FEDERAL TRADE COMMISSION

FTC TOWN HALL: DIGITAL RIGHTS MANAGEMENT TECHNOLOGIES

William H. Gates Hall, Room133
University of Washington Law School
15th Avenue NE & NE 43rd Street
Seattle, Washington

Wednesday, March 25, 2009

COMMENT: PROJECT NO. P094502

ELECTRONIC FRONTIER FOUNDATION

February 9, 2009

Corynne McSherry

Staff Attorney and Kahle Promise Fellow
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

I. Statement Of Interest

EFF is a member-supported, nonprofit organization committed to defending civil liberties and the public interest in a digital world. Founded in 1990, EFF represents more than 14,000 contributing members including consumers, hobbyists, computer programmers, entrepreneurs, students, teachers, and researchers united in their reliance on a balanced copyright system that promotes both adequate protection for copyright owners and access to information in the digital age.

EFF has long been an active participant in the public debate over Digital Rights Management ("DRM") technologies and the impact of such technologies on consumers. In 2001, for example, EFF defended *2600* Magazine after several major movie studios sought to enjoin publication of information about DeCSS, a program that circumvents a standard form of DRM on DVDs. Four years later, EFF took a leading role in the class action litigation against Sony BMG when the DRM in its CDs introduced security flaws into millions of computers. In addition to litigation, EFF attorneys and activists have raised public awareness on DRM issues via EFF's website (one of the most linked-to sites in the world), numerous white papers, press commentary, and public speaking in the United States and abroad. EFF appreciates the opportunity to offer comments in these proceedings.

II. Introduction

It is appropriate that the FTC is convening this Town Hall now, for the preceding year has seen a growing consensus that the DRM experiment has been a resounding failure for consumers, for innovation, and even for some of its most vocal proponents. Indeed, the music industry, which once claimed that DRM "protection" was essential to providing legal access to music, has turned away from DRM in the past year, recognizing at last that the benefits of DRM are far outweighed by the costs.[1] Other industries may follow suit, but in the meantime, DRM continues to impose impermissible burdens on consumers.[2] First, DRM helps industry leaders dominate digital media markets and impede innovation. Second, DRM endangers consumers by rendering their computers insecure and violating consumers' reasonable expectations of privacy. Third, DRM harms consumers by degrading products and restricting consumers' ability to make otherwise lawful uses of their personal property, upsetting the traditional balance between the interests of copyright owners and the interests of the public. What is worse, these

[1] *See, e.g.,* Brad Stone, "Want to Copy iTunes Music? Go Ahead, Apple Says," New York Times Jan. 6, 2009; J. Cheng, Amazon Rounds Out DRM-free Music Offering with Sony BMG, Ars Technica, Jan. 10, 2008.

[2] For example, while Apple recently announced that iTunes would shortly be "DRM-free," the company still uses DRM on movies and TV programs, to lock iPhones to AT&T and Apple's iTunes App Store, and to prevent recent iPods from syncing with software other than iTunes, and so on. *See, e.g.* G. Keizer, Apple Adds DMCA Charge to Lawsuit Against Psystar, Computerworld, Nov. 30, 2008; F. von Lohmann, Apple Downgrades Video with DRM, Nov. 21, 2008, ; *see generally* R. Esguerra, Apple Shows Us DRM's True Colors, Electronic Frontier Foundation Jan. 7, 2009.

social costs far outweigh any conceivable benefit. DRM is touted as an effective means to restrict copyright infringement, yet evidence continues to mount that DRM not only does little to inhibit unauthorized copying, it may actually encourage it.

III. DRM Impedes Innovation and Competition

In the normal course of business, most companies will seek to improve their popular products and keep prices for those improvements reasonable. If they do not, they can be sure other companies will step in to fill the gap. Via DRM, however, industry leaders can thwart the normal market forces that drive innovation by "managing" how consumers and competitors use their products. Because significant improvements to the functionality of a seller's products can only be developed and sold with the seller's consent, DRM renders the seller impervious to the normal forces of market competition. This leaves consumers seeking innovative technologies with three options: an expensive supply, an illicit supply, or no supply at all.

The restrictive power of DRM depends on and is extended by two legal mechanisms: the Digital Millennium Copyright Act ("DMCA")[3] and End User License Agreements ("EULAs"). The entertainment industry maintains that Section 1201 of the DMCA makes it a violation of copyright law for consumers and competitors to circumvent—or even provide information that might help someone else circumvent—technological protection measures, whether or not such circumvention would normally be considered a non-infringing fair use.[4] In practice, the DMCA gives technology vendors a huge legal club against innovators. Vendors complain that they need this club to stop piracy, but it is hard to see why a competitor should have to solve a vendor's piracy problem before it can offer innovative enhancements to legitimate owners of consumer products.

EULAs take matters once step further, using contracts of adhesion to prevent consumers from using products they bought and paid for in any way other than as specified by the seller—again, whether or not such uses would otherwise be perfectly legal.[5]

[3] 17 U.S.C. §§ 512, 1201–1205, 1301–1332; 28 U.S.C. § 4001

[4] Section 1201 includes a number of exceptions for certain limited classes of activities, including security testing, reverse engineering of software, encryption research, and law enforcement. These exceptions have been extensively criticized as being too narrow to be of real use to the constituencies who they were intended to assist. *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).

[5] In March 2008, car product design company XPEL Technologies filed suit against American Filter Film Distributors, a rival who provides services for car paint and window film protection. Among a slew of other claims, XPEL alleged that American Filter violated the DMCA by using "Capture" software to copy product images from the XPEL website and distribute the image and product to other auto dealers. XPEL argued the DMCA was violated because (1) the XPEL website is protected by an end-user license agreement (EULA), (2) American Filter clicked that they agreed to the EULA, and (3) the EULA is a technological measure which effectively controls access to the copyrighted design works on XPEL's website. This is the first case where a "click-thru" EULA has been put forward as an access control protected by the DMCA. In August 2008, the most recent proceedings for this case, American Filter's

Examples of these inhibiting effects are legion.[6] Here are just a few:

A. Gaming:

1. Tecmo vs. Customers

Enthusiastic fans of the videogames Ninja Gaiden, Dead or Alive 3, and Dead or Alive Xtreme Beach Volleyball managed to modify their games to create new "skins" to change the appearance of characters in the game. Because these skins were add-on enhancements, only those who had already purchased the games could make use of the skins. These hobbyist tinkerers traded their modding tips and swapped skins on a website called ninjahacker.net. Tecmo, Inc., which distributes the games, was not amused and brought DMCA circumvention claims against the website operators and tinkerers who frequented the site.[7] The suit was ultimately dismissed after the website was taken down and settlements negotiated with the site's operators.[8]

2. Sony Attacks PlayStation "Mod Chips"

Sony has sued a number of manufacturers and distributors of "mod chips" for alleged circumvention of its region-coding DRM.[9] These "mod chips" are after-market accessories that modify Sony PlayStation game consoles to permit games legitimately purchased in one part of the world to be played on a games console from another geographical region. Sony complains that mod chips can also be used to play pirated copies of games. Sony sued Gamemasters, distributor of the Game Enhancer peripheral device, which allowed owners of a U.S. PlayStation console to play games purchased in Japan and other countries.[10] Although there was no infringement of Sony's copyright, the court granted an injunction under the DMCA's anti-circumvention provisions, effectively leaving gamers at the mercy of Sony's region coding system.[11]

motion to dismiss the DMCA claim was denied. It is still unknown whether XPEL's attempts to transform its EULA into an "access control" will succeed—but in the meantime a legitimate competitor is forced to continue expensive litigation. *See XPEL Techs. Corp. v. American Filter Film Distrs*, No. SA08-CA0175-XR, 2008 WL 3540345 (W.D. Tex. Aug. 11, 2008); Rebecca Tushnet, "Design, Dastar, (registration) dates and the DMCA," Rebecca Tushnet's 43(B)log, Aug. 17 2008.

[6] For more examples, see Electronic Frontier Foundation, "Unintended Consequences: Ten Years Under the DMCA," Oct. 2008, (App. Ex. A).

[7] Kevin Poulson, "Tecmo Spikes Nude Volleyball Suit," Wired (May 18, 2005).

[8] *Id.*

[9] Barry Fox, "Sony PlayStation ruling sets far-reaching precedent," New Scientist, Feb. 15, 2002; *Sony Computer Entmt. Am. Inc. v. Gamemaster*s, 87 F.Supp.2d 976 (N.D. Cal. 1999).

[10] *Sony Computer Entmt. Am. Inc. v. Gamemaster*s, 87 F.Supp.2d 976 (N.D. Cal. 1999)

[11] *Id.*

3. Blizzard Sues bnetd.org

Vivendi-Universal's Blizzard Entertainment video game division brought a DMCA lawsuit against a group of volunteer game enthusiasts 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 filed suit in St. Louis to bar distribution of the software, alleging that it was a DRM "circumvention device" and that the programmers also violated several parts of Blizzard's EULA, including a section on reverse engineering.[12] 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. The court also ruled that a click on a EULA's "I Agree" button is enough to waive fair use reverse engineering rights, further restricting the marketplace for add-on innovation.[13]

B. Cell Phones

Outside of the U.S., most consumers can easily change carriers and keep their phones by replacing an old carrier's SIM chip with a new one. But because of DRM, American cellular phone subscribers are artificially "locked" to their particular carrier's network. Mobile providers can and do use the DMCA to stop American customers from unlocking their phones and selecting a provider of their choice, resulting in poorer service and higher costs for customers, reduced competition contrary to explicit U.S. telecommunications policy, and environmental disaster as a result of mobile handset waste. For example, locked phones block foreign carrier's prepaid SIM chips, so the legal alternatives for traveling Americans are meager: pay a high roaming charge, violate the DMCA by circumventing the lock, or forego use of their phones.[14] Locked phones are also particularly onerous once a subscriber's initial service contract expires, because switching over to a competitor's network requires buying a new phone and manually transferring preferred settings, contacts, and any other stored phone data. More recently, "smartphone" makers like Apple have started locking phones to a single source for applications.[15] This new form of DRM turns distributors into unchecked gatekeepers

[12] *Davidson & Assoc. v. Jung*, 422 F.3d 630 (8th Cir. 2005); Howard Wen, "Battle.net Goes To War," Salon (Apr. 18, 2002).

[13] *Id.*

[14] Cyrus Farivar, "Locked vs. Unlocked: Opening Up Choice," New York Times (Nov. 1, 2007)

[15] Jack Schofield, "iPhone Could Mark the End of the Geek Affair," Guardian Technology Pages (Oct. 4, 2007)

who can exclude programs and even literature that they deem objectionable from all legal users' devices. Consistent with past DRM deployment, the smartphone lock limits the aftermarket functionality of a very expensive device with far more legitimate potential uses than the lock permits.[16]

C. Garage Door Openers

Chamberlain Group, a manufacturer of garage door openers, sued competitor Skylink Technologies after Skylink started selling cheap universal remote openers that worked with Chamberlain's mounted garage door receiver units. Chamberlain claimed that Skylink had circumvented Chamberlain's DRM because Skylink's opener bypassed an "authentication regime" between the Chamberlain remote opener and the mounted garage door receiver unit. In the words of the court of appeals, Chamberlain was trying to use the DMCA, in conjunction with the DRM on its receiver units, "to leverage its sales into aftermarket monopolies."[17] Skylink won its case, but its legal costs would be enough to convince many companies not to enter the market.

D. Printers

Lexmark, the second-largest laser printer maker in the U.S., has long tried to eliminate the secondary market in refilled laser toner cartridges. In January 2003, Lexmark employed the DMCA as a new weapon in its arsenal. Lexmark had added authentication routines between its printers and cartridges explicitly to hinder aftermarket toner vendors.[18] 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 re-manufacturers. SCC ultimately succeeded in getting the injunction overturned on appeal, but only after 19 months of expensive litigation, during which time its product was held off the market.[19] Thus, the litigation sent a chilling message to those in the secondary market for Lexmark cartridges or similar products: you might be able to sell your innovation, but only if you are willing to pony up some major legal fees first.

This is just a sampling of the many instances where, taken in combination with the broad powers conferred by the DMCA and EULAs, DRM has become a significant impediment

[16] *See* Comment of the Electronic Frontier Foundation, In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, U.S. Copyright Office Docket No. RM 2008-8, App. Ex. B.

[17] *Chamberlain Group v. Skylink Techs.*, 381 F.3d 1178 (Fed.Cir.2004).

[18] Hewlett Packard reportedly engages in similar practices, building in software that causes printer cartridges to "expire" within a give time—even if they are still filled with ink. Susan B. Shor, "Ink Expiration Prompts Suit Against HP," CRM Buyer (Feb. 23, 2005); Mike Magee, "HP Inkjet Cartridges Have Built-In Expiry Dates," The Inquirer (Apr. 29, 2003).

[19] D. McCullagh, "Lexmark Invokes DMCA in Toner Suit," CNET News, Jan. 8, 2003; *Lexmark v. Static Control Components*, 387 F.3d 522 (6th Cir. 2004).

to the development and marketing of useful innovations. These examples should suffice, however, to show that many companies do not use DRM solely, or even primarily, to prevent piracy, but rather to insulate themselves from normal competition.

Moreover, in many cases this improper protection from market forces is systematized and enforced by inter-industry bodies led by the companies that benefit most from that insulation. The Advanced Access Content System (AACS), a newer DRM standard, is administered by a consortium that includes some of the largest media, consumer electronics and information technology companies in the world, such as Disney, Warner Bros. Intel, Microsoft and Sony.[20] Similarly, technology companies such as Intel and Toshiba, and movie studios such as Twentieth Century Fox and Warner Bros. lead the DVD Content Control Association (DVD-CCA), the sole licensing entity for CSS.[21] Manufacturers who wish to make products that will play movies must pay a hefty fee and comply with the restrictions imposed by these consortia.

CSS and AACS do little to prevent unauthorized DVD copying; technology to break them has long been available (for many years, in the case of CSS). Yet movie studios continue to embrace these technologies. Why?

Perhaps because DRM for DVDs is not about preventing piracy, but rather protecting Hollywood business models from disruptive innovation. By acting through these consortia, industry leaders can force technology companies to sign license agreements before they build anything that can decrypt a DVD movie. This in turn gives some industry leaders 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 through a three-way "inter-industry" negotiation (movie studios, incumbent consumer electronic companies, and big computer companies). In other words, innovators must get permission from their competitors as well as their potential partners before they can offer new products.

In fact, even companies that play by the rules face business and legal threats. Kaleidescape, which makes a highly-acclaimed digital "jukebox" for DVD movies that complies with the CSS license, nonetheless was sued by DVD-CCA.[22] When DVD-CCA lost the case, DVD-CCA board members introduced an amendment that would change the CSS license to put Kaleidescape out of business.[23]

And in October 2008, RealNetworks was forced to stop sales of its RealDVD software,

[20] "Who Are the Founders," AACS – Advanced Access Control Systems Licensing Administrator.

[21] Federal Register: August 3, 2001 (Volume 66, Number 150)

[22] J. Borland, "Hollywood Allies Sue DVD Jukebox Maker" CNET News (Dec. 7, 2004).

[23] E. Bangeman, "DVD Licensing Group To Vote on Closing Copying Loophole," Ars Technica (Nov. 4. 2007).

designed to allow users to copy a DVD and store it on their hard drive. RealDVD makes an exact copy of everything on a DVD—including the DVD's CSS copy-protection system—and transfers it to the hard drive of a PC. A license from the DVD CCA authorizes RealNetworks to perform the necessary DVD decryption for this process. Moreover, to ensure the resulting DVD copy cannot be shared or stolen, RealDVD encrypts the saved DVDs again and tethers the copy to a limited number of PCs.[24] This format-shifting by RealDVD would empower consumers with numerous fair uses, such as allowing them to create backups, organize a movie collection digitally, and watch a DVD at any time without being tied to a physical disc.,

Yet despite these layers of protection for copyrighted content and the numerous fair uses for which RealDVD was designed, several movie studios sued RealDVD, alleging violations of the DMCA.[25] A temporary restraining order was granted to halt the sale of RealDVD pending a further hearing now scheduled for March 2009.[26]

IV. DRM Burdens Consumers with Inferior, Even Dangerous Products

DRM imposes one form of burden on consumers when it is used to inhibit competition and innovation. But the burdens do not end there. DRM technologies (backed by the DMCA) have also introduced serious security flaws into consumer computers, caused products that included DRM to lose value unexpectedly, and undermined traditional consumer fair use rights.

A. Security and Privacy

In 2005, research by independent security analysts revealed that DRM technology Sony BMG had included in millions of music CDs created serious security, privacy and consumer protection problems.[27]

At issue were two software technologies—SunnComm's MediaMax and First4Internet's Extended Copy Protection (also known as XCP)—which Sony BMG said were placed on music CDs to restrict consumer use of the music on the CDs. In truth, the software did much more, including reporting customer listening of the CDs and installing undisclosed and in some cases hidden ("rootkit") files on users' computers that could expose users to malicious attacks by third parties, all without appropriate notice and consent from purchasers. The CDs also conditioned use of the music on unconscionable licensing

[24] V. Godinez, "For PC: RealDVD Works So Well That It's On Legal Hold," Dallas Morning News (Oct. 10, 2008).

[25] Y. Salcedo, "RealNetworks Defends DVD Copying Software" Inside Counsel (Dec. 1, 2008).

[26] *Id.*

[27] *See generally* Sony BMG Litigation Info, Electronic Frontier Foundation; Comment of Edward Felten and J. Alex Halderman, RM 2005-11 — Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, (Dec. 1, 2005) pgs 6-7.

terms in the End User Licensing Agreement (EULA).

Initially Sony BMG denied there was a problem, claiming the XCP rootkit was "not malicious and [did] not compromise security." Thomas Hesse, President of Sony BMG's global digital business division, dismissed consumers' concerns, saying in an interview for a National Public Radio "Most people, I think, don't even know what a rootkit is, so why should they care about it?"[28]

After receiving harsh public criticism, Sony BMG acknowledged the security harm caused by the XCP CDs and recalled the infected discs.[29] As a result of class action lawsuit, SonyBMG later provided a range of remedies and compensation to purchasers of CDs with the XCP technology or the MediaMax technology.[30]

Ironically, perhaps, just two years earlier Princeton graduate student J. Alex Halderman had been threatened with a DMCA lawsuit after publishing a report documenting weaknesses in prior version of MediaMax.[31] Halderman revealed that merely holding down the shift key on a Windows PC would render SunnComm's copy protection technology ineffective. Furious company executives then threatened legal action.[32] Although the company quickly retreated from its threats in the face of public outcry and negative press attention, the controversy again reminded security researchers of their vulnerability to legal threats for simply publishing the results of their research on DRM.

Since the rootkit scandal, evidence has been uncovered suggesting that other DRM technologies have introduced similar security vulnerabilities. For example, Microsoft admitted last year that Macrovision's SafeDisc DRM, widely used for video games and shipped pre-installed with nearly every copy of Windows XP and Windows 2003 operating systems, could allow attackers to "read or write any area of the hard disk or memory of the PC, thus facilitating the complete compromise of the security. . ."[33] And there have been several reports that SecuROM, used on popular video games such as Spore, disables firewalls and other security mechanisms.[34]

[28] N. Ulaby, "Sony Music CDs Under Fire from Privacy Advocates," NPR Morning Edition (Nov. 4, 2005).

[29] D. Mitchell, "No Shortage of Worries" New York Times (Sept. 1, 2007).

[30] *See* Sony BMG Litigation Info, Electronic Frontier Foundation.

[31] J. Borland, "Student faces suit over key to CD locks," CNET News (Oct. 9, 2003).

[32] *Id.*

[33] Comment, J. Alex Halderman, In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, U.S. Copyright Office Docket No. RM 2008-8, p 5 n19

[34] *Id.*

B. More Unpleasant Surprises

In 2008, three music services (MSN, Yahoo! Music and Walmart Music) told customers that they would be shutting down their DRM servers.[35] Once those servers were shuttered, consumer who had bought music from those services would no longer be able to transfer those songs to "unauthorized computers," or access the songs after changing operating systems. All three services advised customers to back up their music to a CD if they wanted to be able to access it in the future. In other words, the services invited their customers to invest more time, labor and money in order to continue to enjoy the music for which they have already paid. When consumers protested, MSN Music decided to delay its shutdown until 2011 and Walmart decided to delay indefinitely.[36] Yahoo! Music decided to go ahead, but offered to compensate customers damaged by the cutoff.[37] These were good outcomes, for now, but the problem will persist as long as customers must depend on vendors' support for (already outdated) DRM technology to be able to listen to legally purchased media.

Nor is the problem confined to music. On January 30, 2009, the servers that support the DRM on approximately 300,000 electronic books sold by Fictionwise went dark, meaning consumers will no longer be able to download books they paid for.[38] Epic Games, for its part, has offered a unique twist to the "end-date" scenario: the digital certificate required for its "Gears of War" game to run on a PC was set to expire on January 28, 2009 (less than three years after the game was released). As a result, on January 29, 2008, gamers whose computer clocks were accurate found that they could no longer play the game they had paid for. Gamers with pirated copies did not face this problem.

Region-coding DRM imposes comparable restrictions on unwary customers. Consumers expect to be able to make normal uses of physical copies of entertainment products in any country, so long as they can access a player. But an American who buys a perfectly legal DVD while traveling in France will be unable to play that DVD when she gets home because it is flagged to play only on European DVD players. By the same token, an American cannot bring her DVD collection with her to keep herself entertained during a temporary work assignment abroad—unless she wants to bring her American DVD player as well.

[35] G. Sandoval, "Wal-Mart Reversal Teaches Us the Masses Have Spoken," CNET News (Oct. 10, 2008).

[36] *Id.*

[37] G. Sandoval, "Yahoo Music To Offer Refunds, What About MSN?," CNET News (Jul. 28, 2008).

[38] Fictionwise, Inc. "Expiring Download and eReader Replacement FAQ, Fictionwise.com [Accessed 01.28.2009]

Sometimes the unexpected restrictions come buried in the EULA that accompanies the DRM. For example, the EULA that accompanied Sony BMG's XCP and MediaMax copy protection systems[39] included these restrictions:

- No right to play music on a work computer. Consumers could play the music they bought only on a "personal home computer system owned by [them]."
- No right to bring music abroad. The EULA specifically forbade "export" outside the consumer's country of residence.
- No right to refuse updates. The EULA immediately terminated if a customer failed to install any update. No more holding out on those hobble-ware downgrades masquerading as updates.
- No right to manage the desktop. The EULA gave Sony-BMG the right to install and use backdoors in the copy protection software or media player to "enforce their rights" against consumers, at any time, without notice. And Sony-BMG disclaimed any liability if this "self help" crashed its customers' computers, exposed consumers to security risks, or caused any other harm.
- No right to full compensation for harm. The EULA limited Sony-BMG's liability to $5.00—less than the cost of the CD.
- Limited first sale protection. The EULA forbade transferring the music on a consumer's computer, even along with the original CD.
- No fair use. The EULA forbade changing, altering, or make derivative works from the music on the customer's computer, and also forbade reverse engineering. Of course, reverse engineering by independent researchers is exactly how the deep flaws in the technology were exposed in the first place.

C. <u>Restrictions on Fair Use</u>

1. Personal Uses

CD copy-protection technologies interfere with the fair use expectations of music fans by inhibiting the transfer of music from CD to iPods or other MP3 players—despite the fact that making an MP3 copy of a CD for personal use qualifies as a fair use. Other fair uses impaired by copy-protection technologies include making "mix CDs" or making copies of a CD for the office or car. Unfortunately, companies that distribute tools to "repair" these dysfunctional CDs, restoring to consumers their fair use privileges, run the risk of lawsuits under the DMCA's ban on circumvention tools and technologies. As for online music, DRM can prevent a consumer from such clear fair uses as moving song from one

[39] *See* <u>Exhibit A</u>, Class Action Complaint, *Melcon v. Sony BMG et al*, N.D.Cal. Case No 05-5084, filed Dec. 8, 2005.

MP3 player to another, or creating a backup of the digital file.

The bigger problem going forward, however, is the movie industry's continuing use of encryption on DVDs, which has curtailed consumers' ability to make legitimate, personal-use copies of movies they have purchased. Indeed, there are many legitimate reasons to copy DVDs. Once the video is on a PC, lots of fair uses become possible—for example, video creators can remix movie clips into original YouTube videos, travelers can load the movie into their laptops, and DVD owners can skip the otherwise "unskippable" commercials that preface certain films. DRM prevents these uses. More precisely, DRM impedes such uses for those who don't have the time, skill, and/or nerve to use any of the numerous software tools that break or avoid that DRM. The tools are there, but they can't be used without risk of litigation.

Movie fans, film scholars, movie critics, and public interest groups have all repeatedly asked the Copyright Office to grant DMCA exemptions to allow the decryption of DVDs in order to enable noninfringing uses. For example, exemptions were 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.[40] In 2006, a very narrow exemption was granted to allow media studies and film professors to create compilations of motion pictures for educational use in the classroom.[41] The narrowness of this exemption suggests future exemptions may only be granted if constraints can be placed on both the type of use and class of user—two heavy shackles on fair use.

2. Time-shifting and Streaming Media

As more people receive audio and video content from "streaming" Internet media sources, they will want tools to preserve their settled fair use expectations, including the ability to "time-shift" programming for later listening or viewing. As a result of the DMCA, however, the digital equivalents of VCRs and cassette decks for streaming media may never arrive.

Start-up software company Streambox developed exactly such a product. Known simply as the Streambox VCR, it was designed to time-shift streaming media.[42] But when RealNetworks discovered that the Streambox VCR could time-shift streaming RealAudio

[40] *See, e.g.*, Comments of the Electronic Frontier Foundation and Public Knowledge, *In re Exemption to Prohibition on Circumvention of Copyright Protections Systems for Access Control Technologies Copyright Office*, Docket No. RM 2002-4

[41] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,474 (Nov. 27, 2006).

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

webcasts, it invoked the DMCA and obtained an injunction against the new product.[43]

The DMCA was also invoked to threaten the developer of an open source, noncommercial software application known as Streamripper that records MP3 audio streams for later listening.[44]

V. The Costs of DRM Far Outweigh the Benefits

The burdens of DRM for consumers and competition are clear. What makes the burdens outrageous is that DRM is not even very effective at stopping unauthorized copying.

For example, when the long-anticipated PC game Spore was released, fans were outraged to find that the game software installed a separate program called SecuROM that was intended to prevent copying. The scheme backfired: not only had unauthorized copies of the game *already* been released before the launch date, many buyers protested by quickly posting cracked versions of the game. Spore soon became the most pirated game on the Internet — no surprise, since most new games are available almost immediately for free over P2P sites.[45] The game publisher, Electronic Arts, now faces a class action lawsuit based on its alleged failure to fully disclose the nature and effects of the SecuROM technology.[46]

To take another prominent example, in mid-2008, Warner Brothers mounted a very public campaign to prevent the circulation of unauthorized copies of *The Dark Knight*. Yet by the end of 2008, over seven million unauthorized copies had been downloaded.[47] Indeed, a 2008 report found that over 1/3 of U.S. residents copied DVDs, and technologies to facilitate that copying (like Handbrake, DVD Shrink, and MacTheRipper) are routinely reviewed in the mainstream press.[48] Even the supposedly unbreakable Blu-ray and DVD-HD DRM was easily cracked — twice in 2008 — by SlySoft. [49] And, DRM has done nothing to stop one major source of DVD-quality unauthorized copies: Academy screeners.[50] Thanks to all of these sources, a recent report found that high-

[43] *Id.*

[44] Cease and desist letter from Kenneth Plevan on behalf of Live365.com to John Clegg, developer of Streamripper, April 26, 2001.

[45] *See* J. Lee, "Spore Most Pirated Game Ever," Game Industry, Aug. 12, 2008; E. Schonfeld, "Spore and the Great DRM Backlash," Washington Post, Sept. 14, 2008.

[46] J. Guevin, EA Hit with Class Action Over Spore Sept. 24, 2008.

[47] B. Stelter and B. Stone, Digital Pirates Winning Battle with Studios, N.Y. Times, Feb 4. 2009

[48] J. Cheng, "Breaking the Law: One third of U.S. Residents Rip DVDs," Ars Tecnica, July 8, 2008; D. Frakes, Handbrake 0.9.0, MacWorld, Dec 21, 2006.

[49] G. Halfacre, "Sly Soft: Blu-Ray fully cracked" Bit-Tech.net (Dec. 31 2008).

[50] A. Baio, Pirating the Oscars, Waxy.org, Jan. 22, 2009 (updated Feb 3, 2009)

quality, unauthorized copies of 23 out of 26 2009 Oscar nominated movies were already available online on the day the nominations were announced.[51]

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 competing with the darknet, you must compete on the darknet's own terms: that is convenience and low cost rather than additional security.[52]

Nor is this effect confined to music. For example, gamers got a strong message about the benefits of unauthorized (i.e., DRM-free) copies of games when they learned that players who use pirated copies of Gears of War (see Section III.B, above) were *not* cut off from play due to the expiration date that was built into the DRM of the legally purchased copies.

The increasing abandonment of DRM for music demonstrates that the music industry, at least, has recognized that you can't use DRM to compete with the darknet. Here are a few reasons why: Burning and exchanging CDs among friends is commonplace.[53] In fact, 20% of downloaders have copied files directly off another's MP3 player.[54] In Britain, the average teenager has over 800 illegally copied songs on their digital music player, mostly copied from friends. Furthermore, the cost of digital storage media is

[51] *Id.*

[52] Petter Biddle, Paul England, Marcus Peinado, and Bryan Willman, "The Darknet and the Future of Content Distribution" Microsoft Corporation (2002).

[53] Dan Sabbagh, "Average Teenager iPod has 800 Illegal Music Tracks" TimesOnline (Jun. 16, 2008)

[54] Mary Madden and Lee Rainie, "Pew Internet Project Data Memo, RE: Music and Video Downloading Moves Beyond P2P," *Pew Internet & American Life Project*, March 2005.

falling rapidly, while capacity has risen substantially in the past few years. Blu-Ray's recordable formats, BD-R and BD-RE, are capable of storing between 25 and 50 GB per disc, for which PC-based burners have been available since July 2006.[55] Hard drives also continue to fall in price and expand in capacity. As of January 2009, a 1-terabyte drive can be had for about $100, offering music fans the ability to collect and share extremely large music collections from and among their extended circle of friends and acquaintances.[56] USB flashdrives, which now offer for a few dollars as much capacity as the first-generation iPod did in 2001, provide another convenient means for quickly sharing files.

VI. Conclusion

DRM technologies *don't* stop copyright infringement. They *do* impede innovation and thwart traditional consumer rights and expectations. Thus, as long as entertainment companies and their partners continue to use DRM, the FTC should take the following steps to limit DRM's harmful effects.

- Investigate DRM's effect on competition, and particularly if DRM is used primarily to hinder competition rather than hindering unauthorized copyright and distribution. The investigation should pay close attention to the activities of inter-industry consortia such as AACS and DVD-CCA.

- Investigate whether the effects of DRM are fully disclosed to consumers.

- Promulgate a "Best Practices for DRM" that would include at least these elements:

    - Full disclosure of DRM prior to sale or any product that contains it, including an explanation of the specific acts the DRM will restrict and how the DRM will interact with a consumer's computer (e.g., will it install automatically and, if so, can it be easily uninstalled?) and, if applicable, what information the DRM may allow the source(s) of the product to obtain about the purchaser.

    - Elimination of language from EULAs that would restrict fair use, first sale, forbid taking the product abroad, penalize consumers for failing to install updates, and/or require consumers to allow the manufacturer to access his or her computer without further notice or permission.

    - If personal information is collected in the course of the operation of any DRM technology, that information should be destroyed by the recipient as

[55] *See, e.g.* Philips Blu-Ray BD-R Disc in Jewel Case, Supermediastore.com [Accessed 01.28.2009]

[56] *See, e.g.*, Amazon.com: Western Digital My Book Essential Edition 1 TB USB 2.0 External Hard Drive. Amazon. [Accessed 01.28.2009]

soon as practicable, but no later than one month from the date the information is no longer necessary for the purpose for which it was collected, unless there is a pending subpoena or other legally enforceable request for such information.

  - Submission of DRM technologies for independent security testing before those technologies are embedded in any product sold to consumers.

- Issue an opinion statement to the effect that any restriction on fair use, first sale, taking the product abroad, or failing to install updates is substantively unconscionable.

These measures will not prevent the harm caused by DRM, but they may help alleviate the myriad burdens DRM imposes on consumers and competition until DRM's proponents abandon these fatally flawed technologies.

Respectfully submitted,

/s/

____
Corynne McSherry
Staff Attorney
ELECTRONIC FRONTIER FOUNDATION

FTC TOWN HALL: DIGITAL RIGHTS MANAGEMENT TECHNOLOGIES

Comment: Project No. P094502

APPENDIX to Comments Submitted by the Electronic Frontier Foundation

February 9, 2009

APPENDIX A

ELECTRONIC FRONTIER FOUNDATION

Unintended Consequences:

Ten Years under the DMCA

This document collects reported cases where the anti-circumvention provisions of the DMCA have been invoked not against pirates, but against consumers, scientists, and legitimate competitors. It will be updated from time to time as additional cases come to light. The latest version can always be obtained at www.eff.org.

1. Executive Summary

Since they were enacted in 1998, the "anti-circumvention" provisions of the Digital Millennium Copyright Act ("DMCA"), codified in section 1201 of the Copyright Act, have not been used as Congress envisioned. Congress meant to stop copyright infringers from defeating anti-piracy protections added to copyrighted works and to ban the "black box" devices intended for that purpose.[1]

In practice, the anti-circumvention provisions have been used to stifle a wide array of legitimate activities, rather than to stop copyright infringement. As a result, the DMCA has developed into a serious threat to several important public policy priorities:

The DMCA Chills Free Expression and Scientific Research.

Experience with section 1201 demonstrates that it is being used to stifle free speech and scientific research. The lawsuit against *2600* magazine, threats against Princeton Professor Edward Felten's team of researchers, and prosecution of Russian programmer Dmitry Sklyarov have chilled the legitimate activities of journalists, publishers, scientists, students, programmers, and members of the public.

The DMCA Jeopardizes Fair Use.

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 the public's fair use rights. Already, the movie industry's use of encryption on DVDs has curtailed consumers' ability to make legitimate, personal-use copies of movies they have purchased.

The DMCA Impedes Competition and Innovation.

Rather than focusing on pirates, some have wielded the DMCA to hinder legitimate competitors. For example, the DMCA has been used to block aftermarket competition in laser printer toner cartridges, garage door openers, and computer maintenance services. Similarly, Apple invoked the DMCA to chill RealNetworks' efforts to sell music downloads to iPod owners.

The DMCA Interferes with Computer Intrusion Laws.

Further, the DMCA has been misused as a general-purpose prohibition on computer network access, a task for which it was not designed and to which it is ill-suited. As a result, a disgruntled employer has used the DMCA against a former contractor for simply connecting to the company's computer system through a VPN.

2. DMCA Legislative Background

Congress enacted the DMCA's anti-circumvention provisions in response to two pressures. First, Congress was responding to the perceived need to implement obligations imposed on the U.S. by the 1996 World Intellectual Property Organization (WIPO) Copyright Treaty. Section 1201, however, went further than the WIPO treaty required.[2] The details of section 1201, then, were a response not just to U.S. treaty obligations, but also to the concerns of copyright owners that their works would be widely pirated in the networked digital world.[3]

Section 1201 contains two distinct prohibitions: a ban on ***acts*** of circumvention, and a ban on the ***distribution of tools and technologies*** used for circumvention.

The "act" prohibition, set out in section 1201(a)(1), prohibits the act of circumventing a technological measure used by copyright owners to control access to their works ("access controls"). So, for example, this provision makes it unlawful to defeat the encryption system used on DVD movies. This ban on acts of circumvention applies even where the purpose for decrypting the movie would otherwise be legitimate. As a result, the motion picture industry maintains that it is unlawful to make a digital copy ("rip") of a DVD you own for playback on your iPod.

The "tools" prohibitions, set out in sections 1201(a)(2) and 1201(b), outlaw the manufacture, sale, distribution, or trafficking of tools and technologies that make circumvention possible. These provisions ban both technologies that defeat *access* controls, and also technologies that defeat use restrictions imposed by copyright owners, such as *copy controls.* These provisions prohibit the distribution of "DVD back-up" software, for example.

Section 1201 includes a number of exceptions for certain limited classes of activities, including security testing, reverse engineering of software, encryption research, and law enforcement. These exceptions have been extensively criticized as being too narrow to be of real use to the constituencies who they were intended to assist.[4]

A violation of any of the "act" or "tools" prohibitions is subject to significant civil and, in some circumstances, criminal penalties.

3. Chilling Free Expression and Scientific Research

Section 1201 has been used by a number of copyright owners to stifle free speech and legitimate scientific research.

The lawsuit against *2600* magazine, threats against Professor Edward Felten's team of researchers, and prosecution of the Russian programmer Dmitry Sklyarov are among the most widely known examples of the DMCA being used to chill speech and research. Bowing to DMCA liability fears, online service providers and bulletin board operators have censored discussions of copy-protection systems, programmers have removed computer security programs from their websites, and students, scientists and security experts have stopped publishing details of their research.

These developments will ultimately result in weakened security for all computer users (including, ironically, for copyright owners counting on technical measures to protect their works), as security researchers shy away from research that might run afoul of section 1201.

DMCA Delays Disclosure of Sony-BMG "Rootkit" Vulnerability

J. Alex Halderman, a graduate student at Princeton University, discovered the existence of several security vulnerabilities in the CD copy-protection software on dozens of Sony-BMG titles. He delayed publishing his discovery for several weeks while consulting with lawyers in order to avoid DMCA pitfalls. This left millions of music fans at risk longer than necessary.[5] 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 risks created by the DMCA.

Security researchers had sought a DMCA exemption in 2003 in order to facilitate research on dangerous DRM systems like the Sony-BMG rootkit, but their request was denied by the U.S. Copyright Office.[6] In 2006, the Copyright Office granted an exemption to the DMCA for researchers examining the security threat posed by copy protection software on compact discs.[7] This exemption, however, does nothing to protect researchers studying other DRM systems.

Cyber-Security Czar Notes Chill on Research

Speaking at MIT in October 2002, White House Cyber Security Chief Richard Clarke called for DMCA reform, noting his concern that the DMCA had been used to chill legitimate computer security research. The *Boston Globe* quoted Clarke as saying, "I think a lot of people didn't realize that it would have this potential chilling effect on vulnerability research."[8]

Professor Felten's Research Team Threatened

In September 2000, 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 grudgingly withdrew their paper from the conference. The threat was ultimately withdrawn and a portion of the research was published at a subsequent conference, but only after the researchers filed a lawsuit.

After enduring this experience, at least one of the researchers involved has decided to forgo further research efforts in this field.[9]

SunnComm Threatens Grad Student

In October 2003, Princeton graduate student J. Alex Halderman was threatened with a DMCA lawsuit after publishing a report documenting weaknesses in a CD copy-protection technology developed by SunnComm. Halderman revealed that merely holding down the shift key on a Windows PC would render SunnComm's copy protection technology ineffective. Furious company executives then threatened legal action.

The company quickly retreated from its threats in the face of public outcry and negative press attention. Although Halderman was spared, the controversy again reminded security researchers of their vulnerability to DMCA threats for simply publishing the results of their research.[10]

Hewlett Packard Threatens SNOsoft

Hewlett-Packard resorted to DMCA threats when researchers published a security flaw in HP's Tru64 UNIX operating system. The researchers, a loosely-organized collective known as Secure Network Operations ("SNOsoft"), received the DMCA threat after releasing software in July 2002 that demonstrated vulnerabilities that HP had been aware of for some time, but had not bothered to fix.

After widespread press attention, HP ultimately withdrew the DMCA threat. Security researchers got the message, however—publish vulnerability research at your own risk.[11]

Blackboard Threatens Security Researchers

In April 2003, educational software company Blackboard Inc. used a DMCA threat to stop the presentation of research on security vulnerabilities in its products at the InterzOne II conference in Atlanta. Students Billy Hoffman and Virgil Griffith were scheduled to present their research on security flaws in the Blackboard ID card system used by university campus security systems but were blocked shortly before the talk by a cease-and-desist letter invoking the DMCA.

Blackboard obtained a temporary restraining order against the students and the conference organizers at a secret "ex parte" hearing the day before the conference began, giving the students and conference organizer no opportunity to appear in court or challenge the order before the scheduled presentation. Despite the rhetoric in its initial cease and desist letter, Blackboard's lawsuit did not mention the DMCA. The invocation in the original cease-and-desist letter, however, underscores the way the statute has been used to chill security research.[12]

Xbox Hack Book Dropped by Publisher

In 2003, U.S. publisher John Wiley & Sons dropped plans to publish a book by security researcher Andrew "Bunnie" Huang, citing DMCA liability concerns. Wiley had commissioned Huang to write a book that described the security flaws in the Microsoft Xbox game console, flaws Huang had discovered as part of his doctoral research at M.I.T.

Following Microsoft's legal action against a vendor of Xbox "mod chips" in early 2003, and the music industry's 2001 DMCA threats against Professor Felten's research team, Wiley dropped the book for fear that the book might be treated as a "circumvention device" under the DMCA. Huang's initial attempt to self-publish was thwarted after his online shopping cart provider also withdrew, citing DMCA concerns.

After several months of negotiations, Huang eventually self-published the book in mid-2003. After extensive legal consultations, Huang was able to get the book published by No Starch Press.[13]

Censorware Research Obstructed

Seth Finkelstein conducts research on "censorware" software (i.e., programs that block websites that contain objectionable material), documenting flaws in such software. Finkelstein's research, for example, revealed that censorware vendor N2H2 blocked a variety of legitimate websites, evidence that assisted the ACLU in challenging a law requiring the use web filtering software by federally-funded public libraries.[14]

N2H2 claimed that the DMCA should block researchers like Finkelstein from examining its software. Finkelstein was ultimately forced to seek a DMCA exemption from the Librarian of Congress, who granted the exemption in both the 2000 and 2003 triennial rulemakings. The exemption, however, was not renewed in 2006, leaving future researchers without protection from DMCA threats.[15]

Benjamin Edelman has also conducted extensive research into flaws in various censorware products. Edelman's research also led to evidence used by the ACLU in its constitutional challenge to the Children's Internet Protection Act (CIPA), which mandates the use of censorware by public libraries.

In the course of his work for the ACLU, Edelman discovered that the DMCA might interfere with his efforts to learn what websites are blocked by censorware products. Because he sought to create and distribute software tools to enable others to analyze the list if it changed, Edelman could not rely on the limited DMCA regulatory exception in place at the time. Unwilling to risk civil and criminal penalties under Section 1201, Edelman was forced to sue to seek clarification of his legal rights. Unfortunately, the court found that Edelman would have to undertake the research and hazard legal reprisals in order to have standing to challenge the DMCA. The case was therefore dismissed without addressing the DMCA's chill on research.[16]

Dmitry Sklyarov Arrested

In July 2001, Russian programmer Dmitry Sklyarov was jailed for several weeks and detained for five months in the United States after speaking at the DEFCON conference in Las Vegas.

Prosecutors, prompted by software goliath Adobe Systems Inc., alleged that Sklyarov had worked on a software program known as the Advanced e-Book Processor, which was distributed over the Internet by his Russian employer, ElcomSoft. The software allowed owners of Adobe electronic books ("e-books") to convert them from Adobe's e-Book format into PDF files, thereby removing restrictions embedded into the files by e-book publishers.

Sklyarov was never accused of infringing any copyright, nor of assisting anyone else to infringe copyrights. His alleged crime was working on a software tool with many legitimate uses, simply because other people *might* use the tool to copy an e-book without the publisher's permission.

Federal prosecutors ultimately permitted Sklyarov to return home, but brought criminal charges against ElcomSoft. In December 2002, a jury acquitted Elcomsoft of all charges, completing an 18-month ordeal for the wrongly-accused Russian software company.[17]

Scientists and Programmers Withhold Research

Following the Felten and Sklyarov incidents, a number of prominent computer security experts curtailed their legitimate research activities for fear of potential DMCA liability.

For example, when Dutch cryptographer and security systems analyst Niels Ferguson discovered a major security flaw in Intel's HDCP video encryption system, he declined to publish his results on his website on the grounds that he travels frequently to the U.S. and is fearful of "prosecution and/or liability under the U.S. DMCA law."[18]

Following the arrest of Dmitry Sklyarov, Fred Cohen, a professor of digital forensics and respected security consultant, removed his "Forensix" evidence-gathering software from his website, citing fear of potential DMCA liability. Another respected network security protection expert, Dug Song, also removed information from his website for the same reason. Mr. Song is the author of several security papers, including a paper describing a common vulnerability in many firewalls.[19]

In mid-2001 an anonymous programmer discovered a vulnerability in Microsoft's proprietary e-book DRM system, but refused to publish the results, citing DMCA liability concerns.[20]

Foreign Scientists Avoid U.S.

Foreign scientists have expressed concerns about traveling to the U.S. following the arrest of Russian programmer Dmitry Sklyarov. Some foreign scientists have advocated boycotting conferences held in the United States, and some conference organizers have decided to hold events in non-U.S. locations. In 2001, Russia went so far as to issue a travel advisory to Russian programmers traveling to the United States.[21]

Highly respected British Linux programmer Alan Cox resigned from the USENIX committee of the Advanced Computing Systems Association, the committee that organizes many of the U.S. computing conferences, because of concerns about traveling to the United States. He also urged USENIX to move its annual conference offshore.[22]

The International Information Hiding Workshop Conference, the conference at which Professor Felten's team intended to present its original SDMI watermarking paper, chose to break with tradition and held its next conference outside of the U.S. following the DMCA threat to Professor Felten and his team.[23]

IEEE Wrestles with DMCA

The Institute of Electrical and Electronics Engineers (IEEE), which publishes 30 per cent of all computer science journals worldwide, has also grappled with the uncertainties created by the DMCA. Apparently concerned about possible DMCA liability, the IEEE in November 2001 instituted a policy requiring all authors to indemnify IEEE for any liabilities incurred should a submission result in legal action.

After an outcry from IEEE members, the organization ultimately revised its submission policies, removing mention of the DMCA. According to Bill Hagen, manager of IEEE Intellectual Property Rights, "The Digital Millennium Copyright Act has become a very sensitive subject among our authors. It's intended to protect digital content, but its application in some specific cases appears to have alienated large segments of the research community."[24]

2600 Magazine Censored

The *Universal City Studios* v. *Reimerdes* case illustrates the chilling effect that section 1201 has had on the freedom of the press.

In that case, eight major motion picture companies brought DMCA claims against *2600* Magazine seeking to block it from publishing DeCSS, a software program that defeats the CSS encryption used on DVD movies. *2600* had made the program available on its web site in the course of its ongoing coverage of the controversy surrounding the DMCA. The magazine was not involved in the development of software, nor was it accused of having used the software for any copyright infringement.

Notwithstanding the First Amendment's guarantee of a free press, the district court permanently barred *2600* from publishing, or even linking to, the DeCSS software code. In November 2001, the Second Circuit Court of Appeals upheld the lower court decision.[25]

In essence, the movie studios effectively obtained a "stop the presses" order banning the publication of truthful information by a news publication concerning a matter of public concern—an unprecedented curtailment of well-established First Amendment principles.[26]

CNET Reporter Feels Chill

CNET News reporter Declan McCullagh confronted the chilling effect of the DMCA firsthand. In the course of his reporting, he found four documents on the public website of the U.S. Transportation Security Administration (TSA). The website disclosed that the documents contained information about airport security procedures, the relationship between federal and local police, and a "liability information sheet." A note on the site stated that this "information is restricted to airport management and local law enforcement." The documents were distributed in encrypted form and a password was required to open and read them.

McCullagh obtained the passwords from an anonymous source, but did not open the documents, citing concerns that using a password without authorization might violate the DMCA.[27] This is particularly ironic, as any foreign journalist beyond the reach of the DMCA would be free to use the password.

"Journalists traditionally haven't worried about copyright law all that much," said McCullagh, "But nowadays intellectual property rights have gone too far, and arguably interfere with the newsgathering process."[28]

Microsoft Threatens Slashdot

In spring 2000, Microsoft invoked the DMCA against the Internet publication forum Slashdot, demanding that forum moderators delete materials relating to Microsoft's proprietary implementation of an open security standard known as Kerberos.

In the Slashdot forum, several individuals alleged that Microsoft had changed the open, non-proprietary Kerberos specification in order to prevent non-Microsoft servers from interacting with Windows 2000. Many speculated that this move was intended to force users to purchase Microsoft server software. Although Microsoft responded to this criticism by publishing its Kerberos specification, it conditioned access to the specification on agreement to a "click-wrap" license agreement that expressly forbade disclosure of the specification without Microsoft's prior consent.

Slashdot posters responded by republishing the Microsoft specification. Microsoft then invoked the DMCA, demanding that Slashdot remove the republished specifications.

In the words of Georgetown law professor Julie Cohen, "If Microsoft's interpretation of the DMCA's ban on circumvention technologies is right, then it doesn't seem to matter much whether posting unauthorized copies of the Microsoft Kerberos specification would be a fair use. A publisher can prohibit fair-use commentary simply by implementing access and disclosure restrictions that bind the entire public. Anyone who discloses the information, or even tells others how to get it, is a felon."[29]

GameSpy Menaces Security Researcher with DMCA

Luigi Auriemma, an independent Italian security researcher, attracted the attention of GameSpy's lawyers after publishing details on his website regarding security vulnerabilities in GameSpy's online services, including a voice chat program, Roger Wilco, and online game finder, GameSpy 3D. Before publishing the information, Auriemma had informed GameSpy and public security mailing lists of the weaknesses. GameSpy, however, had failed to address the vulnerabilities.

In November 2003, GameSpy's lawyers sent a cease and desist letter to Auriemma, threatening civil and criminal penalties under the DMCA. According to GameSpy, Auriemma was publishing key generators and other piracy tools, rather than simply vulnerability research. Whatever the merits of GameSpy's claims, the invocation of the DMCA was likely improper in light of the fact that Auriemma resides in Italy and thus is beyond the reach of the DMCA.[30]

AVSforum.com Censors TiVo Discussion

The specter of DMCA litigation has chilled speech on smaller web bulletin boards, as well. In June 2001, for example, the administrator of AVSforum.com, a popular forum where TiVo digital video recorder owners discuss TiVo features, censored all discussion about a software program that allegedly permitted TiVo users to move video from their TiVos to their personal computers. In the words of the forum administrator, "My fear with this is more or less I have no clue what is a protected system on the TiVo box under copyright (or what-have-you) and what is not. Thus my fear for the site."[31]

Mac Forum Censors iTunes Music Store Discussion

Macintosh enthusiast website Macosxhints censored publication of information about methods for evading the copy protection on songs purchased from the Apple iTunes Music Store in May 2003, citing DMCA liability concerns. Songs purchased from the Apple iTunes Music Store are downloaded in Apple's proprietary AAC file format, wrapped in digital copy protection. As the webmaster for the site noted, even though information on bypassing the copy protection was readily available on the Internet at the time, republishing user hints on work-arounds risked attracting a DMCA lawsuit and harsh penalties.[32]

4. Fair Use Under Siege

"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, such as using a VCR to record a television program for later viewing. Fair use also includes activities undertaken for purposes such as criticism, comment, news reporting, teaching, scholarship or research.

We are entering an era where books, music and movies will increasingly be "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.

The DMCA, however, prohibits the creation or distribution of these tools, even if they are crucial to fair use. So, as copyright owners use technology to press into the 21st century, the public will see fair uses whittled away by digital locks allegedly intended to "prevent piracy." Perhaps more importantly, **future fair uses will not be developed** for restricted media, 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.

Copyright owners argue that these tools, in the hands of copyright infringers, can result in "Internet piracy." But banning the tools that enable fair use will punish the innocent along with infringers. Photocopiers, VCRs, and CD-R burners can also be misused, but no one would suggest that the public give them up simply because they might be used by others to break the law.

Although the Copyright Office is empowered to grant limited DMCA exemptions in a triennial rule-making, it has repeatedly refused to grant exemptions for consumer fair uses.[33]

Copy-protected CDs & DRM in Online Music

"Copy-protected" CDs and digital rights management (DRM) for online music illustrate the collision between fair use and the DMCA in the music world. As of early 2006, for instance, Sony-BMG had released more than 15 million copy-protected CDs in the U.S. market. Although the momentum toward universal CD copy-protection faltered after the Sony-BMG "rootkit" scandal in late-2005, no major label has publicly renounced the use of copy-protection on CDs.

Such CD copy-protection technologies interfere with the fair use expectations of music fans by inhibiting the transfer of music from CD to iPods or other MP3 players—despite the fact that making an MP3 copy of a CD for personal use qualifies as a fair use. Other fair uses impaired by copy-protection technologies include making "mix CDs" or making copies of a CD for the office or car. Unfortunately, companies that distribute tools to "repair" these dysfunctional CDs, restoring to consumers their fair use privileges, run the risk of lawsuits under the DMCA's ban on circumvention tools and technologies.[34]

With the increasing popularity of online music, DRM has become an increasingly well-known frustration to fair use expectations for digital music, just as copy-protected CDs frustrated fair use expectations for physical CDs. Bypassing DRM to shift a song from one MP3 player to another, or to create a backup of the digital file, can expose a music fan to DMCA liability, even if all of the uses would otherwise qualify as non-infringing fair uses. Although more online music vendors are abandoning DRM—because, among other things, DRM has had no effect on piracy and, in the words of one digital content manager, eliminating DRM would solve "obvious interoperability issues"[35]—DRM is nevertheless another glaring example of the DMCA putting fair use under siege.[36]

Fair Use Tools Banned: DVD Software

Fair use of DVDs has suffered thanks to DMCA lawsuits brought against DVD copying tools. There are many legitimate reasons to copy DVDs. Once the video is on the PC, for example, lots of fair uses become possible—for example, video creators can remix movie clips into original YouTube videos, travelers can load the movie into their laptops, and DVD owners can skip the otherwise "unskippable" commercials that preface certain films. Without the tools necessary to copy DVDs, however, these fair uses become impossible.

In the *Universal v. Reimerdes* case, discussed above, the court held that the DMCA bans DeCSS software. 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.[37]

Movie fans, film scholars, movie critics, and public interest groups have all repeatedly asked the Copyright Office to grant DMCA exemptions to allow the decryption of DVDs in order to enable noninfringing uses. For example, exemptions were 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.[38] In 2006, a very narrow exemption was granted to allow media studies and film professors to create compilations of motion pictures for educational use in the classroom. The narrowness of this exemption was repeatedly emphasized by the Copyright Office: "If it had not been possible to define a class of works by reference to the users or the uses made of those works, it might have been difficult for the Register to recommend an exemption for this class of works."[39] This narrowness suggests future exemptions may only be granted if constraints can be placed on both the type of use *and* class of user—two heavy shackles on fair use.

Even if other narrow exemptions are granted in the future, it is worth noting that the Copyright Office is powerless to grant an exemption to the DMCA's "tools" ban. As a result, fair users are likely to be left with fewer tools at their disposal, even if they succeed in obtaining a DMCA exemption—few companies will want to enter a market making tools that could subject them to lawsuit.

Advanced e-Book Processor and e-Books

The future of fair use for books was at issue in the criminal prosecution of Dmitry Sklyarov and Elcomsoft. As discussed above, Elcomsoft produced and distributed a tool called the Advanced e-Book Processor, which translates e-books from Adobe's e-book format to PDF. This translation process removed various restrictions (against copying, printing, text-to-speech processing, etc.) that publishers can impose on e-books.[40]

The Advanced e-Book Processor allowed those who have legitimately purchased e-books to make fair uses of their e-books, uses otherwise made impossible by the restrictions of the Adobe e-book format. For instance, the program allowed people to engage in the following fair uses:

- read the e-book on a laptop or computer other than the one on which it was first downloaded;
- continue to access the e-book in the future, if the particular technological device for which it was purchased becomes obsolete;
- print an e-book on paper;

- read an e-book on an alternative operating system such as Linux (Adobe's format works only on Macs and Windows PCs);
- have a computer read an e-book out loud using text-to-speech software, which is particularly important for visually-impaired individuals.

Time-shifting and Streaming Media

As more people receive audio and video content from "streaming" Internet media sources, they will want tools to preserve their settled fair use expectations, including the ability to "time-shift" programming for later listening or viewing. As a result of the DMCA, however, the digital equivalents of VCRs and cassette decks for streaming media may never arrive.

Start-up software company Streambox developed exactly such 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 Streambox VCR product.[41]

The DMCA has also been invoked to threaten the developer of an open source, noncommercial software application known as Streamripper that records MP3 audio streams for later listening.[42]

Agfa Monotype and Fonts

In January 2002, typeface vendor Agfa Monotype Corporation threatened a college student with DMCA liability for creating "embed," a free, open source, noncommercial software program designed to manipulate TrueType fonts.

According to the student: "I wrote embed in 1997, after discovering that all of my fonts disallowed embedding in documents. Since my fonts are free, this was silly—but I didn't want to take the time to… change the flag, and then reset all of the extended font properties with a separate program. What a bore! Instead, I wrote this program to convert all of my fonts at once. The program is very simple; it just requires setting a few bits to zero. Indeed, I noticed that other fonts that were licensed for unlimited distribution also disallowed embedding…. So, I put this program on the web in hopes that it would help other font developers as well."

Agfa Monotype nevertheless threatened the student author with DMCA liability for distributing the program. According to Agfa, the fact that embed can be used to allow distribution of protected fonts makes it contraband under Section 1201, notwithstanding the fact that the tool has many legitimate uses in the hands of hobbyist font developers.[43]

Agfa Monotype brought similar DMCA challenges against Adobe Systems for its Acrobat 5.0's FreeText Tool and Forms Tool, which allowed so-called "editable embedding." Agfa claimed that with Acrobat 5.0, the recipient of an electronic document could make use of embedded fonts to change the contents of a form field or free text annotation, thus "circumventing" the embedding bits of some of Agfa's TrueType Fonts.

Fortunately, in 2005, a federal court found that Adobe had not violated either Section 1201(a) or Section 1201(b) of the DMCA. The court noted that embedding bits do not effectively control access to a protected work and, moreover, that Acrobat 5.0 was not designed primarily to circumvent TrueType fonts.[44] Hopefully, this court ruling will discourage Agfa from making abusive DMCA threats in the future.

Load-'N-Go Space-shifting

In November 2006, movie studios wielded the DMCA to rein in Load-'N-Go, a small company that loaded DVDs purchased by a customer onto the customer's iPod. Load-'N-Go would take DVDs purchased by the customer, load the DVDs onto the customer's iPod, and then return both the iPod and the original DVDs.

The movie studios claimed this service violates the DMCA because creating a duplicate copy of the movie—even for personal, fair uses—circumvents the DVD's CSS encryption. Under this theory, any individual attempting to space-shift movies from DVD to iPod or to any other digital media player is violating the DMCA. Conveniently for movie studios, this legal posture enables them to sell consumers the same movies multiple times, for multiple devices.

After some back-and-forth in the courts, the case settled in February 2007.[45]

RealDVD Format-shifting

In October 2008, RealNetworks was forced to stop sales of its RealDVD software, designed to allow users to copy a DVD and store it on their hard drive. This format-shifting by RealDVD would empower consumers with numerous fair uses, such as allowing them to create backups, organize a movie collection digitally, and watch a DVD at any time without being tied to a physical disc. These legitimate expectations of fair use were quickly stifled by a movie studio lawsuit, commenced the same day that RealDVD launched, alleging violations of the DMCA.

RealDVD makes an exact copy of everything on a DVD—including the DVD's CSS copy-protection system—and transfers it to the hard drive of a PC. A license from the DVD Copy Control Association authorizes RealNetworks to perform the necessary DVD decryption for this process. To ensure the resulting DVD copy cannot be shared or stolen, RealDVD encrypts the saved DVDs again and tethers the copy to a limited number of PCs.

Despite these layers of protection for copyrighted content and despite the numerous fair uses for which RealDVD was designed, a temporary restraining order was granted to halt the sale of RealDVD until a further hearing in late 2008.[46]

5. A threat to innovation and competition

The DMCA has frequently been used to deter legitimate innovation and competition, rather than to stop piracy.

For example, the DMCA has been used to block aftermarket competition in laser printer toner cartridges, garage door openers, and computer maintenance services. Apple Computer invoked the DMCA to chill Real Networks' efforts to sell music downloads to iPod owners. Videogame hobbyists have been sued for trying to improve or extend the capabilities of their favorite game titles. Sony has threatened hobbyists for creating software that enables Sony's Aibo robot dog to dance, and has sued to block software that allows gamers to play their PlayStation games on PCs.

In each of these cases, it was legitimate competitors and innovators who suffered, not pirates.[47]

DMCA Used First to Lock Cell Phones to Carriers; Then, to Hammer Phone Resellers

American cellular phone subscribers have long suffered with phones that are artificially "locked" to a particular carrier's network. This creates a variety of burdens for consumers, including high roaming rates when traveling (by preventing the use of prepaid SIM chips from local carriers) and barriers to switching carriers. In addition, these restrictions make locked phones harder to recycle and reuse. "Locking" phones seems particularly unjustifiable in light of the "minimum term" and "early termination fee" clauses that guarantee carriers will recoup the costs of the phones they are so fond of "giving away" to lure subscribers.

Responding to consumer demand, phone "unlocking" services have become widespread. Unfortunately, carriers responded by threatening legal action under the DMCA and, in at least one case, filing suit. Instead of being used against copyright infringers, the DMCA was used to prop up the anticompetitive business models of cellular carriers.[48]

At the 2006 triennial DMCA rulemaking, the Copyright Office granted an exemption for cell phone unlocking. Despite this exemption, however, DMCA lawsuits persist. Tracfone, the nation's largest independent prepaid-wireless provider, aggressively uses the DMCA to sue phone resellers who purchase and unlock Tracfone handsets. Courts have ruled in favor of Tracfone, allowing the company to continue using the DMCA as a hammer against secondary markets, instead of as a deterrent against copyright infringers.[49]

Apple Threatens Real over Harmony

In July 2004, RealNetworks announced its "Harmony" technology, which was designed to allow music sold by Real's digital download store to play on Apple iPods. Until Harmony, the only DRM-restricted music format playable on the iPod was Apple's own "Fairplay" format. Although the iPod plays a variety of DRM-free formats, Real wanted to ensure interoperability without having to give up DRM restrictions, and thus developed Harmony to "re-wrap" its songs using the Fairplay format.[50]

Within days, Apple responded by accusing Real of adopting the "tactics and ethics of a hacker" and threatening legal action under the DMCA. Over the following months, the two competitors engaged in a game of technological cat-and-mouse, with Apple disabling Harmony in updates of its iTunes software and Real revising its technology to re-enable compatibility. In the words of Real's filings before the SEC: "Although we believe our Harmony technology is legal, there is no assurance that a court would agree with our position."[51]

Tecmo Sues to Block Game Enhancements

Enthusiastic fans of the videogames Ninja Gaiden, Dead or Alive 3, and Dead or Alive Xtreme Beach Volleyball managed to modify their games to create new "skins" to change the appearance of characters who appear in the game (including making some characters appear nude). The modifications were add-on enhancements for the games themselves—only those who already had the games could make use of the skins. These hobbyist tinkerers traded their modding tips and swapped skins on a website called ninjahacker.net.

Tecmo Inc., which distributes the games, was not amused and brought DMCA claims against the website operators and tinkerers who frequented it. The suit was ultimately dismissed after the website was taken down and settlements negotiated with the site's operators.[52]

Nikon's Encrypted RAW Format Blocks Adobe

In April 2005, the creator of Adobe's Photoshop revealed that camera-maker Nikon had begun encrypting certain portions of the RAW image files generated by its professional-grade digital cameras. As a result, these files would not be compatible with Photoshop or other similar software unless the developers first took licenses from Nikon. In other words, by encrypting the image files on its cameras, Nikon was obtaining market leverage in the image editing software market.

Adobe cited the prospect of a DMCA claim as one reason why it was unwilling to reverse engineer the format to facilitate interoperability. Nikon and Adobe ultimately negotiated an agreement, an option that may not be practical for smaller software developers in the future.[53]

HP's Region-Coded, Expiring Printer Cartridges

Hewlett-Packard, one of the world's leading printer manufacturers, has embedded software in its printers and accompanying toner cartridges to enforce "region coding" restrictions that prevent cartridges purchased in one region from operating with printers purchased in another. This "feature" presumably is intended to support regional market segmentation and price discrimination.

The software embedded in HP printer cartridges also apparently causes them to "expire" after a set amount of time, forcing consumers to purchase new ink, even if the cartridge has not run dry. This "feature" of HP ink cartridges has lead to at least one consumer class action against the company.

HP has not yet invoked the DMCA to protect these anti-consumer tactics, but both HP's lawyers and its competitors are doubtless well aware of ways in which the DMCA can be used to buttress these tactics.[54]

StorageTek Attempts to Block Independent Service Vendors

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.

A district court granted a preliminary injunction against Custom Hardware. More than a year later, a court of appeals vacated the injunction, holding that where there is no nexus with copyright infringement, there can be no DMCA claim. Although this was a victory for competition, it illustrates the ways in which the DMCA continues to be used to impede competition, rather than prevent piracy.[55]

Lexmark Sues Over Toner Cartridges

Lexmark, the second-largest laser printer maker in the U.S., has long tried to eliminate the secondary market in refilled laser toner cartridges. In January 2003, Lexmark employed the DMCA as a new weapon in its arsenal.

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 sent a chilling message to those in the secondary market for Lexmark cartridges.[56]

Chamberlain Sues Universal Garage Door Opener Manufacturer

Garage door opener manufacturer Chamberlain Group 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.

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 use of the DMCA was nothing less than an "attempt to leverage its sales into aftermarket monopolies."[57]

Sony Sues Connectix and Bleem

Sony has used DMCA to sue competitors who created emulation software that permits gamers to play PlayStation console games on PCs. In 1999, Sony sued Connectix, the maker of the Virtual Game Station, a PlayStation emulator for Macintosh computers. Sony also sued Bleem, the leading vendor of PlayStation emulator software for Windows PCs.

In both cases, Sony claimed that competitors had violated the DMCA by engaging in unlawful circumvention, even though the development of interoperable software has been recognized by the courts as a fair use under copyright law. Because courts have suggested that the DMCA trumps fair use, however, the DMCA has become a new legal weapon with which to threaten those who rely on reverse engineering to create competing products.

Neither Connectix nor Bleem were able to bear the high costs of litigation against Sony and pulled their products off the market. No similar emulation products have been introduced, effectively forcing gamers to use Sony console hardware if they want to play the PlayStation games they have purchased.[58]

Sony Threatens Aibo Hobbyist

Sony has also invoked the DMCA against a hobbyist who developed custom "dance moves" for his Aibo robotic "pet" dog. Developing these new routines for the Sony Aibo required reverse engineering the encryption surrounding the software that manipulates the robot. The hobbyist revealed neither the decrypted Sony software nor the code he used to defeat the encryption, but he freely distributed his new custom programs. Sony claimed that the act of circumventing the encryption surrounding the software in the Aibo violated the DMCA and demanded that the hobbyist remove his programs from his website.

Responding to public outcry, Sony ultimately permitted the hobbyist to repost some of his programs (on the understanding that Sony retained the right to commercially exploit the hobbyist's work). The incident illustrated Sony's willingness to invoke the DMCA in situations with no relationship to "piracy."[59]

Sony Attacks PlayStation "Mod Chips"

Sony has sued a number of manufacturers and distributors of "mod chips" for alleged circumvention under the DMCA. In doing so, Sony has been able to enforce a system of "region coding" that raises significant anticompetitive issues.

"Mod chips" are after-market accessories that modify Sony PlayStation game consoles to permit games legitimately purchased in one part of the world to be played on a games console from another geographical region. Sony complains that mod chips can also be used to play pirated copies of games. As noted above, it is hard to see why an independent vendor of a product with legitimate uses should have to solve Sony's piracy problems before entering the market.

Sony sued Gamemasters, distributor of the Game Enhancer peripheral device, which allowed owners of a U.S. PlayStation console to play games purchased in Japan and other countries. Although there was no infringement of Sony's copyright, the court granted an injunction under the DMCA's anti-circumvention provisions, effectively leaving gamers at the mercy of Sony's region coding system.

Interestingly, courts in Australia, recognizing the anticompetitive and anticonsumer potential of Sony's region coding system, came to a different conclusion under that country's analog to the DMCA. In *Stevens v Kabushiki Kaisha Sony Computer Entertainment*, the High Court of Australia held in 2005 that the regional access coding on Sony PlayStation computer games as implemented by the PlayStation console did not qualify for legal protection, as it did not prevent or inhibit copyright infringement.

Sony, like all vendors, is free to attempt to segregate geographic markets. If it does so, however, it should have to bear its own costs for the effort, rather than relying on the DMCA, which Congress plainly did not enact to trump the usual legal regimes governing parallel importation.[60]

Blizzard Sues bnetd.org

Vivendi-Universal's Blizzard Entertainment video game division brought a DMCA lawsuit against a group of volunteer game enthusiasts 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 own Battle.net service.

Blizzard has a policy of locking in its customers who want to play their games over the Internet—it's the Battle.net servers or nothing. Although access to Blizzard's Battle.net servers is free, the hobbyists decided to create bnetd to overcome difficulties that they had experienced in attempting to use Battle.net. The bnetd software was freely distributed, open source, and noncommercial.

Blizzard filed suit in St. Louis to bar distribution of bnetd, alleging that the software was a "circumvention device" prohibited by the DMCA. According to Blizzard, the bnetd software could be used to permit networked play of pirated Blizzard games. The developers never used the software for that purpose, nor was that the purpose for which the software was designed.

It is hard to see why a competitor should have to solve Blizzard's piracy problem before it can offer innovative products for legitimate owners of Blizzard games. Nevertheless, Blizzard prevailed on its DMCA claim, and the bnetd developers ceased distributing the software.[61]

Apple Harasses Inventive Retailer

When Other World Computing (OWC), a small retailer specializing in Apple Macintosh computers, developed a software patch in 2002 that allowed all Mac owners to use Apple's iDVD software, they thought they were doing Macintosh fans a favor. For their trouble, they got a DMCA threat from Apple.

Apple's iDVD authoring software was designed to work on newer Macs that shipped with *internal* DVD recorders manufactured by Apple. OWC discovered that a minor software modification would allow iDVD to work with *external* DVD recorders, giving owners of older Macs an upgrade path. Apple claimed that this constituted a violation of the DMCA and requested that OWC stop this practice immediately. OWC obliged.

Rather than prevent copyright infringement, the DMCA empowered Apple to force consumers to buy new Mac computers instead of simply upgrading their older machines with an external DVD recorder.[62]

Macrovision Sues Sima for Digitizing Analog Signals

In April 2006, hardware manufacturer Sima Products was forced to stop selling various video-enhancing products that digitized analog signals from DVD players and VCRs. Wielding the DMCA, Macrovision argued that Sima's analog-to-digital video enhancements circumvented Macrovision's analog copy protection (ACP).

Macrovision's ACP functions by inserting noise into the vertical blanking intervals found in analog video signals. This noise is not displayed on a television set, but it does degrade the recording made by most analog VCRs. Sima's products simply convert the analog signal into a digital signal, which eliminates additional noise in the blanking intervals, and then converts the signal back to analog. This video enhancement allows consumers to harness digital techniques to make up for a weakness in VCR analog technology, a weakness which could come from age or distortion as well as from techniques like Macrovision's.

ACP does not prevent digital copies. Moreover, when a digital copy is made, Macrovision's ACP does not survive. Accordingly, Sima's products are not "circumventing" anything by performing its analog-to-digital conversion.

Macrovision, nevertheless, was able to convince the court that Sima had violated the DMCA. This unfortunate result indicates that the DMCA can be manipulated to push obsolete analog copy protection systems onto new technology innovators.[63] Although Sima appealed the ruling, it subsequently settled with Macrovision before the appeal was heard.

Blizzard Attempts to Block World of Warcraft Glider

Blizzard, makers the popular online role-playing game World of Warcraft (WoW), sued MDY Industries, the developer of a program which enables WoW characters to continue playing even when the user is away from her computer. These "bot" programs help reduce the time that a user must otherwise spend to progress in the game. MDY's product, known as "Glider," proved to be very popular with WoW players, selling about 120,000 units.[64]

In July 2008, the court rejected several aspects of Blizzard's DMCA claim (leaving other aspects for exploration at trial, scheduled for January 2009). The court ruled that MDY's "bot" does not violate the DMCA despite the fact WoW has software known as "Warden" designed to scan and deny access to game servers if such bots are detected on a user's computer. The court reasoned that a user has full access to WoW game client software when the user buys it, and therefore the Glider software does not circumvent any access control.[65]

Although the court rejected Blizzard's DMCA claim, it upheld the copyright and contract claims against MDY.[66] Other aspect of Blizzard's DMCA claim will be tested at trial in January 2009.

Car Product Design Company Attempts to Suppres Competition with EULA

In March 2008, car product design company XPEL Technologies filed suit against American Filter Film Distributors, a rival who provides services for car paint and window film protection. Among a slew of other claims, XPEL alleged that American Filter violated the DMCA by using "Capture" software to copy product images from the XPEL website and distribute the image and product to other auto dealers. XPEL argued the DMCA was violated because (1) the XPEL website is protected by an end-user license agreement (EULA), (2) American Filter clicked that they agreed to the EULA, and (3) the EULA is a technological measure which effectively controls access to the copyrighted design works on XPEL's website. This is the first case where a "click-thru" EULA has been put forward as an access control protected by the DMCA.

In August 2008, the most recent proceedings for this case, American Filter's motion to dismiss the DMCA claim was denied. It will be worth watching this case to see whether XPEL's attempts to transform its EULA into an "access control" will succeed.[67]

6. DMCA Shoulders Aside Computer Intrusion Statutes.

The DMCA's anti-circumvention provisions have also threatened to displace "computer intrusion" and "anti-hacking" laws, something that Congress plainly never intended.

State and federal statutes already protect computer network owners from unauthorized intrusions. These include the Computer Fraud and Abuse Act (CFAA), the Wiretap Act, the Electronic Communications Privacy Act (ECPA), and a variety of state computer intrusion statutes. These statutes, however, generally require that a plaintiff prove that the intrusion caused some harm. The DMCA, in contrast, contains no financial damage threshold, tempting some to use it in place of the statutes that were designed to address computer intrusion.

Fortunately, the courts appear to be taking steps to reign in this particular misuse of the DMCA, ruling that the use of authentic usernames and passwords to access computers cannot constitute circumvention, even if done without the authorization of the computer owner.[68] Until more judicial precedents are on the books, however, the improper use of the DMCA as an all-purpose computer intrusion prohibition will continue to muddy the waters for lawyers and professionals.

Disgruntled Company Sues Former Contractor For Unauthorized Network Access

In April 2003, an automated stock trading company sued a former contract programmer under the DMCA, claiming that his access to the company's computer system over a password-protected virtual private network (VPN) connection was an act of circumvention.

Pearl Investments had employed the programmer to create a software module for its software system. In order to complete the work remotely, the programmer used a VPN to connect to the company's computers. Although the contractor created a very successful software module for the company, the relationship turned frosty after the company ran into financial difficulties and terminated the contractor's contract.

The company sued the contractor when it discovered the contractor's VPN connection to the its system, claiming electronic trespass, as well as violations of computer intrusion statutes, the CFAA, and the DMCA's anti-circumvention provisions. Pearl claimed that it had taken away the authorization it had previously given to the contractor to access its system through the password-protected VPN and that the VPN connection was therefore unauthorized. The Court rejected the company's electronic trespass and CFAA claims due to lack of evidence of any actual damage done. Even though the second server was not being used by the programmer at the time, and its hard drive had been accidentally wiped, the court agreed with Pearl that the *existence* of the VPN was a prohibited circumvention of a technological protection measure that controlled access to a system which contained copyrighted software.[69]

Ticketmaster Sues RMG for Bypassing CAPTCHA

In April 2007, Ticketmaster sued RMG Technologies under the DMCA for circumventing the Ticketmaster website CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart"), the image with distorted letters and numbers that a customer must type before purchasing a ticket. The website run by RMG Technologies provided tickets to events that were likely to sell out quickly on Ticketmaster. RMG allegedly used software to quickly make bulk purchases of tickets from Ticketmaster, circumventing the limit of four tickets per customer, in order to re-sell the tickets for profit.

Ticketmaster brought suit under the DMCA, the CFAA, the Copyright Act, breach of contract, and under California's criminal code governing computer crimes. On a motion for preliminary injunction, the court found that Ticketmaster was likely to succeed on its DMCA, Copyright Act, and breach of contract claims; however, Ticketmaster would not have been able to prevail on the CFAA claim. (The court found it did not need to address the claim under California's criminal code.)

This ruling illustrates how the DMCA has shouldered aside computer intrusion statutes like the CFAA. Because the CFAA requires that Ticketmaster prove it suffered $5,000 in damages during one year, whereas the DMCA contains no financial damage threshold, Ticketmaster was able to succeed under the DMCA while failing under the CFAA.[70]

The DMCA was not intended for this purpose. The DMCA was designed to protect copyrighted works, not ticket vendors. Although the defense made both these arguments,[71] the court nevertheless ruled in favor of Ticketmaster on the DMCA claim.[72]

Cable Provider Blocks Cable Digital Filters

In addition to computer intrusion statues, the DMCA may also be starting to shoulder aside penal statues in other industry areas.

In August 2008, cable provider CoxCom Inc. successfully forced Jon and Amy Chaffee, and their one employee, to stop selling cable digital filters at computer trade shows. These low-frequency digital filters blocked pay per view charges from being sent to cable companies, thus giving users free pay per view. Not surprisingly, the court granted summary judgment against the Chaffees for violation of the Cable Communications Policy Act, a statute specifically enacted to address theft of cable services to protect the economic viability of cable operators and cable programmers. However, the court also ruled that the Chaffees violated the DMCA.

The DMCA argument is that the Chaffees' low-frequency filters circumvent CoxCom's pay-per-view *billing mechanism*, allegedly a "technological measure" that controls access to copyrighted works. If a billing mechanism has become a "technological measure" within the meaning of the DMCA—it is troubling to think what else may qualify.[73]

7. Conclusion

Years of experience with the "anti-circumvention" provisions of the DMCA demonstrate that the statute reaches too far, chilling a wide variety of legitimate activities in ways Congress did not intend. As an increasing number of copyright works are wrapped in technological protection measures, it is likely that the DMCA's anti-circumvention provisions will be applied in further unforeseen contexts, hindering the legitimate activities of innovators, researchers, the press, and the public at large.

[1] For examples of Congress' stated purpose in enacting the DMCA's anti-circumvention provisions, *see* 144 Cong. Rec. H7093, H7094-5 (Aug. 4, 1998); Senate Judiciary Comm., S. Rep. 105-190 (1998) at 29; Judiciary Comm., H. Rep. 105-551 Pt 1 (1998) at 18; House Commerce Comm., H. Rep. 105-551 Pt 2 (1998) at 38.

[2] *See WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearing on H.R. 2281 and H.R. 2280 before the House Subcomm. on Courts and Intellectual Prop.*, 105th Cong., 1st sess. (Sept. 16, 1997) at 62 (testimony of Asst. Sec. of Commerce and Commissioner of Patents and Trademarks Bruce A. Lehman admitting that section 1201 went beyond the requirements of the WIPO Copyright Treaty).

[3] For a full description of the events leading up to the enactment of the DMCA, *see* Jessica Litman, Digital Copyright 89-150 (2000).

[4] *See* Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised*, 14 Berkeley Technology L.J. 519, 537-57 (1999) (http://www.sims.berkeley.edu/~pam/papers.html)

[5] Comment of Edward Felten and J. Alex Halderman, RM 2005-11 – Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Dec. 1, 2005, pages 6-7 (http://www.freedom-to-tinker.com/doc/2005/dmcacomment.pdf).

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

[7] 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).

[8] Jonathan Band, "Congress Unknowingly Undermines Cyber-Security," S.J. Mercury News, Dec. 16, 2002; Hiawatha Bray, "Cyber Chief Speaks on Data Network Security," Boston Globe, October 17, 2002.

[9] 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 (http://cryptome.org/sdmi-attack.htm); Felten v. RIAA: EFF Case Archive (http://www.eff.org/IP/DMCA/Felten_v_RIAA/).

[10] John Borland, "Student faces suit over key to CD locks," CNET News, Oct. 9, 2003 (http://news.com.com/Student+faces+suit+over+key+to+CD+locks/2100-1025_3-5089168.html); Declan McCullagh, "SunnComm won't sue grad student," CNET News, Oct. 10, 2003 (http://news.com.com/2100-1027-5089448.html).

[11] Declan McCullagh, "Security Warning Draws DMCA Threat," CNET News, July 30, 2002 (http://news.com.com/2100-1023-947325.html).

[12] John Borland, "Court Blocks Security Conference Talk," CNET News, April 14, 2003 (http://news.com.com/2100-1028-996836.html).

[13] David Becker, "Testing Microsoft and the DMCA," CNET News, April 15, 2003 (http://news.com.com/2008-1082-996787.html); Seth Schiesel, "Behind a Hacker's Book, a Primer on Copyright Law," N.Y. Times, July 10, 2003 (http://www.nytimes.com/2003/07/10/technology/circuits/10book.html).

[14] *Mainstream Loudoun v. Board of Trustees*, 24 F.Supp.2d 552 (E.D. Va. 1998).

[15] Jennifer 8 Lee, "Cracking the Code of Online Censorship", N. Y. Times, July 19, 2001 (http://www.nytimes.com/2001/07/19/technology/circuits/19HACK.html); Transcript of Hearing in Copyright Office Rulemaking Proceeding RM 2002-04, April 11, 2003, pages 11, 31 (http://www.copyright.gov/1201/2003/hearings/schedule.html); 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) (listing "Other Exemptions Considered, But Not Recommended").

[16] ACLU, "In Legal First, ACLU Sues Over New Copyright Law" (http://www.aclu.org/privacy/speech/15201res20020725.html).

[17] Lawrence Lessig, "Jail Time in the Digital Age," N.Y. Times, July 30, 2001, page A7. (http://www.nytimes.com/2001/07/30/opinion/30LESS.html); Lisa Bowman, "Elcomsoft Verdict: Not Guilty," CNET News, Dec. 17, 2002 (http://news.com.com/2100-1023-978176.html).

[18] Niels Ferguson, "Censorship in Action: Why I Don't Publish My HDCP Results," Aug. 15, 2001 (http://www.macfergus.com/niels/dmca/cia.html); Niels Ferguson, Declaration in Felten & Ors v R.I.A.A. case, Aug. 13, 2001 (http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_ferguson_decl.html); Lisa M. Bowman, "Researchers Weigh Publication, Prosecution," CNET News, Aug. 15, 2001 (http://news.cnet.com/news/0-1005-200-6886574.html).

[19] Robert Lemos, "Security Workers: Copyright Law Stifles," CNET News, Sept. 6, 2001 (http://news.com.com/2100-1001-272716.html).

[20] Wade Roush, "Breaking Microsoft's e-Book Code," Technology Review, November 2001, page 24.

[21] Jennifer 8 Lee, "Travel Advisory for Russian Programmers," N.Y. Times, Sept. 10, 2001, page C4 (www.nytimes.com/2001/09/10/technology/10WARN.html).

[22] Alan Cox, declaration in Felten v. RIAA, Aug. 13, 2001 (http://www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_cox_decl.html).

[23] Will Knight, "Computer Scientists Boycott US over Digital Copyright Law," New Scientist, July 23, 2001 (http://www.newscientist.com/article/dn1063.html).

[24] IEEE press release, "IEEE to Revise New Copyright Form to Address Author Concerns," April 22, 2002 (http://www.ieee.org/newsinfo/dmca.html); Will Knight, "Controversial Copyright Clause Abandoned," New Scientist, April 15, 2002 (http://www.newscientist.com/news/news.jsp?id=ns99992169).

[25] *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).

[26] 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 Net Effect: The DVD Rebellion," Technology Review, July/Aug. 2001, page 25 (http://www.simson.net/clips/2001/2001.TR.07.DVDRebellion.pdf); 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.

[27] Subsequent cases have found that using a password in similar circumstances does not violate the DMCA's circumvention ban. *See I.M.S. Inquiry Mgt. Systems v. Berkshire Info. Systems,* 307 F.Supp.2d 521 (S.D.N.Y. 2004).

[28] Declan McCullagh, "Will This Land Me in Jail?", CNET News, Dec. 23, 2002 (http://news.com.com/2010-1028-978636.html).

[29] Julie Cohen, "Call it the Digital Millennium *Censorship* Act – Unfair Use," The New Republic, May 23, 2000 (http://www.law.georgetown.edu/faculty/jec/unfairuse.html).

[30] Robert Lemos, "GameSpy Warns Security Researcher," ZDNet News, Nov. 13, 2003 (http://news.zdnet.com/2100-1009_22-5107305.html).

[31] Lisa M. Bowman, "TiVo Forum Hushes Hacking Discussion," CNET News, June 11, 2001 (http://news.cnet.com/news/0-1005-200-6249739.html).

[32] Regarding hints on evading iTunes Store copy protection, May 7, 2003 (http://www.macosxhints.com/article.php?story=20030507104823670).

[33] EFF, DMCA Triennial Rulemaking: Failing the Digital Consumer, Dec. 1, 2005 (http://www.eff.org/IP/DMCA/copyrightoffice/DMCA_rulemaking_broken.pdf).

[34] Rep. Rick Boucher, "Time to Rewrite the DMCA," CNET News, Jan. 29, 2002 (http://news.com.com/2010-1078-825335.html); Dan Gillmor, "Entertainment Industry's Copyright Fight Puts Consumers in Cross Hairs," S. J. Merc. News, Feb. 12, 2002; Jon Healey & Jeff Leeds, "Record Labels Grapple with CD Protection", L.A. Times, Nov. 29, 2002, C1; John Borland, "Copy-blocked CD Tops U.S. Charts," CNET News, June 17, 2004 (http://news.com.com/Copy-blocked+CD+tops+U.S.+charts/2100-1027_3-5238208.html).

[35] Tim Anderson, "How Apple is Changing DRM," The Guardian, May 15, 2008, Technology News, page 1 (http://www.guardian.co.uk/technology/2008/may/15/drm.apple).

[36] EFF, The Customer Is Always Wrong: A User's Guide to DRM in Online Music, (http://www.eff.org/pages/customer-always-wrong-users-guide-drm-online-music). For information on online music vendors abandoning DRM, *see* Tim Anderson, "How Apple is Changing DRM," The Guardian, May 15, 2008, Technology News, page 1 (http://www.guardian.co.uk/technology/2008/may/15/drm.apple).

[37] Matthew Mirapaul, "They'll Always Have Paris (and the Web)," N.Y. Times, March 16, 2002, page E2; 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).

[38] Recommendation of the Register of Copyrights in RM 2002-4, Oct. 27, 2003, pages 109-26 (http://www.copyright.gov/1201/docs/registers-recommendation.pdf).

[39] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 68,472, 68,474 (Nov. 27, 2006) (http://www.copyright.gov/fedreg/2006/71fr68472.pdf).

[40] EFF, Frequently Asked Questions re *U.S. v. Sklyarov* (http://www.eff.org/IP/DMCA/US_v_Sklyarov/us_v_sklyarov_faq.html).

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

[42] Cease and desist letter from Kenneth Plevan on behalf of Live365.com to John Clegg, developer of Streamripper, April 26, 2001 (http://streamripper.sourceforge.net/dc.php).

[43] Tom Murphy, "embed: DMCA Threats" (http://www.andrew.cmu.edu/~twm/embed/dmca.html); cease and desist letter from Agfa to Murphy (http://www.chillingeffects.org/copyright/notice.cgi?NoticeID=264).

[44] *See Agfa Monotype Corp. v. Adobe Sys.*, 404 F. Supp. 2d 1030 (N.D. Ill. 2005).

[45] Eric Bangeman, "MPAA Sues Over DVD-to-iPod Service," *Ars Technica*, Nov. 17, 2006 (http://arstechnica.com/news.ars/post/20061117-8241.html); Fred von Lohmann, "Movie Studios Sue to Stop Loading of DVDs onto iPods," EFF Deep Links blog, Nov. 16 2006 (http://www.eff.org/deeplinks/2006/11/movie-studios-sue-stop-loading-dvds-ipods).

[46] Ajay Kamalakaran, "U.S. Judge Halts Sales of RealNetworks DVD Software," Reuters, Oct. 9, 2008 (http://www.reuters.com/article/technologyNews/idUSTRE4982C920081009); Greg Sandoval, "Judge Keeps RealDVD Restraining Order In Place," CNET News, Oct. 7, 2008 (http://news.cnet.com/8301-1023_3-10060481-93.html); Press Release, RealNetworks, "RealNetworks Introduces RealDVD: The Best Way to Watch DVDs" (Sept. 8, 2008) (http://www.realnetworks.com/company/press/releases/2008/realdvd.html). The court filings for this case are available at EFF, "RealNetworks v. DVD-CCA (RealDVD case)" (http://www.eff.org/cases/universal-city-studios-v-realnetworks).

[47] Others have also recognized the anti-competitive effects of the DMCA. *See* Timothy B. Lee, "Circumventing Competition: The Perverse Consequences of the Digital Millennium Copyright Act," CATO Policy Analysis No. 564 (Mar. 21, 2006) (http://www.cato.org/pub_display.php?pub_id=6025).

[48] Jennifer Granick, "Free the Cell Phone!," WIRED News, Sept. 30, 2005 (http://www.wired.com/news/culture/0,1284,68989,00.html); Reply Comments of the Wireless Alliance, Copyright Office, Docket No. RM-2005-11 (http://www.copyright.gov/1201/2006/reply/14granick_WAreply.pdf).

[49] David Kravets, "Ruling Allows Cell Phone Unlocking, but Telco Sues Anyway," Wired, Aug. 8, 2007 (http://www.wired.com/politics/onlinerights/news/2007/08/tracfone). For cases brought by Tracfone against phone resellers *see, e.g. TracFone Wireless, Inc. v. Dixon*, 475 F. Supp. 2d 1236 (M.D. Fla. 2007) (ruling in favor of TracFone); *TracFone Wireless, Inc. v. GSM Group, Inc.* 555 F.Supp.2d 1331 (S.D. Fla. 2008) (ruling in favor of TracFone by denying defendant motion to dismiss).

[50] Real has since abandoned DRM for its music download service. *See* Brian Heater & Chloe Albanesius, "Update: Rhapsody DRM-Free Music Targets iTunes," PC Magazine, June 30, 2008 (http://www.pcmag.com/article2/0,2817,2324184,00.asp).

[51] Matt Hines, "'Stunned' Apple rails against Real's iPod move," CNET News, July 29, 2004 (http://news.com.com/'Stunned'+Apple+rails+against+Real's+iPod+move/2100-1041_3-5288378.html); "Real Reveals Real Apple Legal Threat," MacWorld UK, Aug. 10, 2005 (http://www.macworld.co.uk/news/index.cfm?RSS&NewsID=12310); RealNetworks 10-Q filing (May 2005) (http://docs.real.com/docs/investors/V08778.pdf).

[52] Kevin Poulsen, "Hackers Sued for Tinkering with Xbox Games," SecurityFocus, Feb. 9, 2005 (http://www.securityfocus.com/news/10466).

[53] Michael R. Tompkins, "Nikon Encrypts RAW File Data," Imaging Resource, Apr. 20, 2005 (http://www.imaging-resource.com/NEWS/1113977781.html); Declan McCullagh, "Nikon's Photo Encryption Reported Broken," CNET News, Apr. 21, 2005 (http://news.com.com/Nikons+photo+encryption+reported+broken/2100-1030_3-5679848.html).

[54] David Pringle & Steve Stecklow, "Electronics With Borders: Some Work Only in the U.S.," Wall St. J., Jan. 17, 2005, at B1; Reuters, "HP Sued Over Printer Cartridge Expiration," MSNBC, Feb. 22, 2005 (http://www.msnbc.msn.com/id/7012754/).

[55] Fred von Lohmann, "DMCA Used to Stymie Competition … Again," EFF Deep Links blog, Nov. 4, 2005 (http://www.eff.org/deeplinks/archives/004123.php); *Storage Technology v. Custom Hardware Engineering*, 421 F.3d 1307 (Fed. Cir. 2005).

[56] 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).

[57] 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).

[58] Pamela Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised," 14 Berkeley Tech. L.J. 519, 556 (1999) (http://www.sims.berkeley.edu/~pam/papers.html); Testimony of Jonathan Hangartner on behalf of Bleem, Library of Congress, Hearing on DMCA, Stanford University, May 19, 2000, pp. 221-28 (http://www.loc.gov/copyright/1201/hearings/1201-519.pdf).

[59] David Labrador, "Teaching Robot Dogs New Tricks," Scientific American, Feb. 12, 2002 (http://www.sciam.com/article.cfm?articleID=0005510C-EABD-1CD6-B4A8809EC588EEDF&sc=I100322).

[60] "Sony PlayStation ruling sets far-reaching precedent," New Scientist, Feb. 22, 2002 (http://www.newscientist.com/news/news.jsp?id=ns99991933); *Sony Computer Entertainment America Inc.* v. *Gamemasters*, 87 F.Supp.2d 976 (N.D. Cal. 1999); *Stevens v Kabushiki Kaisha Sony Computer Entertainment,* [2005] HCA 58 (Oct. 6, 2005) (http://www.austlii.edu.au/au/cases/cth/high_ct/2005/58.html).

[61] *Davidson & Assoc. v. Jung,* 422 F.3d 630 (8th Cir. 2005); Howard Wen, "Battle.net Goes To War," Salon, April 18, 2002 (http://archive.salon.com/tech/feature/2002/04/18/bnetd/); *Davidson & Assoc. v. Internet Gateway* EFF case archive (http://www.eff.org/IP/Emulation/Blizzard_v_bnetd/).

[62] Declan McCullagh "Apple: Burn DVDs—and We'll Burn You," CNET News, Aug. 28, 2002 (http://news.com.com/2100-1023-955805.html).

[63] *See Macrovision v. Sima Prod. Corp.*, No. 2006-1441, 2006 WL 1063284 (S.D.N.Y. Apr. 20, 2006), *reh'g denied,* 2006 WL 1472152 (S.D.N.Y May 26, 2006), *appeal dismissed* 219 Fed. Appx. 997 (Fed. Cir. Mar. 15, 2007); Nate Anderson, "Digitizing Video Signals Might Violate the DMCA," *Ars Technica*, Aug. 16 2006 (http://arstechnica.com/news.ars/post/20060816-7517.html); Fred von Lohmann, "Another DMCA Misuse: Macrovision v. Sima," EFF Deep Links blog, Aug. 15 2006 (http://www.eff.org/deeplinks/2006/08/another-dmca-misuse-macrovision-v-sima).

[64] Dan Goodin, "Blizzard Awarded $6m in *WoW* Bot Case," Register Hardware, Oct. 1, 2008 (http://www.reghardware.co.uk/2008/10/01/world_of_warcraft_bot_ruling/).

[65] *MDY Industries v. Blizzard,* No. CV-06-2555-PHX-DGC, 2008 WL 2757357 (D. Ariz., July 14, 2008).

[66] *See* Corynne McSherry, "You Bought It, But You Don't Own It," EFF Deep Links blog, July 15, 2008 (http://www.eff.org/deeplinks/2008/07/you-bought-it-you-dont-own-it).

[67] *XPEL Technologies Corp. v. American Filter Film Distributors*, No. SA08-CA0175-XR, 2008 WL 3540345 (W.D. Tex. Aug. 11, 2008); Rebecca Tushnet, "Design, Dastar, (registration) dates and the DMCA," Rebecca Tushnet's 43(B)log, Aug. 17 2008 (http://tushnet.blogspot.com/2008/08/design-dastar-registration-dates-and.html).

[68] *See Egilman v. Keller & Heckman LLP,* 401 F.Supp.2d 105 (D.D.C. 2005); *I.M.S. Inquiry Mgt. Systems v. Berkshire Info. Systems,* 307 F.Supp.2d 521 (S.D.N.Y. 2004).

[69] *Pearl Investments LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326 (D.Me., Apr. 23, 2003).

[70] *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1113 (C.D. Cal. 2007) (". . . because [Ticketmaster] has not quantified its harm as required by the statute or even attempted to show what portion of the harm is attributable to [RMG], the Court cannot find that [Ticketmaster] has affirmatively shown that its harm caused by [RMG] exceeds the $ 5,000 minimum. Thus, the CFAA claim does not provide a basis for a preliminary injunction.").

[71] *Id.* at 1112 ("Defendant's only unique arguments as to the DMCA claim are that CAPTCHA is not a system or a program, but is simply an image, and that CAPTCHA is designed to regulate ticket sales, not to regulate access to a copyrighted work.").

[72] *See id.*; Randall Stross, "Hannah Montana Tickets on Sale! Oops, They're Gone," N.Y. Times, Dec. 16, 2007 (http://www.nytimes.com/2007/12/16/business/16digi.html).

[73] *CoxCom, Inc. v. Chaffee*, 536 F.3d 101 (1st Cir. 2008) (affirming *CoxCom, Inc. v. Chaffee*, No. CA05-107S, 2007 WL 1577708 (D.R.I. May 41, 2007)).

APPENDIX B

Before the

U.S. COPYRIGHT OFFICE

LIBRARY OF CONGRESS

In the matter of exemption to prohibition on circumvention of copyright protection systems for access control technologies

Docket No. RM 2008-08

Comment of the Electronic Frontier Foundation

Submitted by:
Fred von Lohmann
Jennifer S. Granick
Electronic Frontier Foundation
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)
fred@eff.org

Pursuant to the Notice of Inquiry of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies[1] ("NOI"), the Electronic Frontier Foundation (EFF) submits the following comments and respectfully asks that the Librarian of Congress exempt the following classes of works from 17 U.S.C. § 1201(a)(1)'s prohibition on the circumvention of access control technologies for the period 2009-2012:

Proposed Class #1: Computer programs that enable wireless telephone handsets to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the telephone handset.

Proposed Class #2: Audiovisual works released on DVD, where circumvention is undertaken solely for the purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright.

I. The Commenting Party

EFF is a member-supported, nonprofit public interest organization devoted to maintaining the traditional balance that copyright law strikes between the interests of copyright owners and the interests of the public. Founded in 1990, EFF represents more than 13,000 dues-paying members including consumers, hobbyists, computer programmers, entrepreneurs, students, teachers, and researchers united in their reliance on a balanced copyright system that ensures adequate protection for copyright owners while ensuring broad access to information in the digital age.

[1] 73 Fed. Reg. 58083 (Oct. 6, 2008).

In filing these comments, EFF represents the interests of hundreds of thousands of citizens who have "jailbroken" their cellular phone handsets, or would like to do so, in order to use lawfully obtained software of their own choosing, as well as the tens of thousands of noncommercial remix video creators who have or would like to include clips from DVDs in their work.

II. The Proper Role of Fair Use and Other Limitations and Exceptions in These Proceedings

In evaluating the two exemptions proposed in these comments, as well as exemptions proposed by others, EFF urges the Librarian to adopt a new approach when considering how fair use and other statutory exceptions should be taken into account. The approach can be summarized as follows: where assertions of fair use or other statutory exceptions lead the Librarian into areas that have not yet been addressed by the courts, the Librarian should err on the side of accepting these assertions of noninfringement, but narrow any resulting exemption to activities that are ultimately found by the courts to be noninfringing.

Congress intended the DMCA's triennial rulemaking to act as a "fail-safe mechanism" to mitigate the risk that access controls on copyrighted works would interfere with otherwise lawful uses of those works.[2] As the Copyright Office has noted, "[t]he goal of the proceeding is to assess whether the implementation of technological protection measures that effectively control access to copyrighted works is adversely affecting the ability of individual users to make lawful uses of copyrighted works."[3]

Among the lawful uses that Congress intended to preserve when enacting § 1201(a)[4] was fair use.[5] Preserving fair use in the context of this rulemaking, however, poses a challenge—how can the courts continue to develop fair use jurisprudence in light of new technologies and practices if the activities in question are impeded by access controls?

The Copyright Office has stated that "[t]he proponents of an exemption bear the burden of proving that their intended use is a noninfringing one."[6] For some proposed exemptions, this will be a straightforward matter. For example, the activity in question may not implicate any of the exclusive rights granted to copyright owners, or may be authorized by license, or may fall squarely within a clear statutory exception. Still other activities will fall comfortably within the ambit of settled fair use precedents. In these cases, it is a simple matter for the Librarian to recognize the noninfringing nature of the activity and move on to weigh the other factors that must be considered in evaluating a proposed exemption.

But not all fair use questions will be so cut and dried. Because Congress has left fair use for the courts to develop on a case-by-case basis, there are always many activities on which the courts

[2] Recommendation of the Register of Copyrights in RM 2005-11, Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Nov. 17, 2006 ("2006 Recommendation") at 6 (citing H.R. Rep. No. 105-551, pt.2 ("DMCA Commerce Comm. Report"), at 35).

[3] *Id.* at 7 (quoting DMCA Commerce Comm. Report at 37).

[4] Unless otherwise noted, all section references are to Title 17 of the U.S. Code.

[5] DMCA Commerce Comm. Report at 25-26.

[6] Recommendation of the Register of Copyrights in RM 2002-4; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Oct. 27, 2003) ("2003 Recommendation") at 106.

have not yet passed. This ability of fair use to evolve in light of new technologies and practices is one of its great strengths.[7]

This, then, poses the dilemma. If the proponents of an exemption assert that the activity in question is a fair use, but the activity does not come within the ambit of previously decided fair use precedents, how should the Librarian respond? While it may be true that "this rulemaking is not the forum in which to break new ground on the scope of fair use,"[8] Congress did not mean to foreclose *the courts* from "breaking new ground" in fair use cases, notwithstanding the use of access controls by copyright owners. Accordingly, to enable courts to assess whether activities that are otherwise "adversely affected" by access controls are noninfringing in light of fair use or another statutory exception, this rulemaking must grant exemptions for activities that a court *might* find to be noninfringing.

In resolving this dilemma, the Librarian must be mindful of the fact that Congress has entrusted the courts with the task of adjudicating the scope of fair use, as well as interpreting and applying the other statutory exceptions to a copyright owner's exclusive rights. The Librarian should therefore exercise caution lest this judicial prerogative be displaced by these rulemakings. For example, if a proposed exemption involved an activity supported by a fair use argument that has yet to be addressed by the courts, and the exemption were denied, a court may never have the opportunity to rule on the question because a defendant may be unable to raise the fair use defense against a § 1201(a)(1) claim.[9]

In short, only if this proceeding grants exemptions in untested cases will a court have an opportunity to address fair use claims involving new technologies and practices. The same is true of other statutory exceptions to copyright, such as those set out by § 109 ("first sale") and § 117 ("essential step and back-up copies").[10] Denying exemptions based on the Librarian's best guesses about how a court might rule on these questions, in contrast, would potentially set the Librarian up as the final arbiter of statutory exceptions with regard to works subject to access controls.

To resolve this dilemma, EFF proposes that the Librarian adopt the following approach when evaluating an assertion of fair use or other statutory exception:

> 1. If, based on existing precedents, the Librarian is satisfied that the activity in question is likely to be deemed to be a fair use or otherwise covered by a statutory exception, then the Librarian should conclude that the activity is noninfringing and proceed to weigh the other factors that must be considered in evaluating a proposed exemption;
>
> 2. If the Librarian is satisfied that the activity in question might plausibly be a fair use or be protected by any other statutory exception, but has some doubt on the question, then the

[7] *See, e.g., Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007) (finding that creation of "thumbnails" by an Internet search engine qualified as a fair use).

[8] 2003 Recommendation at 106.

[9] *See Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 322-23 (S.D.N.Y. 2000) (suggesting in dicta that fair use is no defense to a § 1201(a)(1) claim), *aff'd on other grounds sub nom. Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001).

[10] Recent court cases are grappling with novel issues as they apply § 109 and § 117 in new contexts. *See, e.g., Vernor v. AutoDesk, Inc.*, 555 F. Supp. 2d 1164 (W.D. Wash. 2008) (applying § 109 to computer software); *MDY Indus., LLC v. Blizzard Enter., Inc.*, 2008 WL 2757357 (D. Ariz. July 14, 2008) (applying § 117 to video game software).

Librarian should narrow the proposed exemption to apply only so long as the activity in question is noninfringing;

3. If the Librarian concludes that no reasonable court could find that the activity in question would constitute a fair use or fall within any other statutory exception, it should reject the proposed exemption.

This approach comports with both the letter and spirit of this rulemaking. Where a proposed exemption turns on the application of fair use or another statutory exception in a context that has not been definitively addressed by the courts, this approach would favor granting the exemption (subject to the other factors to be weighed pursuant to the statutory scheme), thereby allowing circumventers to bring their fair use or other statutory defenses to the courts for resolution. This, in turn, will foster the development of judicial precedents that will assist the Librarian in future rulemaking proceedings.

At the same time, an exemption whose scope is limited only to activities that are noninfringing does not release any infringers. If litigation were to ensue, the defendant would be entitled to mount her defense to the claim of infringement—a successful defense on the question of infringement would thus also result in a successful defense to any circumvention claim. In contrast, a failed fair use defense and finding of infringement would simultaneously disqualify the defendant from relying on the exemption as a shield against circumvention liability. This "double jeopardy" should preserve any deterrence value that the ban on circumvention would otherwise provide. This approach also respects the wisdom of case-by-case adjudication in fair use cases, as a defeat for any individual defendant would not adjudicate the applicability of the circumvention exemption for defendants in different circumstances.

If the courts are to continue to develop the jurisprudence of fair use and other statutory exceptions notwithstanding the increasing use of access controls on copyrighted works, the triennial rulemaking must allow as-yet untested questions to find their way to the courts. The approach described above strikes this balance, preserving for the courts their traditional role as case-by-case adjudicators of fair use and other statutory exceptions.

III. Proposed Class #1: Circumvention Necessary for "Jailbreaking" Cellular Phone Handsets

Proposed class: Computer programs that enable wireless telephone handsets to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the telephone handset.

A. Summary

Cellular phones are increasingly sophisticated computing devices, capable of running applications from a variety of software vendors. Several mobile phone providers, however, have deployed technical measures that prevent subscribers from installing applications from vendors of their choice, instead forcing customers to purchase their applications only from the providers' preferred sources.

Apple's iPhone represents the most widely known example of this strategy. Apple uses various technological means to prevent owners of the iPhone from loading or executing applications unless they are purchased from Apple's own iTunes App Store or otherwise approved by Apple. iPhone owners eager to run applications legitimately obtained from different sources must decrypt and modify the iPhone firmware in order to allow those applications to function, a process colloquially known as "jailbreaking."

There is no copyright-related rationale for preventing iPhone owners from decrypting and modifying the device's firmware in order to enable their phones to interoperate with applications lawfully obtained from a source of their own choosing. As the Copyright Office noted in 2006:

> When application of the prohibition on circumvention of access controls would offer no apparent benefit to the author or copyright owner in relation to the work to which access is controlled, but simply offers a benefit to a third party who may use § 1201 to control the use of hardware which, as is increasingly the case, may be operated in part through the use of computer software or firmware, an exemption may well be warranted.[11]

For the same reason, the proposed exemption should be granted.

B. Factual Background

So-called "smart phones" frequently come burdened with technical measures designed to force the owners of these devices to purchase applications only from a limited number of authorized sources. As consumers increasingly adopt these devices, their market choices are increasingly limited by this hindrance.

1. Smart Phone Makers Restrict the Software Applications That Users Can Run, to the Detriment of Competition, Consumer Choice, and Innovation

Smart phone makers use software locks to control a phone owner's ability to install and run applications of his or her own choosing. The iPhone has brought this practice to the attention of the public, if only because of the device's popularity. In less than two years, the iPhone has displaced the Motorola Razr to become the best selling mobile handset in the United States.[12] The iPhone, however, includes software locks that prevent the device from running applications obtained from sources other than Apple's own iTunes App Store. Independent software developers who want to sell software through Apple's App Store must pay a 30% commission to Apple.[13] This restriction is not necessitated by the iPhone technology. Rather, the effort to tie the iPhone, as well as independent developers, exclusively to Apple's own App Store is a business model decision on Apple's part, unrelated to any copyright interest in the firmware that operates the iPhone. There is no technological reason other than the software lock that iPhone owners who are dissatisfied with the selection or price at the App Store cannot shop elsewhere. In fact, today there are many iPhone applications created by third party developers catering to more than 350,000 iPhone owners who have "jailbroken" their iPhones, notwithstanding the risk of circumvention liability.[14]

[11] 2006 Recommendation at 52.

[12] Joshua Topolsky, *iPhone 3G overtakes the RAZR as best-selling domestic handset*, ENGADGET, Nov. 10, 2008, available at <http://www.engadget.com/2008/11/10/iphone-3g-overtakes-the-razr-as-best-selling-domestic-handset/>.

[13] John Markoff & Laura M. Holson, *Apple's Latest Opens a Developers' Playground*, N.Y. TIMES, July 10, 2008.

[14] Erica Sadun, *The story behind Cydia on the iPhone*, ARS TECHNICA, Oct. 8, 2008, available at <http://arstechnica.com/journals/apple.ars/2008/10/08/the-story-behind-cydia-on-the-iphone>.

Apple's policies regarding the approval of iPhone applications for inclusion in the iTunes App Store illustrate some of the costs paid by independent software developers and iPhone users as a result of this restrictive practice. First, as noted above, Apple requires that application developers pay Apple a 30% commission on any sales consummated through the App Store. Second, Apple refuses to authorize applications that "duplicate functionality" offered by Apple's own software.[15] So, for example, Apple has refused to authorize email applications that compete with Apple Mail,[16] music applications that compete with iTunes,[17] or web browsers that compete with Safari.[18] This acts as a damper on both competition and innovation, as it protects Apple's own products from competition in critical areas. Third, Apple has demonstrated a willingness to remove applications from the App Store with little or no notice, a power it reserves to itself in its contractual agreements with developers.[19]

Apple's iPhone is not the only smart phone that consumers have jailbroken in order to enable interoperability with software programs of their own choosing. The T-Mobile G1 smart phone, the first built around Google's "Android" operating system, is relatively open when compared to the iPhone. The Open Handset Alliance, the group behind the Android G1 phone, has said that "anyone can download, build, and run the code needed to create a complete mobile device."[20] Still, G1 owners find that the phone comes with a number of restrictions that restrict the range of applications that the phone will run.[21] For example, only a jailbroken G1 phone can run a full array of Unix tools in the background to enable automated functions such as appointment reminders or scanning for nearby wireless hotspots.[22] In addition, the G1 as delivered will run applications only from the phone's built-in memory; jailbroken G1 phones allow the user to bypass the limits of the G1's internal storage, allowing the phone to run applications from SD memory expansion cards.[23] Google responded to the jailbreak news by releasing an update to disable it, much as Apple has in its efforts to combat jailbreaking of the iPhone.[24]

[15] Jason Snell, *Don't drive iPhone developers away, Apple*, MacWorld, Sept. 24, 2008, available at <http://www.macworld.com/article/135729/2008/09/app_store_policies.html>.

[16] *Id.* (describing the rejection of MailWrangler for "duplicating Apple functionality").

[17] *Id.* (describing the rejection of Podcaster for "duplicating Apple functionality").

[18] Fred Vogelstein, *The Mozilla CEO on His Firefox Strategy, His Google Gambit, and Working with Apple*, Wired (Aug. 2008) (describing difficulties getting Firefox approved for the iPhone), available at <http://www.wired.com/techbiz/people/magazine/16-08/ff_lilly>.

[19] Snell, *supra* n.15 (describing arbitrary App Store removal policies).

[20] Erica Sadun, *Android liberation: T-Mobile G1 jailbroken*, Ars Technica, Nov. 5, 2008, available at <http://arstechnica.com/news.ars/post/20081105-android-liberation-t-mobile-g1-jailbroken.html>.

[21] For example, it appears that the G1 phone will only load signed firmware images, which prevents G1 users from making modifications to the operating system kernel that might be necessary to enable certain kinds of applications. *See* "Confirmed by Android team: G1 only accepts firmware signed by manufacturer," Oblomovka blog, Nov. 1, 2008, available at <http://www.oblomovka.com/wp/2008/11/01/confirmed-by-android-team-g1-only-accepts-firmware-signed-by-manufacturer/>.

[22] *Id.*

[23] *Id.*

[24] Donald Melanson, *Google patches up Android jailbreak with RC30 update*, Engadget, Nov. 7,

2. Section § 1201(a)(1)'s Prohibition on Circumventing Access Controls is Adversely Affecting the Ability of Smart Phone Owners to "Jailbreak" Their Phones

Both smart phone owners and independent software developers have chafed under the artificial restrictions imposed by smart phone vendors on the range of applications that a user can install. As a result, a large community of "jailbreakers" has arisen. For example, literally dozens of tools exist to jailbreak the various iterations of the iPhone, and more than 350,000 iPhone owners have taken advantage of these tools in order to have access to software from sources other than Apple.[25] It appears that these tools depend on circumventing technical measures that smart phone vendors may argue are protected by §1201(a)(1)'s circumvention ban, thereby putting phone owners who use these tools in jeopardy of legal liability.

Let's take the example of the iPhone. Apple encrypts and signs its firmware as a technical protection measure to restrict access to the operating system firmware that controls the iPhone. The firmware includes copyrighted computer programs, is normally decrypted only inside the iPhone, and has not been distributed by Apple in unencrypted form. The firmware must be authenticated by the iPhone's bootloader and decrypted before the iPhone can be used. Once the firmware has been authenticated and decrypted, various components of the firmware authenticate applications before permitting them to run on the iPhone. These components of the firmware ensure that only applications that have been signed by Apple are permitted to run. Other firmware components prevent users from being able to write applications into the "OS partition," where applications must be stored in order to run on the iPhone.

These measures make it necessary for an iPhone owner who would like to run an application obtained from a source other than the iTunes App Store to defeat or bypass a number of technical measures before doing so. For example, the most popular iPhone jailbreaking software, PwnageTool, decrypts and creates a modified version of the iPhone firmware so as to neutralize the authentication checks that prevent applications not signed by Apple from running.[26] This decryption and modification of the iPhone firmware appears to be necessary for any jailbreak technique to succeed on a persistent basis. Apple is likely to assert that this decryption and modification constitutes a circumvention in violation of § 1201(a)(1), even if undertaken by iPhone owners solely for the purpose of running legitimately obtained applications from sources other than Apple.

As more smart phones come on the market to compete with the iPhone, consumers will discover other technological protection measures that restrict their freedom to run software of their choosing. These protection measures will almost certainly operate, at least in part, by restricting access to the smart phone's firmware, potentially putting anyone who jailbreaks the phone at risk of liability under § 1201(a)(1), and thus adversely affecting noninfringing uses of the phone.

2008, available at <http://www.engadget.com/2008/11/07/google-patches-up-android-jailbreak-with-rc30-update/ >.

[25] *See* Sadun, *supra* n.14 (putting the number of users of Cydia, a leading alternative to the iTunes App Store for owners of jailbroken iPhones, at more than 350,000).

[26] Jailbreaking techniques are likely to change over time as Apple updates its software to block specific techniques from working. Although PwnageTool is the most popular jailbreaking application, there are many others that utilize different techniques to accomplish the same end.

C. Jailbreaking a Smart Phone for the Purpose of Running Lawfully Obtained Software Does Not Infringe Copyright

Running lawfully obtained software on a smart phone does not infringe copyright, nor does the process of jailbreaking a smart phone in order to accomplish this goal. As a result, the use of technological protection measures by smart phone makers to prevent these activities adversely affects, and is likely to continue adversely affecting, these lawful uses of smart phones.

There are at least three reasons why jailbreaking a smart phone does not infringe any copyright. First, it may be that under some circumstances jailbreaking can be accomplished without exceeding the scope of the authorization granted to the phone owner when she buys the phone. For example, every iPhone owner is licensed by Apple to "use the iPhone Software on a single Apple-branded iPhone."[27] Although the license agreement also obligates the iPhone owner not to "decrypt, modify, or create derivative works of the iPhone Software," some jailbreaking methods may not transgress this limitation. The iPhone firmware is comprised of a collection of computer programs. To the extent a jailbreaking technique does not modify any of the individual software programs that comprise the iPhone firmware collection, but instead simply adds additional software components to the collection, the practice may not exceed the scope of the license to "use the iPhone software" or constitute a "modification" of any Apple software components, any more than the addition of a new printer driver to a computer constitutes a "modification" of the operating system already installed on the computer. In order to insert these additional components into the iPhone firmware bundle, however, the iPhone user would have to first decrypt the firmware, potentially triggering liability under § 1201(a)(1).

Second, to the extent a jailbreak technique requires the reproduction or adaptation of existing firmware beyond the scope of any license or other authorization by the copyright owner, it would fall within the ambit of 17 U.S.C. § 117(a), which provides that:

> [I]t is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided...that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner.

For example, an iPhone owner qualifies as the "owner of a copy" of the iPhone firmware. The iPhone Software License Agreement expressly acknowledges that while Apple retains ownership of the copyrights to the software that accompanies the iPhone, "[y]ou own the media on which the iPhone Software is recorded...."[28] Every iPhone owner obtains the firmware pursuant to a one-time payment, is entitled to keep the firmware forever, has the freedom to transfer the firmware when transferring the iPhone, and is free to discard or destroy all copies at any time.[29] Owners of other smart phones are likely to obtain firmware on essentially the same terms. The Second Circuit held on similar facts in *Krause v. Titleserv, Inc.* that the defendant had "sufficient incidents of

[27] Apple iPhone Software License Agreement, § 2, available at <http://images.apple.com/legal/sla/docs/iphone.pdf>.

[28] *Id.*, § 1.

[29] *Id.*, §§ 1-3.

ownership over a copy of the program to be sensibly considered the owner of the copy for purposes of § 117(a)."[30]

The court in *Krause v. Titleserv* also recognized that § 117(a) permits the owner of a copy of a computer program not only to make additional copies, but also to adapt those copies to add new capabilities, so long as the changes do not "harm the interests of the copyright proprietor."[31] Where jailbreaking is concerned, the changes to the smart phone firmware are made solely in order to facilitate the interoperability of the phone with third party applications, and the resulting modified firmware is used on the phone on which the firmware was originally installed. In short, jailbreaking qualifies as an "adaptation" authorized by § 117(a).

Third, even if any reproduction and modification of firmware incident to jailbreaking were to fall outside the scope of both authorization and § 117(a), it would nevertheless constitute a noninfringing fair use. In evaluating a fair use defense, courts consider the four nonexclusive factors prescribed in § 107:

1. the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
2. the nature of the copyrighted work;
3. the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
4. the effect of the use upon the potential market for or value of the copyrighted work.

The first and fourth factors have been understood to be of special importance in many fair use cases, and here both of these factors point towards fair use. The first factor favors fair use because jailbreaking a phone in order to use lawfully obtained computer programs is a purely noncommercial, private use.[32] The fourth factor also favors fair use. Insofar as smart phone makers do not copy or distribute firmware separately from the smart phones themselves, the jailbreaking activities of individual phone owners cannot harm the market for the phone/firmware bundle. Indeed, Apple makes various versions of the iPhone firmware available for free from its own website, demonstrating that the firmware has no independent economic value apart from the iPhones that run it. In fact, if users know that they can jailbreak their phones in order to take advantage of a wider array of third party applications, this is likely to increase demand for the phones, for the attendant firmware, and for independently distributed applications.

[30] 402 F.3d 119, 124 (2d Cir. 2005). Although some cases have suggested that § 117 has limited application to software that is "licensed," rather than sold, those cases have involved license agreements that "imposed severe restrictions" on the licensee's freedom to retain and dispose of the software. *Wall Data Inc. v. Los Angeles County Sheriff's Dept.*, 447 F.3d 769, 785 (9th Cir. 2006); *accord DSC Comm. Corp. v. Pulse Comm., Inc.*, 170 F.3d 1354, 1360 (Fed. Cir. 1999); *see generally* Nimmer, NIMMER ON COPYRIGHT § 8.08[B][1][c]. Apple iPhone owners are not bound by "severe restrictions" of the kind found in those cases.

[31] 402 F.3d at 127-29.

[32] *See Sony Corp. of Amer. v. Universal City Studios*, 464 U.S. 417, 449 (1984) (first factor favored a fair use finding for private time-shifting of broadcast television programming); *Perfect 10 v. Amazon.com*, 508 F.3d at 1169 (finding that noncommercial, private creation of browser cache copies is a fair use).

The second and third factors are of less importance in a case such as this one, involving a private, noncommercial use where the first and fourth factors strongly favor fair use. With respect to the second factor, courts have recognized computer software as a hybrid work, combining both unprotectible functional elements and creative elements.[33] Where jailbreaking is concerned, both the functional and creative elements must necessarily be used, since the phone owner will continue to rely on the original firmware (albeit altered to permit third party applications to run) for the operation of the phone after the jailbreaking has been accomplished. With respect to the third factor, this same consideration makes it necessary for individuals who jailbreak their phones to reuse the vast majority of the original firmware. This ought not preclude a fair use finding, however, as courts have been willing to permit extensive copying of the original where it is necessary to accomplish a salutary purpose.[34]

Almost every jailbreaking circumstance will be noninfringing for at least one of the three reasons described above. While smart phone manufacturers may try to engineer a situation in which a finding of noninfringement is less likely, i.e. by implementing an access control that can only be circumvented by acts that exceed the scope of the applicable license, or by reserving sufficient "incidents of ownership" to disqualify the user as the owner under § 117(a), these instances should be left for the courts to address in the first instance. Granting an exemption to § 1201(a)(1)'s circumvention prohibition is the proper way to permit non-infringing jailbreaking while affording courts the opportunity to reach any undecided issues.

D. The Four Nonexclusive Statutory Factors

Section 1201(a)(1)(C) delineates four nonexclusive factors to be weighed in evaluating proposed exemptions. With respect to this proposed exemption, the importance of the four statutory factors recedes because "the access controls do not appear to actually be deployed in order to protect the interests of the copyright owner or the value or integrity of the copyrighted work; rather they are used by [smart phone makers] to limit the ability of [users to run third party applications], a business decision that has nothing whatsoever to do with the interests protected by copyright."[35] By the same token, however, the Register should consider additional public interest factors that militate strongly in favor of granting the exemption.

1. The Availability for Use of Copyrighted Works

In considering this statutory factor, the Register considers whether "the availability for use of copyrighted works would be adversely affected by permitting an exemption."[36] The Register also "consider[s] whether a particular [noninfringing] use can be made from another readily available format when the access-controlled digital copy of that 'work' does not allow that use."[37]

The availability of firmware for smart phones would not be adversely affected by an exemption that permits smart phone users to jailbreak their phones to enable interoperability with

[33] *Sega Ent. Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1524-26 (9th Cir. 1993).

[34] *See Sony v. Universal*, 464 U.S at 449-50 (permitting copying of the entire work where necessary for time-shifting purposes); *Perfect 10 v. Amazon.com*, 508 F.3d at 1167 (holding that copying entire images for inclusion in an Internet search engine was a fair use because the amount copied was "reasonable in light of the purpose of a search engine").

[35] 2006 Recommendation at 52.

[36] *Id.* at 51

[37] *Id.* at 21-22.

lawfully obtained software programs. As discussed above, firmware for smart phones is not generally sold separately from the phone hardware. Consequently, the software locks that prevent phone owners from running software of their choosing are not intended to protect the market for copyrighted firmware—instead, these software locks are intended to "control the use of hardware which, as is increasingly the case, may be operated in part through the use of computer software or firmware."[38] If anything, jailbreaking should increase demand for smart phone firmware, as firmware that is capable of running more applications should, all else being equal, be more valuable to phone owners.

While an exemption is unlikely to harm the availability of smart phone firmware, the lack of an exemption is certain to adversely affect owners of smart phones. Owners of smart phones that are "locked" to a single source for many kinds of applications currently have no alternatives to circumvention if they would like to use software from third party sources. The iPhone jailbreaking experience illustrates the kinds of pervasive technical measures that smart phone makers are likely to deploy in order to ensure that only approved applications are able to run on these devices. Because the firmware necessary to operate the iPhone is designed to (1) prevent users from installing applications on the iPhone in the first instance and (2) prevent the iPhone from running applications that are not approved by Apple, there is no way for iPhone owners to run unapproved applications without circumventing these technical measures.

2. The Availability for Use of Works for Nonprofit Archival, Preservation, and Educational Purposes

As noted in connection with the preceding statutory factor, some smart phone vendors (Apple) do not make smart phone firmware available in any form other than an encrypted digital copy. Others (Open Handset Alliance) make the firmware freely available, but prevent smart phones from running modified versions of the firmware. In any event, there is no reason to believe that the availability (or lack of availability) of smart phone firmware for nonprofit uses would be harmed by an exemption that permits smart phone users to jailbreak their phones to enable interoperability with lawfully obtained software programs.

3. The Impact on Criticism, Comment, News Reporting, Reaching, Scholarship, or Research

While the continued use of access-control measures on smart phone firmware is likely to inhibit research, teaching, and scholarship relating to smart phone technology, the proposed exemption is not directed toward ameliorating those harms. Where phone vendors (like the Open Handset Alliance) currently make firmware freely available for criticism, comment, news reporting, teaching, scholarship, and research, there is no reason to believe that an exemption that permits smart phone users to jailbreak their phones would curtail that availability.

4. The Effect on the Market for, or Value of, Copyrighted Works

As discussed above in connection with the fourth fair use factor, permitting circumvention of access-control measures on smart phones will not harm the market for the firmware that operates smart phones.

Nor does circumvention of the technical measures contained in the iPhone firmware that prevent third party applications from running increase the risk of circumvention of the "digital

[38] *Id.* at 52.

rights management" protections applied to media files, such as music or movie files encrypted by Apple's FairPlay system. In other words, the technical measures that control access to the firmware are not the same ones that control access to music or movies on the phone.

Similarly, enabling an iPhone to run third party applications does not interfere with the security regime that applies to applications purchased from the iTunes App Store. Those applications are tethered to the particular Apple User ID that was used to purchase them, a mechanism designed to discourage users from freely reproducing and distributing applications purchased from the App Store. Nothing about the jailbreak process tampers with this tethering mechanism.

Finally, jailbreaking increases the value of copyrighted works created by independent developers that would not otherwise have been "approved" by the phone maker, creating incentives for additional creativity on the part of competitors.

5. Other Factors

As the Register recognized in 2006, "when application of the prohibition on circumvention of access controls would offer no apparent benefit to the author or copyright owner in relation to the work to which access is controlled, but simply offers a benefit to a third party who may use § 1201 to control the use of hardware which, as is increasingly the case, may be operated in part through the use of computer software or firmware, an exemption may well be warranted."[39]

Here, this same consideration supports the granting of an exemption in favor of smart phone owners who want to run lawfully obtained software of their own choosing. Granting the exemption will not impair the legitimate copyright interests of those who create smart phone firmware. At the same time, an exemption would vindicate the "strong public interest" in fostering competition in the software market, thereby encouraging innovation, and expanding consumer choice.[40]

[39] 2006 Recommendation at 52.

[40] *Id.* at 64.

IV. Proposed Class #2: Extracting Clips from DVDs for Use in Remix Videos

Proposed class: Audiovisual works released on DVD, where circumvention is undertaken solely for the purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright.

A. Summary

Every day, thousands of Americans create and share original, noncommercial videos that include clips taken from movies and television shows released on DVD (referred to hereafter, for the sake of brevity, as "remix videos"). Thanks to the falling price of digital video editing technologies and the popularity of video hosting websites like YouTube, this activity has grown from a niche hobby into a mainstream activity that is certain to become even more popular over the next three years.

Some remix videos doubtless infringe copyrights; others, thanks to the fair use doctrine, just as surely do not. Regardless, for most of modern American copyright history, the fair use doctrine has left room for this kind of "remix culture." Whether any particular creation was, or was not, infringing, was to be determined only after a court had undertaken a fair use analysis. Moreover, as applied by the courts, the fair use factors favor remix video creators who recontextualize existing works for transformative purposes.

Unfortunately, the DMCA's anticircumvention provisions threaten to alter this balance. In the view of many rightsholders, once a creator circumvents CSS in order to obtain clips from a DVD, that creator cannot invoke the fair use doctrine in her defense against a claim brought under § 1201(a)(1). This short circuits the fair use inquiry, denies the creator her day in court, and dries up an important well of future fair use precedents to the detriment of remixers and rightsholders alike.

Some professional creative communities, if well-advised by counsel and indifferent to the loss in video quality, may be able to avoid this dilemma by extracting clips from DVDs without circumventing CSS—either by taking advantage of the "analog hole" or by obtaining "pre-circumvented" copies from unauthorized Internet sources. None of these alternatives, however, is as simple and straightforward as the use of software to copy digital video from DVDs using widely available DVD "rippers." Lacking access to sophisticated legal counsel to advise them, the vast majority of amateur remix video creators rely on DVD rippers to obtain the clips they need. These creators thus risk civil liability based on their circumvention of CSS, even where their videos would otherwise be adjudicated to be noninfringing fair uses. This risk of circumvention liability also chills the ability of remix video creators to resist unfounded DMCA "takedown notices" that impair their ability to share remix videos on the Internet.

An exemption to § 1201(a)(1) is necessary if these remix video creators are to have a meaningful opportunity to engage in noninfringing creativity without unintentionally transgressing the prohibitions of § 1201(a)(1). The exemption should encompass audiovisual works released on DVDs protected by CSS. The proposed exemption class is further narrowed so as to reach only circumvention undertaken solely for the purpose of extracting clips for inclusion in noncommercial videos, the category whose creators are most likely to lack access to sophisticated legal counsel and technical means to take clips without circumventing CSS.

In addition, the proposed exemption is further limited to uses that do not infringe copyright. In other words, this exemption is intended to afford noncommercial videographers an opportunity, if they are sued by rightsholders, to make their fair use cases in court. If the remix video creator prevails on a fair use theory, this exemption would shield her from circumvention liability; if, on the other hand, she does not prevail, then she would be subject to both infringement and circumvention liability. In this way, the exemption will benefit *only* noninfringing creators—infringers gain nothing by it.

Finally, given the maturity of the DVD format and the widespread, mainstream availability of DVD rippers for many years, granting this exemption will have no significant impact on the availability of audiovisual works on DVD.

B. Factual Background

The practice that the proposed exemption is intended to reach—the noncommercial creation of videos that includes clips taken from commercially released DVDs—is already widespread. It will only become more common over the next three years. Accordingly, the Librarian should grant the exemption both based on § 1201(a)(1)'s existing effect on noninfringing activities, as well as its likely future affect on those activities.

1. The Remix is Becoming an Increasingly Popular and Important Form of Creativity

The creative practice of "remixing" existing video content to create original expression is a time-honored tradition, stretching back to 1918 when Lev Kuleshov began splicing and reassembling film fragments to tell new stories. It was not until the 1970s, however, that video editing capabilities became cheap enough to allow (a few, dedicated) amateurs to engage in remix creativity. Today, the ability to remix existing video content (including content released on DVD) has been democratized to an unprecedented degree, thanks to the combination of inexpensive video editing tools on personal computers and easy-to-use video hosting services such as YouTube.

As a result, there has been an enormous increase in remix creativity, a trend that is likely to continue and accelerate in during the next three years. A 2007 survey of U.S. teens by the Pew Internet & American Life Project found that 26% of all online teens remix pre-existing content into their own creations, up from 19% in 2004.[41] This growing practice has attracted the attention of prominent commentators, such as Professor Lawrence Lessig, who stresses the importance of remix creativity to building communities of common interest and fostering new forms of interactive education.[42] Kevin Kelly argues that facility with "re-writing" video will be critical to the conception of literacy in a 21st century more at home with video than text: "We are now in the middle of a second Gutenberg shift — from book fluency to screen fluency, from literacy to visuality."[43]

2. YouTube Creators are Remixing Film and Television Thousands of Times Each Day

Viewed both on an aggregate basis and in light of specific creator communities, YouTube illustrates that large communities of remix video creators frequently depend on clips taken from

[41] Pew Internet & American Life Project, "Teens and Social Media," Dec. 19, 2007, available at <http://www.pewinternet.org/pdfs/PIP_Teens_Social_Media_Final.pdf>.

[42] Lawrence Lessig, REMIX 76-83 (2008).

[43] Kevin Kelly, *Becoming Screen Literate*, N.Y. TIMES, Nov. 21, 2008, available at <http://www.nytimes.com/2008/11/23/magazine/23wwln-future-t.html>.

contemporary films and television programs in the course of creating original videos. Consequently, to the extent § 1201(a)(1)'s prohibition on ripping DVDs applies to this activity, it is putting a large group of noninfringing creators in legal jeopardy.

Professor Michael Wesch, the nation's leading ethnographer studying YouTube, has concluded that thousands of original videos that include clips from film or television sources are likely being uploaded to YouTube *each day*.[44] During October and November 2008, Prof. Wesch's Digital Ethnography project examined two separate random samples of YouTube videos in an effort to estimate how many YouTube videos are remixes that include clips likely to have been drawn from DVD sources. Based on these experiments, he concluded that between 2,000 and 6,000 videos uploaded to YouTube each day fall into this category.[45]

Professor Wesch also identified a number of genres of short-form videos on YouTube that appear to be popular and frequently depend on clips drawn from film or television sources. These new YouTube genres include:

- **Movie trailer remixes**: Original "trailers" for famous films, made by movie fans, often for a humorous purpose. Prof. Wesch estimates that approximately 13,000 of these are posted on YouTube.

  Example: Brokeback to the Future (viewed more than 5 million times) <http://www.youtube.com/watch?v=8uwuLxrv8jY>

- **Film analysis**: Amateur film critics provide their commentary and criticism as a voice-over to clips taken from the films being analyzed. Prof. Wesch estimates that approximately 10,000 of these are posted on YouTube.

  Example: Psychological Aspects of the Matrix <http://www.youtube.com/watch?v=AEisRob4xKw>

- **Movie mistakes**: Film buffs collect and comment on anachronisms, continuity errors, and other "mistakes" found in films and television programs.

  Example: Harry Potter Movie Mistakes <http://www.youtube.com/watch?v=FiZHji1CE9I>

- **Comic juxtaposition remixes**: Often humorous videos created by combining video clips from one film with audio clips from another.

  Example: the phenomenon of "Downfall remixes"[46]

- **Political commentary**: Videos intended to make a political statement that borrow clips from film or television to illustrate their message.

  Example: Jeremiah Wright Illustrated with Movies <http://www.youtube.com/watch?v=xQkHBJS19F8>

[44] *See* Statement of Prof. Michael Wesch, attached as Appendix A.

[45] *Id.*

[46] Jenna Wortham, *Hitler Remixes are Big—on YouTube*, Wired Underwire blog, May 14, 2008, available at <http://blog.wired.com/underwire/2008/05/adolf-hitler-is.html>.

- **Political criticism of film**: Videos that utilize clips in the course of explicitly criticizing the underlying themes or politics of a film.

  Example: Disney Racism
  <http://www.youtube.com/watch?v=LibK0SCpIkk>

- **"YouTube Poop"**: Absurdist remixes that ape and mock the lowest technical and aesthetic standards of remix culture to comment on remix culture itself.

  Example: Youtube Poop: Arthur's Massive, Throbbing Hit
  <http://www.youtube.com/watch?v=RJk4N9gEEmk>

In short, Prof. Wesch's research merely confirms what the millions in YouTube's audience already know—there are tens of thousands of amateur creators who rely on clips taken from DVDs in the course of creating remix videos.

3. The Vidding Community is One Example of an Established Remix Creator Community that Relies on Clips from DVDs

A closer examination of one creator community—vidders—supplements Prof. Wesch's research regarding YouTube creators more generally. Vidders are certainly not the only established community of remix video creators. Movie trailer mashups, for example, have proven extremely popular since bursting on the scene in 2005.[47] The anime music video ("AMV") creator community has also received increasing attention as scholars begin documenting amateur creator communities that are arising around these new video technologies.[48] Vidders, however, are an instructive example because they have a history that predates digital video technologies, and thus a stronger sense of community arising out of that history.

"Vidding" arose in television fan communities in the mid-1970s. In the words of Prof. Francesca Coppa, a scholar who has studied the vidding community:

> Vidding is a form of grassroots filmmaking in which clips from television shows and movies are set to music. The result is called a vid or a songvid. Unlike professional MTV-style music videos, in which footage is created to promote and popularize a piece of music, fannish vidders use music in order to comment on or analyze a set of preexisting visuals, to stage a reading, or occasionally to use the footage to tell new stories. In vidding, the fans are fans of the visual source, and music is used as an interpretive lens to help the viewer to see the source text differently. A vid is a visual essay that stages an argument, and thus it is more akin to arts criticism than to traditional music video. As Margie, a vidder, explained: "The thing I've never been able to explain to anyone not in [media] fandom (or to fans with absolutely no exposure to vids) is that where pro music videos are visuals

[47] *See generally* The Trailer Mash, a website that collects recut trailers and trailer mash-ups, available at <http://www.thetrailermash.com>; David M. Halbfinger, *His 'Secret' Movie Trailer is No Secret Anymore*, N.Y. Times, Sept. 30, 2005 (describing the success of one of the first trailer remixes, a trailer for the horror classic, *The Shining*, recut to make it appear to be a romantic comedy).

[48] Lessig, *supra* n.42, at 77-80 (describing research of Prof. Mimi Ito studying AMV creators).

> that illustrate the music, songvids are music that tells the story of the visuals. They don't get that it's actually a completely different emphasis."[49]

In other words, the archetypal "vid" is a music video created by and for fans of a particular television show or film, where the video content is a collection of clips from a favorite television program or film, and where the audio content is a song that comments on the collection of clips.

According to Prof. Coppa, more than 10,000 vids have been created by creators that self-identify as part of the vidding community.[50] This community embraces a strongly noncommercial ethos and views their works as "a visual essay responding to a visual source."[51] To reiterate the point made by Prof. Coppa above, "fannish vidders use music in order to comment on or analyze a set of preexisting visuals, to stage a reading, or occasionally to use the footage to tell new stories." Vids are commentaries, executed in a visual medium rather than in text, on the original source material—sometimes celebrating or criticizing political, sexual, or cultural elements that were obvious in the original; sometimes uncovering meanings that were latent in the original; and sometimes creating entirely new meanings with the characters and plotlines of the original. In other words, vids are fundamentally transformative visual works, using clips of existing footage in order to comment and build on the meanings of the original source materials.

Vidders frequently rely on footage digitally copied ("ripped") from commercial DVDs in creating their vids, an activity that previous rulemakings have treated as a violation of § 1201(a)(1).[52] Because the vast majority of vidders are amateur videographers who engage in video creation as a hobby, however, they are unlikely to have access to copyright counsel to explain the nuances of circumvention liability. This is particularly true in light of the counterintuitive nature of circumvention liability as applied to DVDs. For example, it will strike many laypersons as bizarre that relying on infringing copies taken from unauthorized Internet sources is preferable (from a circumvention point of view) to ripping a DVD that you have purchased. Similarly, many may find it hard to believe that taking the same excerpts by means of video capture (an alternative that requires additional equipment and expertise that many amateur vidders lack) carries different legal consequences than using a DVD ripper to accomplish the same thing. In fact, when asked, an active vidder (who insisted on anonymity) and Prof. Coppa both agreed that vidders are not likely to understand the legal distinction between "ripping" a DVD and using alternative methods.[53]

Nor is the vidding community's practice of ripping DVDs merely an expression of legal naïveté or convenience. The vidding community takes video quality very seriously, and therefore many vidders favor DVD ripping for aesthetic reasons. In the words of Prof. Coppa, "Vidders typically want the cleanest, biggest clips their systems can handle, because they want to transform/rework the footage in various ways—changing speed, color, adding effects, creating

[49] Francesca Coppa, *Women, Star Trek and the Early Development of Fannish Vidding*, TRANSFORMATIVE WORKS AND CULTURES, Issue 1, September 15, 2008, available at <http://journal.transformativeworks.org/index.php/twc/article/view/44>.

[50] Interview with Prof. Francesca Coppa, attached as Appendix B.

[51] *Id.*

[52] *See, e.g.,* "Making Fan Videos on Your Mac: Mac Vidding for Newbies," available at <http://sweeney32.livejournal.com/1354.html> (recommending the use of Mac the Ripper and Handbrake, two leading DVD rippers for the Macintosh).

[53] Interview with Prof. Coppa, attached as Appendix B; Interview with an anonymous vidder, attached as Appendix C.

manipulations, masking out elements—and the better the footage you start with, the more you can do with it."[54] This is particularly true for vidders who intend to display their videos at conferences and other gatherings, where display technology is likely to be much better than the typical low-resolution YouTube video. Many vidders also distribute high-quality versions of their works from their own Internet sites, demonstrating a commitment to video quality that far exceeds that of most YouTube creators.

The practices of the vidding community demonstrate that noncommercial video creators have valid, noninfringing uses for clips taken from DVDs protected by CSS. Nor do these creators have realistic access to the same material from non-DVD sources, thanks both to a lack of sophisticated legal counsel and a lack of high quality video alternatives.

C. Without an Exemption, Remix Video Creators are at Risk of Liability if They Circumvent the Content Scramble System (CSS) Used on DVDs

The vast majority of mainstream commercial works released on DVD utilize CSS to encrypt the audiovisual work stored on the DVD. The Copyright Office and the courts have concluded that CSS is an "access control" protected by § 1201(a)(1).[55] Moreover, major entertainment companies have repeatedly shown a willingness to commence litigation against those who circumvent CSS or traffic in CSS circumvention tools.[56] Accordingly, but for an exemption granted in this proceeding, those who circumvent CSS to take short clips for inclusion in original remix videos run the risk of civil liability under § 1201(a)(1).

D. Many Remix Videos that Include DVD Clips are Noninfringing Fair Uses

While it is impossible to evaluate the fair use merits of all of the tens of thousands of remix videos that make use of clips taken from DVDs, the general characteristics of these videos make it clear that many qualify as noninfringing fair uses under existing precedents, and many others may qualify, depending on the future development of fair use jurisprudence.[57] Granting an exemption for circumvention, limited solely to remix videos that qualify as fair uses, would preserve the breathing room for transformative expression that the fair use doctrine has always provided, without giving a free pass to others that are infringing.

Turning to the first fair use factor—the purpose and character of the use—two characteristics of remix videos will generally favor fair use. First, the exemption sought here for remix videos is limited to those created for noncommercial purposes. Noncommercial activities have historically been favored under the first fair use factor.[58] Second, remix videos are, by their nature, transformative, creating a new work that does not substitute for the original. Remix videos

[54] Interview with Prof. Coppa, attached as Appendix B.

[55] 2006 Recommendation at 12; *Universal City Studios v. Corley*, 273 F.3d 429 (2d Cir. 2001).

[56] *See, e.g., Universal v. Corley*, 273 F.3d 429 (2d Cir. 2001); *321 Studios v. Metro-Goldwyn-Mayer Studios*, 307 F. Supp. 2d 1085 (N.D. Cal. 2004); *Paramount Pictures Corp. v. 321 Studios*, 2004 WL 402756 (S.D.N.Y. Mar. 3, 2004).

[57] *See generally* American University Center for Social Media, *Code of Best Practices in Fair Use for Online Video*, June 2008, <http://www.centerforsocialmedia.org/resources/publications/fair_use_in_online_video>.

[58] *See Sony v. Universal*, 464 U.S. at 449 (first factor favored a fair use finding for noncommercial time-shifting of broadcast television programming); *Perfect 10 v. Amazon.com*, 508 F.3d at 1169 (finding that noncommercial, private creation of browser cache copies is a fair use).

are frequently parodic, satiric, or created for purposes of commentary or criticism, precisely the kind of transformative uses that have been treated favorably by courts with respect to the first factor.[59]

The third fair use factor—the amount taken—also tips in favor of remix video creators. The excerpts taken by remix video creators from films or television programs will generally comprise only a small fraction of the works from which they are taken.[60] Where the amount taken is both qualitatively and quantitatively small, and reasonable in light of the purpose of the copying, courts generally find that the third factor favors fair use.[61]

The fourth fair use factor—the effect of the use on the potential market for the work—also favors remix video creators. Where noncommercial uses are concerned, copyright owners bear the burden of proving that the use in question undermines the economic value of the copyrighted work.[62] It is unlikely that a copyright owner will be able to meet that burden in challenging remix videos. These videos will almost never be a substitute for the original works. In fact, in many cases, a remix video will be hardly comprehensible to someone who has not already seen the original video "texts" from which the clips are drawn. In the vidding community, for example, fan-made vids often presuppose a high level of familiarity with the source material, without which the vids cannot be fully appreciated.[63] Moreover, to the extent that any particular remix video is a parody of the original, or associates the original work with any political message or controversial subjects, it is unlikely that the copyright owner would license the remix. Courts have found that a fair use finding is appropriate where these considerations make licensing unlikely or impossible.[64]

Finally, even if the second fair use factor—the creative nature of the original work—tips in favor of copyright owners, courts have recognized that this factor is likely to be of little importance in fair use cases involving the creation of transformative, original works.[65]

[59] *See Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994) (finding that the first factor favors transformative uses); *Blanch v. Koons*, 467 F.3d 244, 253 (2d Cir. 2006) (same).

[60] Although most vids include only a small fraction of the video sources from which they draw, they generally include a complete sound recording as the audio track. Courts have found, however, that the use of an entire work can nevertheless qualify as a fair use where the use is transformative. *See Bill Graham Archives v. Dorling Kindersley Ltd.*, 448 F.3d 605 (2d Cir. 2006) (fair use where entire poster copied for transformative purpose); *Nunez v. Caribbean Int'l News Corp.*, 235 F.3d 18 (1st Cir. 2000) (fair use where entire photograph copied for news reporting purposes).

[61] *See Blanch v. Koons*, 467 F.3d at 257-58 (portion of photograph taken); *Consumers Union of U.S., Inc. v. General Signal Corp.*, 724 F.2d 1044, 1050 (2d Cir. 1983) (29 words taken from 2100 word article)

[62] *Sony v. Universal*, 464 U.S. at 451 ("A challenge to a noncommercial use of a copyrighted work requires proof either that the particular use is harmful, or that if it should become widespread, it would adversely affect the potential market for the copyrighted work.").

[63] Jesse Walker, *Remixing Television*, REASON (Aug/Sept. 2008) (quoting Prof. Coppa as saying, "[s]ome of the best vids in the world don't look like anything special unless you know how to read them and interpret them."), available at <http://www.reason.com/news/show/127432.html>.

[64] *Campbell v. Acuff-Rose*, 510 U.S. at 592 ("Yet the unlikelihood that creators of imaginative works will license critical reviews or lampoons of their own productions removes such uses from the very notion of a potential licensing market.").

[65] *Id.* at 586 (finding that the second factor is of little assistance in parody cases).

Of course, whether any *particular* remix video qualifies as a fair use will depend on the facts of the case and is for a court to determine. For the reasons discussed in detail at the outset of these comments, however, if the courts are to have the opportunity to address these fair use questions, the Librarian must grant an exemption where a plausible fair use argument would otherwise be foreclosed by a § 1201(a)(1) claim. Noncommercial remix videos present precisely such a circumstance—most will have plausible fair use arguments to make, and none will see their day in court unless an exemption to excuse circumvention claims arising from ripping DVDs. And because the proposed exemption is expressly limited to "noncommercial videos that do not infringe copyright," any videos that are deemed to be infringing will not get the benefit of the circumvention exemption.

E. Section 1201(a)(1) Adversely Affects Remix Video Creators

Section 1201(a)(1)'s prohibition on circumvention has, and will continue to, adversely affect the noninfringing activities of remix video creators. Most obviously, to the extent the circumvention ban prohibits ripping DVDs in order to extract clips, the law puts remix video creators in legal jeopardy when they engage in authorship that would otherwise be protected by fair use. This adverse affect is compounded by a lack of access to sophisticated copyright counsel and the fact that DVD ripping is an "attractive nuisance"—the fastest, cheapest, and easiest way for most amateur videographers to obtain clips from DVD. These two realities mean that the majority of remix video creators will unintentionally violate § 1201(a)(1) in the course of authoring their noninfringing videos.

There is another, more subtle, way in which § 1201(a)(1) is adversely affecting the noninfringing activities of video remix creators: the interaction between the DMCA's online service provider safe harbors and § 1201(a)(1) frequently makes it impossible for remix video creators to keep their videos online. Large media companies are delivering hundreds of thousands of "takedown" notices each month to online service providers who host and link to information posted by Internet users. While many of those notices target clear cases of copyright infringement, remix video creators have found themselves mistakenly caught in the takedown notice driftnet.[66] Assuming the creator had ripped DVDs in order to obtain clips included in the video, she would face a difficult set of choices. If she were to insist on her right to "counter-notice" pursuant to 17 U.S.C. § 512(g) in an effort to have her video restored, she would be exposing herself to a potential circumvention claim from the copyright owner who sent the DMCA takedown demand. In other words, thanks to § 1201(a)(1)'s ban on circumvention, remix video creators are unable to take full advantage of the protections they would otherwise enjoy against having their noninfringing works improperly censored off the Internet.

F. The Four Nonexclusive Statutory Factors

[66] For example, the creators of the renowned trailer mashup, *Ten Things I Hate About Commandments*, saw their video taken down from YouTube thanks to a DMCA takedown notice issued by Viacom. *See* <http://blog.myspace.com/index.cfm?fuseaction=blog.view&friendID=134516305&blogID=278439535>. Similarly, after the video, *Vogue*, was featured in *New York Magazine*, it was removed from iMeem, apparently in response to a DMCA takedown notice. *See* Walker, *supra* n.63.

1. The Availability for Use of Copyrighted Works

Section 1201(a)(1)(C) instructs the Librarian of Congress to consider four nonexclusive considerations in weighing proposed circumvention exemptions. The first consideration is "the availability for use of copyrighted works."[67] In the context of exemptions that would permit the circumvention of CSS on DVDs, the Copyright Office has interpreted this statutory instruction to require "examination of the alternative forms in which the 'work,' i.e., the motion picture or audiovisual work, was available for use."[68]

In previous rulemaking proceedings, the motion picture industry has argued that circumvention of CSS on DVDs should not be permitted so long as noninfringing uses can be accomplished by other, albeit more expensive and less convenient, means. These alternatives are impractical, inadequate, or both, for many remix video creators engaged in the noninfringing uses describe above. In other words, even one were to assume, *arguendo*, that CSS has made more copyrighted works available for purely consumptive uses, it has simultaneously made those works *less available* to remix video creators.

The alternatives for taking clips from DVDs proposed in previous rulemakings fall short for most remix video creators for one simple reason: they lack the legal sophistication necessary to understand that their legal risk may vary based on the technologies they use to capture DVD clips. The proposed exemption is limited to noncommercial remix video creators, the group that is most likely to lack access to legal advice in advance of creating their videos. While these creators might have a rudimentary understanding of copyright law, and perhaps even some notion of fair use, they are particularly unlikely to appreciate the different (and counterintuitive) ways that § 1201(a)(1) treats the following scenarios:

- Ripping from a DVD you lawfully possess, using widely available free software such as Handbrake, in order to take short clips for use in a remix video (viewed as illegal circumvention by major motion picture studios);
- Using a camcorder and flat screen TV in order to capture the same clips for the same purpose (no circumvention);
- Connecting the analog outputs from a DVD or VHS player to a personal computer equipped with video capture capabilities in order to capture the same clips for the same purpose (no circumvention);
- Downloading a digital copy of a DVD from an unauthorized BitTorrent site, like those that can be found through The Pirate Bay, in order to excerpt the same clips for the same purpose (no circumvention).

As applied to hobbyist creators engaging in noncommercial creativity, these legal distinctions amount to little more than a trap for the unwary. By taking the course that seems most fair and "legitimate"—namely, using your own DVD drive to take excerpts from a DVD you lawfully possess—these creators will have unknowingly violated § 1201(a)(1).

In short, in the absence of sophisticated copyright counsel, the "alternatives" posited by motion picture studios are largely irrelevant to remix video creators—they will never know to seek

[67] 17 U.S.C. § 1201(a)(1)(C)(i).

[68] 2006 Recommendation at 22.

them out in the first place. Their first encounter with § 1201(a)(1) and its counterintuitive set of distinctions is likely to come only if their video is targeted for enforcement action, whether in the form of a DMCA takedown notice or direct threat of suit.

Moreover, many of the "alternatives" theoretically available to remix video creators require additional equipment and technical expertise that are beyond their reach. Many computers of recent vintage include a DVD drive and video editing software (all Apple Macintosh computers, for example, include software like iMovie). Simply downloading one of a number of free DVD "rippers," such as Handbrake, DVD Shrink, or Mac The Ripper, equips the aspiring remix video creator with the tools to take high-quality excerpts from DVDs. In contrast, "camcording" alternatives require that the creator purchase a camcorder, find a flat screen display[69] from which to record, and figure out how to import the resulting footage into video editing software on a personal computer. Alternatives that rely on the "analog hole" or the use of VHS source materials require creators to obtain and learn how to use additional video capture hardware for their computers. These additional hurdles will increase costs (in both time and money) for many noninfringing amateur creators, and may well deter others from undertaking projects at all.

Strict application of § 1201(a)(1) would also result in perverse incentives for remix video creators. Of all the "alternatives" available to creators who understand the circumvention restrictions imposed by § 1201(a)(1), by far the easiest and least cumbersome would be to simply download content from unauthorized Internet sources. This outcome seems distinctly less desirable than permitting remix video creators, many of whom are fans who eagerly purchase the works that they remix, to use their own DVD copies in the course of creating noninfringing remix videos.

Finally, as the Copyright Office recognized in 2006, many "alternatives" for taking clips from DVDs result in compromised video quality. Video quality matters to many kinds of remix creators today and is likely to become more important in the next three years. For example, in the vidding community, using the highest quality video available is frequently critical to the expressive message that vidders are attempting to convey. In the words of one vidder:

> Vidders want to create immersive experiences, and they are highly invested in visual communication and aesthetics. Poor-quality source interferes with all of these, hence the community's determination to use the best-quality source footage available.[70]

Professor Coppa agrees:

> Vidders want the best-looking footage available, and will rate "crisp source" highly when discussing a vid's merits. While there are some folks who still capture, capturing is more expensive, requires more technical expertise, and typically looks less good. Ripping from DVDs tends to get you better source than downloaded .avis, which are frequently recorded off broadcast television, and may be low-resolution or have bugs or other visual artifacts.[71]

[69] Recording from a traditional CRT displays frequently results in "roll bar" distortion unless a "sync box" is used. *See generally* Kris Malkiewicz, M. David Mullen & Jim Fletcher, CINEMATOGRAPHY: A GUIDE FOR FILMMAKERS AND FILM TEACHERS 213 (3d ed. 2005).

[70] Interview with anonymous vidder, attached as Appendix C.

[71] Interview with Prof. Coppa, attached as Appendix B.

The critically acclaimed vid, *Vogue*, created by a vidder known as Luminosity, illustrates the importance of video quality to the expressive content of vids. *Vogue* sets a montage of expertly edited, visually arresting excepts from the film *300* against the music of Madonna's hit song, *Vogue*, thereby commenting on both the film and the song. Comparing the YouTube version with the original makes the importance of video quality starkly obvious. Viewed in "full screen" mode, the high quality original has a clean, professional look that reminds viewers of the self-conscious visual extravagance of the original film, even as Madonna's song reminds us that the film's imagery is an exercise in sexual objectification and violence.[72] Viewed in YouTube's "full screen" mode, in contrast, the same video loses much of its visual impact and therefore fails to deliver its message with the same emotional force.[73] In this context, it is plain that having access to high-quality video excerpts is "necessary to achieve a productive purpose,"[74] namely to engage in effective criticism and comment within the meaning of § 1201(a)(1)(C)(iii).

Vogue is a reminder that many remix videos are not intended (or not solely intended) for distribution in low-quality mediums like YouTube. Rather, as personal computers and living room home theater systems continue down the road to "convergence," remix videos will increasingly be called upon to deliver their messages on large, high-definition screens. If remix video creators are to have meaningful access to this medium, they have to be able to take high-quality, full-resolution excerpts from DVDs.

2. The Availability for Use of Works for Nonprofit Archival, Preservation, and Educational Purposes

According to the Copyright Office, "the second factor requires a more particularized inquiry than the first," examining the impact of technical protection measures on nonprofit archival, preservation, and educational uses.[75] While EFF believes that CSS has also had a deleterious effect on these uses, the proposed exemption for remix video creators is not aimed at those categories of uses. In any event, for the reasons discussed below, there is no reason to believe that granting an exemption to noncommercial video remix creators will harm the availability of copyrighted works for these nonprofit uses.

3. The Impact on Criticism, Comment, News Reporting, Reaching, Scholarship, or Research

The third statutory factor "requires consideration of whether the [§ 1201(a)(1)] prohibition has an impact on criticism, comment, news reporting, teaching, scholarship, or research."[76] This consideration reflects Congress' special solicitude for these "traditionally socially productive noninfringing uses."[77]

As discussed above, the prohibition on circumvention of CSS is having a deleterious effect on the a wide variety of remix video creators who are engaged in criticism and commentary. Many of the most widely known remix videos are exercises in (often humorous) commentary or criticism. For example, many leading examples of the so-called "trailer mashup" genre find their

[72] Available at <http://slum.slashcity.com/lum/eyecandy/multi/vogue-xvid.zip>.

[73] Available at <http://www.youtube.com/watch?v=IBnKivzLbJE>.

[74] 2006 Recommendation at 22.

[75] *Id.*

[76] 2006 Recommendation at 23.

[77] *Id.*

humor in exposing, and thereby commenting on, the emotional manipulation that is the stock in trade of many movie trailers.[78] One of the most popular trailer mashups, *Brokeback to the Future*, uncovers latent homoerotic themes and possibilities in the midst of the *Back to the Future* family film franchise.[79]

Members of the vidding community are also engaged in a project of criticism and commentary, with many leading vids acting as visual essays regarding the characters and plots of the sources from which they are excerpted. In the words of an anonymous vidder:

> Vidding aims to create new meanings from the juxtaposition of video clips and music. These meanings may include parody, criticism, the creation of entirely new stories, meta-discussion, and beyond.[80]

Professor Coppa also emphasizes the centrality of commentary and criticism to vidding:

> Vids are arguments. A vidder makes you see something. Like a literary essay, a vid is a close reading. It's about directing the viewer's attention to make a point.[81]

Examining the history of vidding, Professor Coppa finds a consistent focus on the part of vidders, who are predominantly female, on fleshing out marginalized (often female) perspectives that are implicit in televisions shows like *Star Trek* or *Quantum Leap*.[82] A vid like *Vogue* is a direct exercise in cultural criticism—a stylish attack on the romanticized conjunction of violence and male sexuality in a major Hollywood film. Some vids (such as *Us* by the vidder known as Lim[83]) can be far-reaching commentaries on vidding and fan culture itself, while other vids (like *Superstar* by the vidder known as here's luck[84]) serve the more modest (but equally fair) purpose of commenting on characters in a favorite TV show.

Professor Wesch has identified a number of popular genres of remix videos on YouTube that are expressly devoted to criticism and commentary.[85] For example, he points to some 10,000 videos dedicated to film analysis, as well as to videos that collect and comment on "movie mistakes." He also identifies videos that directly criticize the racist stereotypes contained in Disney films or implicit politics of Hollywood blockbusters like *300*. He also notes that clips taken from films or television programs are often used to illustrate political commentaries, such as the speeches of Rev. Jeremiah Wright. And even absurdist videos like those grouped together in the genre "YouTube Poop" can be read as a commentary on remix culture more generally.

Because remix videos are so often created for the purpose of commentary or criticism, the third statutory factor favors the granting of an exemption to alleviate the adverse affects that § 1201(a)(1) has inflicted on remix video creators.

[78] *See, e.g., Scary Mary Poppins*, <http://www.youtube.com/watch?v=2T5_0AGdFic>; *Must Love Jaws*, <http://www.youtube.com/watch?v=92yHyxeju1U>.

[79] *See Brokeback to the Future*, <http://www.youtube.com/watch?v=8uwuLxrv8jY>.

[80] Interview with anonymous vidder, attached as Appendix C.

[81] *See* Walker, *supra* n.63.

[82] *See* Coppa, *supra* n.49.

[83] Available at <http://www.imeem.com/sublim/video/LQU2ToIY/lim_us/>.

[84] Available at <http://www.heresluck.net/videos/index.html>.

[85] Statement of Prof. Wesch, attached as Appendix A.

4. The Effect on the Market for, or Value of, Copyrighted Works

In weighing proposed exemptions to § 1201(a)(1), Congress instructed the Librarian to consider "the effect of circumvention of technological protection measures on the market for or value of copyrighted works." In previous rulemaking proceedings, motion picture studios have asserted that any exemption that permits circumvention of CSS would reduce their willingness to make films available on DVD. In the 2000 and 2003 rulemaking proceedings, the Copyright Office accepted these assertions, finding that "the motion picture industry's willingness to make audiovisual works available in digital form on DVDs is based in part on the confidence it has that CSS will protect it against massive infringement."[86] Whatever the merits of that view as applied to the facts in 2003, the facts have plainly changed since then, as EFF explained in its submission during the 2006 rulemaking proceeding.[87] Simply put, if the widespread, free availability of CSS circumvention tools since the 2003 rulemaking has not dampened Hollywood's ardor for DVDs, authorizing remix video creators to circumvent CSS will hardly tip the scales.

Notwithstanding the anti-trafficking prohibitions contained in § 1201(a)(2), tools capable of circumventing CSS have been widely, continually, and freely available since the 2003 rulemaking proceeding. Free, easy-to-use DVD ripping software has been continually available on the Internet for all major personal computer operating systems. DVD Shrink, Mac The Ripper, Handbrake, and dvd::rip are among the most popular DVD decryption solutions—all are available free-of-charge and have remained continually available since the 2006 rulemaking.[88] Many other less popular DVD ripper alternatives, some distributed for free, others for a small fee, also compete with these leading products. Even DeCSS, the first widely distributed DVD decryption software, remains widely available online, even though it has long-since been surpassed in ease-of-use and sophistication by its descendants.[89]

These tools have been readily accessible to mainstream personal computer users for many years. DVD ripping software, once the domain of a small band of enthusiasts, is now regularly reviewed in mainstream publications, including *USA Today, MacWorld, PC World, PC Magazine*, and the *Fort Worth Star Ledger*.[90] In light of this reality, millions of Americans have had DVD circumvention tools at their disposal for many years.

[86] 2003 Recommendation at 119.

[87] Reply Comment of the Electronic Frontier Foundation, Docket No. RM 2005-11 (filed Feb. 2, 2006).

[88] *See* Adam Pash, *Five Best DVD Ripping Tools*, LifeHacker blog, Apr. 17, 2008, available at <http://lifehacker.com/380702/five-best-dvd-ripping-tools>.

[89] *See* Anuj C. Desai, *Software as Protest: the Unexpected Resiliency of U.S. Based DeCSS Posting and Linking*, 20 The Information Society 101 (2004), available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=729931>.

[90] *See* Christopher Breen, *Updated Handbrake encodes more than DVDs*, MacWorld, Oct. 1, 2008, available at <http://www.macworld.com/article/135834/2008/10/handbrake_update.html>; Kyle Monson, *7 Tools for Ripping Your DVDs*, PC Magazine, Sept. 11, 2008, available at <http://www.pcmag.com/article2/0,2817,2330176,00.asp>; Preston Gralla, *14 Great Multimedia Utilities*, PC World, May 28, 2007, available at <http://www.pcworld.com/article/131990-3/14_great_multimedia_utilities.html>; *What Apple TV Hackers are Hacking,* USA Today, Apr. 15, 2007, at 3B; Michael Gerst, *Dr. Emilio Bombay Column*, Ft. Worth Star-Ledger, June 11, 2004.

The potential impact of these CSS circumvention tools on movie industry incentives has doubtless been exacerbated now that DVD burners have been eclipsed by devices that can play video files directly without the need for optical media. Whereas many consumers in 2006 needed to copy a DVD to recordable DVD blanks before they could play them, today even that minor inconvenience has been eliminated. For example, digital media players like the iPhone and iPod Touch allow consumers to watch movies ripped from DVD. Media extenders, such as the Apple TV and Microsoft Xbox 360, also permit consumers to watch content ripped from DVDs on their TVs. As a result, today most DVD ripping software comes preconfigured to rip, transcode, and compress DVDs so as to enable direct playback of the video files. The continued popularity of "all you can rent" video rental operations, the model pioneered by Netflix, has also facilitated access to a large library of DVDs from which copies can be made. Over the next three years, none of these realities is likely to change.

The efficacy of CSS as a mechanism for preventing widespread unauthorized copying has also been eroded by the continued popularity of peer-to-peer file sharing and other so-called "darknet" technologies.[91] In a digital environment characterized by high-bandwidth communications channels, the leakage of even a small number of formerly "protected" copies into these channels leads to their widespread distribution without any further need for circumvention by the ultimate users. Accordingly, so long as even a small number of individuals are able to circumvent CSS, decrypted copies of formerly CSS-encrypted films will be widely distributed to large numbers of less sophisticated users, none of whom will need access to circumvention tools themselves. This reality accounts for the near-instantaneous availability of a vast library of films and television programs from sites like The Pirate Bay, which recently boasted 25 million users simultaneously sharing material over the Internet. Downloading these films does not require any circumvention tools—the content drawn from DVDs comes "pre-circumvented." Despite efforts by law enforcement and the motion picture industry, it seems apparent that much of the most popular material released on DVD will continue to be freely available through Darknet channels during the next 3 years.

In summary, developments during the most recent exemption period have made it clear that, whatever its efficacy in the past, CSS is no longer protecting digital content on DVD from widespread infringement. Millions of U.S. consumers already possess circumvention tools capable of defeating CSS. Millions more are able to download DVD content from P2P networks and other darknet channels without having to circumvent CSS at all. And new technologies, including portable media players and home media servers, are giving consumers ever more reasons to copy their DVDs.

What impact has the widespread circumvention of CSS had on the availability of digital audiovisual content on DVD? As mentioned above, the Copyright Office in 2000 and 2003 feared that the grant of even a limited DVD exemption might undermine the motion picture industry's incentives to continue making content available on DVD. Had those anxieties been well-founded,

[91] The term "darknet" and its implications for digital distribution were developed in a paper authored by senior Microsoft engineers in 2002. *See* Peter Biddle, Paul England, Marcus Peinado & Bryan Willman, *The Darknet and the Future of Content Distribution* (2002), available at <http://crypto.stanford.edu/DRM2002/darknet5.doc>; *see also* Fred von Lohmann, *Measuring the Digital Millennium Copyright Act Against the Darknet: Implications For the Regulation of Technological Protection Measures,* 24 Loy. Ent. L. Rev. 635 (2005).

then the broad availability of DVD ripping software should have resulted in a conspicuous downturn in the number of DVDs released.

The empirical evidence proves just the opposite. Even though DVD sales have begun to plateau as the format reaches its maturity, major motion picture studios have continued to release new DVD titles in ever-increasing numbers, including classic titles, television series, and growing array of "direct to DVD" releases.[92] DVD sales and profitability continue to account for a large portion of movie studio revenues.[93] This evidence suggests that, whatever the contribution of CSS to the availability of content on DVD may have been in the past, today the motion picture industry's willingness to release material on DVD is not correlated to any illusory security provided by CSS.

Moreover, the proposed exemption for remix video creators would authorize circumvention solely for noninfringing purposes and would not authorize distribution of CSS circumvention devices. Accordingly, nothing about the proposed exemption would hinder any enforcement efforts by movie studios against those who traffic in circumvention tools, just as the exemption granted to film professors in 2006 had no impact on those efforts.

Accordingly, if the widespread circumvention of CSS has not adversely affected movie studio incentives to release material on DVD, the activities of remix video creators certainly will not do so. If anything, granting this exemption will support legitimate sales of DVDs, as many video remix creators will have a reason to prefer purchasing DVDs over utilizing unauthorized sources.[94]

EFF expects the motion picture studios will once again rely on self-serving statements regarding the industry's reliance on CSS as a linchpin for DVD distribution. Unless those assertions are backed by concrete evidence that an exemption for noncommercial video remix creators will result in diminished availability of audiovisual content on DVDs, the Librarian should discount those assertions. Moreover, because the Copyright Act has never granted copyright owners any right to control fair uses, any argument that an increase in fair use (as distinguished from infringements) might diminish copyright owners' incentives to release their works should also be discounted, as the right to control fair uses were never meant to be part of those incentives in the first place.

V. Conclusion

For the reasons described above, the Librarian should determine that the noninfringing uses described herein are, and are likely to be, adversely affected by the prohibitions of § 1201(a)(1), and therefore approve the two proposed exemptions for the period 2009-2012.

December 2, 2008 *Submitted by:*

[92] According to The Digital Bits, <http://thedigitalbits.com>, there are more than 93,000 titles available on DVD as of November 2008, as compared to 65,937 as of November 2006.

[93] Brooks Barnes, *DVDs, Hollywood's Profit Source, Are Sagging*, N.Y. Times, Nov. 20, 2008, available at <http://www.nytimes.com/2008/11/21/business/21dvd.html>.

[94] *See* Interview with Prof. Coppa, attached as Appendix B (noting that vidders often purchase multiple versions of their favorite shows from which to draw clips).

Fred von Lohmann
Jennifer S. Granick
Electronic Frontier Foundation
454 Shotwell St.
San Francisco, CA 94110
(415) 436-9333
(415) 436-9993 (fax)
fred@eff.org

APPENDIX A

Statement of Prof. Michael Wesch
Assistant Professor of Cultural Anthropology and Digital Ethnography
Kansas State University
November 28, 2008

I am Assistant Professor of Cultural Anthropology and Digital Ethnography at Kansas State University in Manhattan, Kansas. My research is focused on exploring the impact of new media on society and culture. More information about my publications and research interests can be found at my website, Mediated Cultures (<http://mediatedcultures.net/ksudigg/>).

As part of my research, I teach a course in digital ethnography and am the project director for the Digital Ethnography of YouTube project. Combining the efforts of both professors and students, the project has since 2007 simultaneously participated in and observed (a technique known as "participant observation") the YouTube community. On June 23, 2008, I presented a talk entitled "An Anthropological Introduction to YouTube" at the Library of Congress describing some of the early insights gleaned from this research effort.[95]

During October and November 2008, the Digital Ethnography project examined two separate random samples of YouTube videos in an effort to roughly estimate how many YouTube videos are "remixes" that include clips taken from television or films.

Our October random sample consisted of 240 videos, of which 18 were remixes. Of the 18 remixes, half (9) involved clips that appear to have been taken from DVDs, and thus whose creation may have involved a violation of the Digital Millennium Copyright Act's prohibition on ripping DVDs. Although this sample suggests that only 7.5% of the videos uploaded to YouTube are remixes, and only 3.75% include clips taken from DVD sources, even these small percentages translate into large numbers of videos, given the enormous number of videos uploaded to YouTube. For example, 7.5% of YouTube videos translates into approximately 15,000 videos uploaded each day.

In November, we repeated our experiment and found 5 remixes that included movie clips in a relatively random sample of 240, suggesting that about 4,000 are uploaded every day. However, given the small number in our sample, the actual daily average is more likely to fall somewhere between 2,000 and 6,000.

Given the small sample sizes involved, these numbers are necessarily only suggestive. We would have to do several more studies before coming to firm conclusions regarding the overall number of movie-related remixes on YouTube. Nevertheless, based on these two samples, as well as my anecdotal experience with the Digital Ethnography project, I believe that there are large communities of YouTube users who regularly, albeit unintentionally, violate the DMCA's ban on ripping DVDs in the course of creating original remixes.

[95] The presentation can be viewed at <http://www.youtube.com/watch?v=TPAO-lZ4_hU>.

The following constitute a sampling of established, popular YouTube remix genres and communities that are likely to fall into this category of unintentional DMCA violators:

1. **Movie Trailer Remixes.**

A search for "remix trailer" on YouTube returns more than 17,000 hits, and, based on analysis of a sample of these results, we estimate that there are probably about 13,000 of these posted on YouTube.

Examples include:

- Brokeback to the Future (viewed more than 5 million times)

<http://www.youtube.com/watch?v=8uwuLxrv8jY >

- Scary Mary Poppins (viewed more than 7 million times)

<http://www.youtube.com/watch?v=2T5_0AGdFic>

2. **Film Analysis.**

There are probably about 10,000 of these, such as:

- Psychological Aspects of the Matrix

<http://www.youtube.com/watch?v=AEisRob4xKw>

3. **Movie Mistakes.**

People like to share little inconsistencies, anachronisms, and other mistakes they find in the movies. It is hard to estimate how many of these there are. Here is an example:

Movie Mistakes 1

<http://www.youtube.com/watch?v=8ra-7brEEsg>

Harry Potter Movie Mistakes

<http://www.youtube.com/watch?v=FiZHji1CE9I>

4. **Comic Juxtaposition Remixes.**

The most popular of late would be the Downfall remixes (Hitler Remixes)

<http://blog.wired.com/underwire/2008/05/adolf-hitler-is.html>

5. **Political commentary.**

People often borrow clips from movies and television to illustrate political points in various ways. Here is an example:

- Jeremiah Wright Illustrated with Movies

<http://www.youtube.com/watch?v=xQkHBJS19F8>

6. **Political Criticism of Movies**

Here are 2 examples:

- 300 Epithets <http://www.youtube.com/watch?v=XwFOpYOXBQ0>

- Disney Racism <http://www.youtube.com/watch?v=LibK0SCpIkk>

7. "YouTube Poop"

A small but thriving community making remixes that ape and mock the lowest technical and aesthetic standards of remix culture to comment on remix culture itself. For example:

- Youtube Poop: Arthur's Massive, Throbbing Hit

<http://www.youtube.com/watch?v=RJk4N9gEEmk>

APPENDIX B

Interview with Prof. Francesca Coppa
Director of Film Studies at Muhlenberg College
November 18, 2008

Professor Francesca Coppa is the Director of Film Studies at Muhlenberg College and a founding member of the Board of Directors for the Organization for Transformative Works (OTW), a nonprofit organization dedicated to celebrating and preserving fanworks and fan practices, including vidding.

She has written and lectured extensively on vidding and directed a series of short films explaining vidding to middle and high schoolers for MIT's New Media Literacy project.[96] She is also the director of the OTW's "Vidding History" project, which is documenting the oral history of some of the first vidders. Her lectures and publications on vidding include:

"A Fannish Taxonomy Of Hotness," Cinema Journal (forthcoming Summer, 2009)

"Vidding," for Women in Science Fiction and Fantasy: An Encyclopedia, ed. Robin Reid (North Carolina: Greenwood, 2008)

"Women, Star Trek and the Early Development of Fannish Vidding," for Transformative Works and Cultures (Published by the Organization For Transformative Works.) Issue 1, September 15, 2008.[97]

"A Brief History of Media Fandom," in Fan Fiction and Fan Communities in the Age of the Internet, ed. Hellekson & Busse, (MacFarland, 2006) p. 41-59.

Curator, In Media Res, an experiment in collaborative, multi-modal scholarship sponsored by Media Commons.

Panelist, "Media Cannibals: A History of Vidding Women," IP/Gender: Mapping the Connections (American University School of Law, April 4, 2008)

Speaker, "Media Fetish: The Vidshow," Beyond Queer: The Spectacle of the Performing Body (Brown University, April 6, 2008)

Panelist, "From Number One to First Lady: Trek's Christine Chapel and the Development of Fannish Music Video," Slash 3: The Final Cut (Leicester, UK; Feb 25, 2008)

Presenter, "Geneology of Vidding," 24/7: A DIY Video Summit (February 8-10, 2008; School of Cinematic Arts, University of Southern California)

[96] Available at <http://techtv.mit.edu/tags/2522-otw/videos>.

[97] Available at <http://journal.transformativeworks.org/index.php/twc/article/view/44>.

Panelist, "'We are controlling transmission': Female Video Editors and the Literary Music Video," "Creative Transformation: Specificity and Continuity in Unofficial Creative Authorship," MIT5: Creativity, Ownership, and Collaboration in the Digital Age (MIT, April 27-29, 2007)

Panelist, "Media Cannibals: A History of Vidding Women," Inside/Outside: The Gaze and PsychoAnalysis. Feminism(s): Film, Video, and Politics Symposium. (University of Hartford, April 21, 2007)

Could you briefly describe what sets the vidding community apart from other clip-based video creators? Do vidders see themselves as different from many more recent creator communities who have been getting attention on sites like YouTube?

I think that vidders, who are overwhelmingly female, differ from other DIY artists in their aesthetics and purpose. Many vidders use vids to analyze or supplement their mainstream film and television viewing, to draw out their preferred subtextual readings or otherwise reframe visual elements.

Vids are visual essays that respond to a visual source. Many vidders use music to create, extrapolate, or analyze the relationships between characters, or to articulate a character's otherwise opaque interiority. (One of the first VCR vids ever made, in 1980, set the Who's "Behind Blue Eyes" to a single, wavering frame of Starsky from Starsky and Hutch—the best she could do—thereby imputing an interiority and emotional subjectivity to the Starsky character that the show never gave him.)

Vidders tend to feel that they were making "user-generated content" uphill in the snow both ways—that is to say, long before the internet and the rise of digital culture made it much easier. The organized vidding community dates their art form from the slideshows that Kandy Fong made in 1975, and there was a twenty-five year period where VCRs were the dominant technology. Many of the aesthetic and technical problems vidders face existed before the web and digital video. For example, vidders have always wanted to get clean source, to isolate the most beautiful frames, to be able to color tint footage, or otherwise create emotionally meaningful color palettes. They're now artists working mainly with digital tools, but they're trying to solve technical problems and work to aesthetic standards that predate the digital world.

Are most vidders amateurs in video editing? Are their activities generally noncommercial?

Yes, most vidders are amateurs with no professional training in filmmaking or film editing, though many of the best vidders did some sort of art (drawing, painting) at school, and others have technical or computer backgrounds. I have argued that this latter point was important in the vidding community: vidding women tend to be women who are not afraid of technology, and they tend to see vidding as a series of technical challenges without being aware of the legal issues associated with those technologies. The vidding community is a great source of technical and aesthetic mentoring, particularly for women who might not otherwise ever have thought of themselves as filmmakers, but it does not prepare them to deal with the legal questions.

Vidding is entirely noncommercial, part of fandom's "gift culture." Vidders just want to share their work with like-minded fans, and so will stream their vids online, or offer them for download, or give DVDs away at cons. Some vidders charge for the cost of the DVD disc or shipping. (I saw my first vids on VHS, on a tape that was mailed to me for the cost of shipping.)

That being said, non commercial does not mean "not serious." Vidders take their art seriously, and there is a culture of public review and criticism. Moreover, vids are being recognized as "art" in various ways. My essay in *Cinema Journal*, above, is one of three dealing with vids in that issue. Lim's vid "Us," which was shown at 24/7 DIY at USC and was part of Michael Wesch's presentation on YouTube to the Library of Congress, is now going to appear in an exhibition entitled "Mediated" at the California Museum of Photography (January 24, 2009 - April 4, 2009). Luminosity's vid "Vogue" was cited as one of the 20 best user-generated videos of 2007 by *New York Magazine*.[98] Seah and Margie's vid "Handlebars" was sent to the creative team behind *Doctor Who*, who then raved about it in their blog. Those are only three of many recent examples.

Do vidders frequently rip commercially-released DVDs in order to extract clips? It sounds like some vidders use .avis downloaded from unauthorized BitTorrent sources (are all the source materials available that way? obscure shows?). Others rely on video capture from analog outputs. Is DVD viewed as superior to these alternatives?

Vidders want the best-looking footage available, and will rate "crisp source" highly when discussing a vid's merits. While there are some folks who still capture, capturing is more expensive, requires more technical expertise, and typically looks less good. Ripping from DVDs tends to get you better source than downloaded .avis, which are frequently recorded off broadcast television, and may be low-resolution or have bugs or other visual artifacts.

Vidders typically want the cleanest, biggest clips their systems can handle, because they want to transform/rework the footage in various ways—changing speed, color, adding effects, creating manipulations, masking out elements—and the better the footage you start with, the more you can do with it.

This was always a concern, even before DVDs. First generation broadcast tapes (VHS taped off television) were prized; in the days before everything was on DVD, you might only have seen an old show because someone had double-taped their tapes for you, so most vidders were working from tapes of tapes of tapes. Vidders raced to buy the first professional VHS issues of popular fannish shows like *Star Trek* and *Highlander* when they became available, though few TV shows made it to professional VHS. Vidders then bought the DVDs of those same shows when they became available, and are likely customers for anything with bonus footage or extended editions. (For example, the blooper clip version/easter egg clip of Yoda dancing that appeared on the *Star Wars* extended edition was featured in a vid. It is also worth noting that vidders tend to keep every version of a beloved source, so many Star Wars vidders are holding onto their VHS cassettes of *Star Wars* to vid with since Lucas changed the source in subsequent editions.)

Could you make a rough order of magnitude estimate of the number of vids that have been created by self-identified vidders?

By self-identified vidders, tens of thousands easily. That number goes into the millions if you look at YouTube and what organized vidders sometimes call the "feral" vidders—vidders who

[98] Logan Hill, *The Vidder*, New York Magazine, Nov. 12, 2007, available at <http://nymag.com/movies/features/videos/40622/>.

have been inspired by vids they've seen, or have just invented some version of the idea for themselves in their basement, without becoming involved in the community of self-identified vidders.

Is the quality of the video source important to members of the vidding community?

Yes, very much so, see question four, above. I want to reiterate again that vidders are visual artists. They are deeply invested in aesthetics. They want to make smart vids that are also beautiful. And the better the source footage you start with, the more you can do to it, the "shinier" it looks. It is also worth noting that vidding is a real labor of love. Some vidders may spend half a year on a single vid.

Do you think the vidding community has a clear understanding of what the DMCA prohibits, particularly the legal difference between digitally "ripping" a DVD and using the "analog hole" to capture from a DVD?

While vidders tend to think more about copyright and DMCA than the average person, no, I don't think there's a clear understanding of DMCA: certainly not of any legal difference between capturing and ripping.

I'd say that the big legal line many vidders draw is between "paying" and "not paying" for source footage—vidders are likely to pay for DVDs, even to pay multiple times for multiple sets of DVDs, and to feel that they have the right to make art from them.

APPENDIX C

Interview with an anonymous vidder

November 18, 2008

The anonymous subject of this interview has been vidding since 2000. In that time, she has made approximately 30 vids. She has also mentored young vidders, provided "beta" (critique) for dozens of other vidders seeking help with their vids in progress, led panels on vidding at conventions, and curated vid shows.

Could you briefly describe what sets the vidding community apart from other clip-based video creators? Do vidders see themselves as different from many more recent creator communities who have been getting attention on sites like YouTube?

Vidders definitely see themselves as different from other creator communities. The differences are in part historical—we've been doing this since the 1970s—but primarily artistic and aesthetic. Vidding aims to create new meanings from the juxtaposition of video clips and music. These meanings may include parody, criticism, the creation of entirely new stories, meta-discussion, and beyond. Many vidders see themselves as visual storytellers.

Are most vidders amateurs in video editing? Are their activities generally noncommercial?

Very few vidders have any training in film arts or video editing, although a handful have studied them in college.

The vidding community, like the larger media fandom community, has long-held standards against any vidder making a profit from her work. The primary means of distribution is on the Internet, for free. Secondarily, vidders show their vids at conventions, where they are not paid for their submissions. A small number of vidders release collections of their work, often for free, sometimes for the cost of materials and postage. No one makes money from this hobby; in fact, we tend to spend a good deal of money on it, from souped-up computers and external hard drives to high-end professional editing and post-production software to the show DVDs and music we buy.

Do vidders frequently rip commercially-released DVDs in order to extract clips? Is DVD ripping viewed as superior to other available alternatives?

Most vidders I know rip source from commercially-released DVDs. Some also download footage, but not all sources are available for download. Some vidders still use video capture, but the community at large is very concerned with the quality of the footage, and video capture results in noticeable quality loss. Increasingly, Windows-based vidders rip DVDs and work directly with the VOB files in AVISynth in order to avoid any quality loss at all.

Could you make a rough order of magnitude estimate of the number of vids that have been created by self-identified vidders?

I have thousands of vids in my personal collection alone. My guess is that there are tens of thousands of vids in the world at the moment, and that number is increasing all the time.

Is the quality of the video source important to members of the vidding community?

Source quality is very important. It always has been, even when vidders were using videotaped source—dedicated vidders would buy high-end "pro-sumer" machines that could record S-VHS (Super-VHS) for the best possible quality in that medium. You worked from first-generation tapes as much as possible.

Vidders want to create immersive experiences, and they are highly invested in visual communication and aesthetics. Poor-quality source interferes with all of these, hence the community's determination to use the best-quality source footage available.

Do you think the vidding community has a clear understanding of what the DMCA prohibits, particularly the legal difference between digitally "ripping" a DVD and using the "analog hole" to capture from a DVD? How likely is it that vidders will have access to the legal expertise to address these subtle issues?

Some vidders are fairly savvy on copyright issues in general, but as most of us are not lawyers, it doesn't make sense to us to differentiate ripping from video capturing. And increasingly, vidding is being practiced by large numbers of young people who may have no roots in the traditional vidding community, who came of age with the Internet, and who have no sense of the legal restrictions that may affect their hobby. These are the people the rest of us tend to worry most about, in terms of potential legal liability.