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

---

[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.

purchasers. The CDs also conditioned use of the music on unconscionable licensing 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

---

[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

Spore, disables firewalls and other security mechanisms.[34]

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

---

[34] *Id*.

[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]

temporary work assignment abroad—unless she wants to bring her American DVD player as well.

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. Restrictions on Fair Use

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

---

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

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 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