition-again; *Storage Technology v. Custom Hardware Engineering,* 421 F.3d 1307 (Fed. Cir. 2005).

[9] 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).

[10] 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).

[11] 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.

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 the DMCA. In a nutshell, Microsoft forced consumers to purchase its own memory cards and then used the DMCA to attack legitimate competitors.

Moreover, manufacturers of ordinary consumer products have sought to extend the DMCA to police consumer behaviors and innovations that happen to be contrary to the manufacturers preferences. For example, calculator manufacturers have brought circumvention claims against hobbyists who reverse-engineered their personal graphing calculators to develop alternative operating systems for personal use.[12]

Those manufacturers were likely influenced by the outcome of an earlier case, in which Vivendi-Universal's Blizzard Entertainment video game division brought a DMCA lawsuit against another group of hobbyists who created software that allowed owners of Blizzard games to play their games over the Internet. The software, called "bnetd," allowed gamers to set up their own alternative to Blizzard's Battle.net service. The bnetd software was freely distributed, open source, and noncommercial. Blizzard argued that the software could be used for illegal copying, although it had been neither designed nor used for that purpose by its creators. In a widely criticized decision, the Court of Appeals for the Eighth Circuit held that Congress' explicit protections for reverse engineering and add-on innovation in the DMCA are too narrow and weak to protect innovators from lawsuits when the software they create is used for illegal copying, even if the copying occurs without the knowledge or participation of the program's creators.[13]

2. Section 1201 Chills Free Expression and Scientific Research.

a. Freedom of the press

One of the first cases involving Section 1201, *Universal City Studios v. Reimerdes,* illustrated the chilling effect that the law would have on the freedom of the press. When 15-year-old Norwegian teenager announced that he had developed DeCSS, a software program that defeats the CSS encryption used on DVD movies, many news publications covered the story, including 2600 Magazine. In the course of its coverage, the magazine made the program that was at the heart of the controversy available on its web site. Dozens of other news organizations made a similar journalistic decision, including the New York Times, San Jose Mercury News and CNN, a division of Appellant Time Warner. Indeed, renowned copyright scholar Jane Ginsburg of Columbia Law School linked to sites that published DeCSS in order to help her students understand the controversy surrounding this litigation. 2600 was not involved in the development of the software, nor was it accused of having used the software for any copyright

[12] 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.

[13] *Davidson & Assoc. v. Jung*, 422 F.3d 630 (8th Cir. 2005).

infringement. Nonetheless, eight major motion picture companies used the brought DMCA claims against the magazine, seeking to block it from publishing the code, even though it was by then widely available.

Notwithstanding the First Amendment's guarantee of a free press, the district court permanently barred 2600 from publishing, or even linking to, the DeCSS code. The Second Circuit Court of Appeals upheld the lower court decision.[14] In essence, the movie studios effectively obtained a "stop the presses" order banning the publication of truthful information concerning a matter of public concern—an unprecedented curtailment of well-established First Amendment principles.[15]

b. Security research

Since 1998, Section 1201 has been used repeatedly to prevent researchers from investigating various DRM technologies, and/or from talking about what they find. The threat was illustrated early on by the actions of a multi-industry group known as the Secure Digital Music Initiative (SDMI) issued a public challenge encouraging skilled technologists to try to defeat certain watermarking technologies intended to protect digital music. Princeton computer science professor Edward Felten and a team of researchers at Princeton, Rice, and Xerox took up the challenge and succeeded in removing the watermarks.

When the team tried to present their results at an academic conference, however, SDMI representatives threatened the researchers with liability under the DMCA. The threat letter was also delivered to the researchers' employers and the conference organizers. After extensive discussions with counsel, the researchers withdrew their paper from the conference. The researchers took the matter to court, the threat was ultimately withdrawn and a portion of the research was published at a subsequent conference. After enduring this experience, at least one of the researchers involved has decided to forgo further research efforts in this field.[16]

---

[14] *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d. 294 (S.D.N.Y. 2000), aff'd sub nom. *Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001).

[15] Carl S. Kaplan, *Questioning Continues in Copyright Suit*, N.Y. Times, May 4, 2001, http://www.nytimes.com/2001/05/04/technology/04CYBERLAW.html; Simson Garfinkel, *The DVD Rebellion*, MIT Technology Review (July 1, 2001), http://www.technologyreview.com/article/401086/the-dvd-rebellion/; Xenia P. Kobylarz, *DVD Case Clash—Free Speech Advocates Say Copyright Owners Want to Lock Up Ideas*; *Encryption Code is Key*, S.F. Daily J., May 1, 2001.

[16] Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, 293 Science 2028, Sept. 14, 2001; Letter from Matthew Oppenheim, SDMI General Counsel, to Prof. Edward Felten, April 9, 2001, *available at* http://cryptome.org/sdmi-attack.htm; *Felten, et al. v. RIAA, et al.*, EFF, https://www.eff.org/cases/felten-et-al-v-riaa-et-al (last visited Jan. 10, 2013).

Threats like these have chilled the legitimate activities of journalists, publishers, scientists, students, programmers, and others. Bowing to DMCA liability fears, online service providers have censored discussions of copy-protection systems, programmers have removed computer security programs from their websites, and students, and security experts have stopped publishing details of their research.

These developments weaken security for all computer users, as security researchers shy away from performing and/or sharing research that might run afoul of section 1201. For example, when a group of Princeton researchers discovered the existence of several security vulnerabilities in the CD copy-protection software on dozens of Sony-BMG titles, they delayed publishing the discovery for several weeks while consulting with lawyers in order to avoid DMCA pitfalls.[17] This left millions of music fans at risk, until the security flaws inherent in Sony-BMG's "rootkit" copy-protection software were subsequently publicized by another researcher who was apparently unaware of the legal cloud created by the DMCA.

Researchers estimated that the rootkit compromised the security of more than 500,000 networks, including government and military networks.[18] As consumers and government become increasingly aware of the importance of protecting computer security, they should be deeply concerned about any legal restriction that might inhibit researchers' ability to find and publicize security vulnerabilities.

Section 1201 does include a number of exceptions for certain limited classes of activities, including security testing, reverse engineering of software, encryption research, and law enforcement. However, these exceptions are much too narrow to be of real use to the constituencies they were intended to assist.[19] As Professor Felten put it, the security research exceptions "appear[] to have been written without consulting any researchers. There may be someone, somewhere, who has benefited from this exemption, but it fails to protect almost all of the relevant research."[20]

---

[17] *See* Edward Felten, *The Chilling Effects of the DMCA*, Slate, Mar. 29, 2013, http://www.slate.com/articles/technology/future_tense/2013/03/dmca_chilling_effects_how_copyright_law_hurts_security_research.single.html

[18] Cory Doctorow, Sony Infects More Than 500k networks, Including Military and Govt., BoingBoing, Nov. 5, 2005, http://boingboing.net/2005/11/15/sony-infects-more-th.html

[19] *See* Pamela Samuelson, Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised, 14 Berkeley Law Journal 519, 537-57 (1999).

[20] *See* Edward Felten, *The Chilling Effects of the DMCA*, Slate, Mar. 29, 2013, http://www.slate.com/articles/technology/future_tense/2013/03/dmca_chilling_effects_how_copyright_law_hurts_security_research.single.html

3. Section 1201 Jeopardizes Fair Use.

"Fair use" is a crucial element in American copyright law—the principle that the public is entitled, without having to ask permission, to use copyrighted works in ways that do not unduly interfere with the copyright owner's market for a work. Fair uses include personal, noncommercial uses. Fair use also includes activities undertaken for purposes such as criticism, comment, news reporting, teaching, scholarship or research.

By banning all acts of circumvention, and all technologies and tools that can be used for circumvention, the DMCA grants to copyright owners the power to unilaterally eliminate many fair use rights. To make a fair use of a copyrighted work, a person must be able to access that work. Today, many forms of digital content—including e-books and video—are "copy-protected" and otherwise restricted by technological means. Whether scholars, researchers, commentators and the public will continue to be able to make legitimate fair uses of these works will depend upon the availability of tools to bypass these digital locks, and the legal right to use those tools.

The DMCA, however, prohibits the creation or distribution of such tools, even if they are needed to enable fair uses. As a result, fair uses have been whittled away by digital locks allegedly intended to "prevent piracy." Equally importantly, the DMCA prevents the law from developing to encompass new technologies. Future fair uses may not be developed for restricted content, because courts will never have the opportunity to rule on them. Fair users will be found liable for "picking the lock" and thereby violating the DMCA, whatever the merits of their fair use defense.

For example, e-books often include DRM technology that prevents people who are blind or visually impaired from running book that they have lawfully purchased through a text-to-speech converter. Similarly, Internet-distributed video and DVD and Blu-ray discs include DRM features that inhibit development of advanced closed captioning and video description technologies that make movies and television shows accessible.[21] Technologies for bypassing these technologies are available and clearly serve a valuable and non-infringing purpose. Nonetheless, using them may be unlawful under the DMCA except where disability rights advocates have managed to obtain a temporary exemption. Moreover, as discussed below, because the exemption process does not apply to the distribution of tools, companies and individuals that develop these technologies remain under threat.

DVD technologies provide another object lesson. There are many legitimate reasons to copy DVDs. Once the video is copied to a computer, for example, lots of fair uses become possible—video creators can remix movie clips into original YouTube

[21] Blake Reid, *The Digital Millennium Copyright Act Is Even Worse Than You Think*, Slate, Mar. 20, 2013, http://www.slate.com/articles/technology/future_tense/2013/03/dmca_copyright_reform_u_s_law_makes_digital_media_inaccessible.html

videos, frequent travelers can load the movie into their laptops, and DVD owners can skip the otherwise "unskippable" commercials that preface certain films.

DMCA lawsuits targeting makers of DVD copying tools hampered these and other fair uses. In *Universal v. Reimerdes*, for example, the court held that the DMCA bans DeCSS, the first of many widely available free tools for decrypting and copying DVDs. In another case, federal courts ordered 321 Studios' DVD X Copy product taken off the shelves for violating the DMCA. Major movie studios also used the DMCA to sue Tritton Technologies, the manufacturer of DVD CopyWare, and three website distributors of similar software.[22]

Those lawsuits, and the Section 1201 generally, cast a legal cloud over a variety of valuable creative activities, particularly audiovisual "remixes."

The creative practice of "remixing" existing video content to create original expression is a time- honored tradition dating to 1918 when Lev Kuleshov began splicing and assembling film fragments to tell new stories.[23] Today, the ability to remix and share video content has been democratized to an unprecedented degree, thanks to the combination of inexpensive video editing tools on personal computers and free, easy-to-use video hosting services such as YouTube. Every day, thousands of Americans create and share original, primarily noncommercial videos that include clips taken from works released on DVD. Remixing is also being recognized as an important pedagogical practice on every educational level, with scholarship as well as practical classroom textbooks being written on this subject.[24]

All of these forms of remix are valuable not only as creative works, but also because they help create the next generation of artists, who can gain skills and exposure otherwise entirely unavailable to them. As one artist told the Organization for Transformative Works, a nonprofit dedicated to promoting remix culture,

---

[22] Matthew Mirapaul, *They'll Always Have Paris (and a Scholarly Web Site)*, N.Y. Times (March 16, 2002), http://www.nytimes.com/2002/03/18/movies/arts-online-they-ll-always-have-paris-and-a-scholarly-web-site.html; Lisa Bowman, *Hollywood Targets DVD- Copying Upstart*, CNET News (Dec. 20, 2002), http://news.com.com/2100-1023-978580.html; *Paramount Pictures Corp. v. Tritton Technologies Inc*., No. CV 03-7316 (S.D.N.Y. filed Sept.17, 2003); *321 Studios v. MGM*, 307 F.Supp.2d 1085 (N.D. Cal. 2004).

[23] Lev Kuleshov, *Kuleshov on Film* (1974).

[24] Colin Lankshear & Michele Knobel, *Remix: The Art and Craft of Endless Hybridization*, 52 Journal of Adolescent & Adult Literacy 22-33 (2008), *available* http://extendboundariesofliteracy.pbworks.com/f/remix.pdf; Catherine Latterell, *Remix: Reading and Composing Culture* (2005); Kristina Busse & Alexis Lothian, *Scholarly Critiques and Critiques of Scholarship: The Uses of Remix Video*, 26 Camera Obscura 2 77: 139, 142 (2011).

> I began [creating remix videos] in 1999 as a teenager living in Australia, mainly in The X-Files fandom and long before the days of YouTube. The advent of that site gave a much larger audience for my work, including some Creative Directors at various trailer houses who began offering me paid work and beginning my career as a trailer editor and producer. I now live in New York city cutting high-end theatrical trailers for cinema. The point is, had I not had the outlet such as YouTube to conceive, develop and showcase my work, I would not be in this profession today. There is a great need for trailer cutters in my highly competitive and niche industry, and we need to develop as many of the best next generation of trailer editors as we can.[25]

The Register of Copyrights has acknowledged that many remix videos are protected by the fair use doctrine and, therefore, do not infringe copyright. Nonetheless, the process of creating them risks violating the DMCA where, as is common, the creator must use a "DVD ripper" to extract video clips. Moreover, because the vast majority of remix creators are amateur videographers who engage in video creation as a hobby, they are unlikely to have access to copyright counsel to explain the subtleties of the DMCA to them and are likely unaware of the counterintuitive nature of circumvention liability as applied to DVDs. It will strike many laypersons as bizarre that relying on infringing copies taken from unauthorized Internet sources are preferable (from a circumvention point of view) to "ripping" a DVD that you have purchased. Similarly, the public may find it hard to believe that taking excerpts by means of video capture carries different legal consequences than using a DVD ripper to accomplish the same result.

Working closely with OTW, EFF has managed to obtain exemptions for some forms of remix activities, but those exemptions are limited and temporary. A permanent fix is needed to truly protect these creators.

Other kinds of fair uses were also hampered, particularly format-shifting. In October 2008, RealNetworks was forced to stop sales of its RealDVD software, which allowed users to copy a DVD and store it on their hard drive. This format-shifting by RealDVD would have enabled DVD owners to create backups, organize a movie collection digitally, and watch a DVD at any time without being tied to a physical disc—all valuable personal uses. Nor did RealDVD represent a "piracy" threat: RealDVD preserved the DVD's CSS copy-protection system and added numerous additional control measures. RealNetworks also took a license from the DVD Copy Control Association to perform the necessary DVD decryption. Nevertheless, a federal court ruled in August

[25] Email from Lyle to OTW (July 27, 2010) (on file with authors). Another vidder recently secured a contract with the producers of House because of the editing capability she demonstrated in her House vids. See Live Journal, http://vidding.livejournal.com/2751680.html (last visited Nov. 30, 2011).

2009 that, even if the uses enabled by RealDVD were lawful fair uses, the DMCA forbids the distribution of tools like RealDVD.[26]

The same anti-innovation tactics have also been applied to streaming. One example involved, ironically enough, RealNetworks. Start-up software company Streambox developed a product, known simply as the Streambox VCR, designed to time-shift streaming media. When RealNetworks discovered that the Streambox VCR could time-shift streaming RealAudio webcasts, it invoked the DMCA and obtained an injunction against the product.[27]

4. Section 1201 harms the environment by impeding electronics repair and recycling.

From phones to cars to refrigerators to farm equipment, software is helping our stuff work better and smarter, with awesome new features. But if that software is protected by DRM, repair and recycling these goods may require circumvention, in violation of Section 1201. That means more people will feel pressured to simply throw those goods away, rather than repairing and re-using them.

For example, phones that are locked to a single carrier are less likely to be reused, particularly if the act of unlocking a phone could expose a person to civil and criminal liability under the DMCA. According to the Environmental Protection Agency, as of February 2009 only 10 percent of unwanted cell phones were recycled each year.[28] And sending used phones and other electronics to landfills isn't just wasteful, it also contributes to air and water pollution and greenhouse gas emissions.[29] Cell phones are actually considered to be hazardous waste by the California Department of Toxic Substances Control, because they may contain antimony, arsenic, beryllium, cadmium, copper, lead, nickel, and zinc.[30]

5. The costs don't outweigh the benefits.

These costs might be tolerable if they were outweighed by real benefits, i.e., if our anti-circumvention rules and the technologies they are supposed to backstop actually

---

[26] *Real Networks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 942 (N.D. Cal., 2009).

[27] *RealNetworks, Inc. v. Streambox, Inc*., No. C99-2070P, 2000 WL 127311 (W.D. Wash. Jan. 18, 2000).

[28] EPA, *Fact Sheet: Recycle Your Cell Phone: It's An Easy Call* (Feb. 2009), http://www.epa.gov/osw/partnerships/plugin/cellphone/cell-fs.htm.

[29] *Id.*

[30] Cal. Dep't of Toxic Substances Control, *Universal Waste*, http://www.dtsc.ca.gov/hazardouswaste/universalwaste/index.cfm.

deterred infringement. Sadly, they do not.[31] For example, notwithstanding the DMCA, the encryption on movie DVDs was broken early and provided no meaningful protection against widespread infringement. Every film that Hollywood releases is available within days, or even hours for those who really want an unauthorized copy. The same was true with respect to music and is still true with respect to games and other content. Individuals and companies that engage in large-scale copyright infringement are not deterred by Section 1201. After all, chances are they are *already* on the hook for substantial copyright damages.

Nevertheless, legitimate media sources manage—year after year—not only to stay afloat, but to flourish. iTunes, Amazon, Magnatune and dozens of other sites sell huge volumes of music without the need for DRM. Streaming services like Netflix and Spotify have succeeded because they are more convenient than unauthorized alternatives, not because DRM does anything to enhance their economics. Indeed, just a few months ago Frank Gibeau, the president of Electronic Arts, declared DRM to be a "failed dead-end strategy."[32]

In fact, DRM may actually encourage more infringement by making "legitimate" media options less attractive. In 2002, Microsoft engineers considering the effectiveness of DRM suggested as much, noting that DRM was likely to drive consumers to unauthorized distribution mechanisms, i.e., "the darknet."

> There is evidence that the darknet will continue to exist and provide low cost, high-quality service to a large group of consumers. This means that in many markets, the darknet will be a competitor to legal commerce. From the point of view of economic theory, this has profound implications for business strategy: for example, increased security (e.g. stronger DRM systems) may act as a *disincentive* to legal commerce. Consider an MP3 file sold on a web site: this costs money, but the purchased object is as useful as a version acquired from the darknet. However, a securely DRM- wrapped song is strictly *less* attractive: although the industry is striving for flexible licensing rules, customers *will* be restricted in their actions if the system is to provide meaningful security. This means that a vendor will probably make more money by selling unprotected objects than protected objects. In short, if you are

[31] This likelihood was spotted early on. See, e.g., Stuart Haber, Bill Horne, Joe Pato, Tomas Sander, Robert Endre Tarjan, "If Piracy is the Problem, is DRM the Answer?" http://www.hpl.hp.com/techreports/2003/HPL-2003-110.pdf

[32] Andras Neltz, EA Labels President Calls DRM a "Failed, Dead-End Strategy." http://kotaku.com/ea-labels-president-calls-drm-a-failed-dead-end-strat-461313335

> competing with the darknet, you must compete on the darknet's own terms: that is convenience and low cost rather than additional security.[33]

DRM technologies, even supported by legal protections such as Section 1201, don't stop copyright infringement. They do impede innovation and thwart traditional consumer rights and expectations.

6. The Exemption Process Does Not Save Matters.

The DMCA triennial rulemaking was meant as a "fail-safe" to prevent DRM from encroaching on the public's ability to engage in activities that would otherwise be perfectly legal under copyright law. Unfortunately, the rulemaking has not served its purpose. The exemptions created by the Copyright Office can be helpful but, as the cell phone unlocking episode showed, they are too narrow and too brief. They also turn a small, specialized federal office into a sort of Technology Regulation Bureau. However well intentioned and dedicated the Copyright Office and the Library of Congress may be, it does not make sense to task a small group of overburdened copyright lawyers and librarians with making decisions that can shape the future of technology markets.

The process does not apply to tools. The DMCA provides that the Librarian of Congress can only grant exemptions from the DMCA's prohibition on *acts* of circumvention; exemptions from the DMCA's prohibition on distributing *tools* of circumvention are not within the scope of the rulemaking. As a result, exemptions granted can only be exercised by persons who have the technical know-how to fashion their own software or hardware circumvention tools. Thus, the rulemaking proceeding holds out, at best, an empty promise to consumers: a legal right to circumvent, without access to the tools necessary to make that right a reality.

The process is complex and burdensome. Any person interested in participating meaningfully in the DMCA rulemaking process must first decipher a bewildering array of legal arcana and independently gather considerable evidence. Rather than receiving public comments and engaging in independent fact-finding, as many administrative agencies do, the Copyright Office has instead laid a heavy burden on the shoulders of those seeking DMCA exemptions: "[P]roponents must show by a preponderance of the evidence that there has been or is likely to be a substantial adverse effect on noninfringing uses by users of copyrighted works."[34] Meeting that standard—which is not found in the DMCA's text—generally requires the assistance of specialized copyright attorneys, technical experts, researchers, and industry analysts. Without expert assistance, individuals cannot reasonably gather the evidence and devote the time

[33] Petter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" Microsoft Corporation (2002); *see also* M. Masnick: "File-sharing Moving En Masse to the Darknet," Techdirt, Mar. 5 2012.
[34] Register's 2003 Recommendation at 6. 7 17 U.S.C. § 1201(a)(1)(C).

necessary to participate successfully in the DMCA rulemaking process. And even if she does succeed, she must be prepared to make the case again, three years later.

The exemptions that are granted continue to be unnecessarily narrow. Security researchers had sought a DMCA exemption in 2003 in order to facilitate research on dangerous DRM systems like the Sony-BMG rootkit, but the Librarian of Congress denied their request.[35] In 2006, the Librarian granted an exemption to the DMCA for researchers examining copy protection software on compact discs.[36] However, this exemption, did not protect researchers studying other DRM systems. In 2009, security researchers again sought a DMCA exemption for computer security research relating to DRM systems, including the protection mechanisms used on the Electronic Arts videogame, Spore, which has been the subject of class action lawsuits alleging security vulnerabilities.[37] A narrow version of this exemption was granted in 2010. However, the exemption was not renewed in 2012, leaving this research vulnerable to legal action.[38]

The fight for DVD exemptions offers another telling example. Exemptions have been sought to allow movie critics to post movie clips, DVD owners to skip "unskippable" previews and commercials, and legitimate purchasers to bypass "region coding" restrictions on their DVD players. Every DVD-related request was denied in both the 2000 and 2003 triennial rulemakings.[39] In 2006, a narrow DMCA exemption was granted to allow film professors to create compilations of motion pictures for educational use in the classroom.[40]

In 2009, educators renewed their request for an exemption that would allow film professors, media studies educators, and students to use short clips taken from DVDs for educational purposes.[41] EFF and the Organization for Transformative Works also applied

---

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

[36] 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.

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

[38] 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.

[39] Copyright Office, Recommendation of the Register of Copyrights in RM 2002-4, 109-26 2003), *available at* http://www.copyright.gov/1201/docs/registers-recommendation.pdf.

[40] Statement of the Librarian of Congress Relating to Section 1201 Rulemaking, Copyright Office (Nov. 27, 2006), http://www.copyright.gov/1201/docs/2006_statement.html.

[41] Comments of Renee Hobbs, Peter Decherney, Library Copyright Alliance, http://www.copyright.gov/1201/2008/index.html.

for an exemption to allow remixers to extract clips from DVDs to create noncommercial remix videos.[42] While the motion picture industry endorsed a renewal of the narrow exemption for film professors, it opposed any expansion to permit other noninfringing uses of DVDs, going so far as to suggest that noninfringing users should camcord DVD clips from flat screen televisions.[43] In a major victory for remixers, educators, and other innovators, the Librarian of Congress finally approved several requests in 2010. These exemptions were renewed and expanded in 2012. But in about a month, we will have to start the process all over again, without any certainty as to whether we will succeed.

7. What can we do to "fix" Section 1201?

We believe the best outcome would be for Congress to overturn Section 1201 altogether. Short of that, the law should be scaled back to ensure that its applicability is limited to the situations it was intended to target: using or distributing tools for circumvention should not be a violation 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. That is why we strongly support the "Unlocking Technology Act," introduced last year by Representative Zoe Lofgren and a bipartisan group of sponsors.

In the meantime, the triennial rulemaking process should be reformed. Such reforms should include:

• *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 DRM technologies.

• *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 DRM restrictions, the burden should then shift to the copyright owner to (1) describe how the DRM technology functions and how widely it is deployed; and (2) demonstrate by a preponderance of the evidence that continuing DMCA protection for the DRM in question is necessary to the market viability of the work.

---

[42] Comments of EFF and OTW, http://www.copyright.gov/1201/2008/comments/lohmann-fred.pdf

[43] Jacqui Cheng, *MPAA: Teachers Should Videotape Monitors, Not Rip DVDS, Ars Technica*, May 7, 2009, http://arstechnica.com/tech-policy/news/2009/05/mpaa-teachers-should-video-record-tv-screens-not-rip-dvds.ars

• *Leave Fair Use to the Courts*. Where a petitioner comes forward with a use, otherwise impeded by DRM 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.

The 15-year history of DMCA abuse has cast a long shadow. Consumers, researchers, journalists, programmers, and others now must approach non-infringing activities with fear of legal liability—even if litigation never materializes. The DMCA has given anti-competitive, anti-consumer, and speech and research-chilling forces a powerful tool that now requires little effort to leverage. Given the existence of other legal mechanisms for policing actual infringement, we believe the costs far outweigh the benefits. We encourage you to continue this important conversation and consider legislative proposals that would limit those costs.