CIRCUMVENTING ACCESS CONTROLS UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT: ANALYZING THE SECUROM DEBATE

DAVID FRY[1]

ABSTRACT

Despite using one of the most sophisticated digital rights management systems currently available, the video game Spore *was illegally downloaded approximately 1.7 million times between September and December of 2008, making it the most widely pirated game of 2008 by more than half a million downloads. This iBrief addresses several legal arguments that have been raised against a digital rights management system called "SecuROM," which is widely used by video game companies like Electronic Arts, the publisher of* Spore*. First, the iBrief discusses the comparisons that have been drawn between SecuROM and the controversial digital rights management technologies previously employed by Sony BMG Music Entertainment. Second, the iBrief addresses the question of whether highly restrictive implementations of SecuROM may be legally circumvented under the Digital Millennium Copyright Act. Third, the iBrief discusses the potential for using the Digital Millennium Copyright Act's three-year rulemaking procedure to obtain certain exemptions for circumventing systems like SecuROM.*

INTRODUCTION

¶1 The release of the video game *Spore* by Electronic Arts highlighted the controversy surrounding software-based digital rights management ("DRM") systems.[2] Software-based DRM systems function as a kind of digital fence to protect the intellectual property rights of copyright owners after their products have been sold to the public. Electronic Arts employed a DRM system in *Spore* that, among other things, requires users to authenticate the product in order to ensure it is a legitimate copy.[3] The inclusion of this DRM system sparked an intense public debate. Consumer

---

[1] J.D. candidate, Duke University School of Law, 2010; B.A. in Philosophy, Wheaton College, 2006. Thanks to Professor Jennifer Jenkins for her invaluable assistance. Any errors are the author's alone.

[2] Andy Greenberg & Mary Jane Irwin, *Spore's Piracy Problem*, FORBES, Sept. 12, 2008, http://www.forbes.com/technology/2008/09/12/spore-drm-piracy-tech-security-cx_ag_mji_0912spore.html.

[3] *Id.*

rights advocates argued that *Spore* and its DRM scheme infringe on the rights of legitimate consumers to use their lawfully purchased goods.[4] On the other side of the debate, copyright owners like Electronic Arts claimed that DRM systems are necessary to prevent infringement of their intellectual property rights, and that the vast majority of legitimate users are completely unaffected by DRM.[5]

¶2 Early software DRM systems were both low-tech and relatively easy to bypass. For example, the original *Warcraft* game released by Blizzard Entertainment in 1994 required the user to type a word from the game manual during installation[6]—a measure that could be easily defeated by merely obtaining a scan or photocopy of the manual. Another popular DRM scheme required the user to input a unique CD Key, a series of characters printed somewhere on the software packaging, to authenticate the product during installation.[7] This proved ineffective, because many websites offered "key generators," which generate a series of characters that the software accepts as a legitimate CD Key.[8]

¶3 Since the beginning of the twenty-first century, software publishers have taken advantage of more advanced hardware- and software-based

---

[4] *Id.*

[5] David Kaplan, *Electronic Arts' Riccitiello: Last Year for "Offline-Only" Games*, PAIDCONTENT.ORG, Oct. 14, 2008, http://www.paidcontent.org/entry/419-media-money-eas-riccitiello-last-year-for-offline-only-games. In discussing Electronic Arts' decision to modify the DRM system that it used for *Spore* after it received many consumer complaints, the company's CEO, John Riccitiello, stated that DRM is "something that 99.8 percent of users wouldn't notice. But for the other .2 percent, it became an issue and a number of them launched a cabal online to protest against it. I personally don't like DRM. It interrupts the user experience. We would like to get around that. But there is this problem called piracy out there." *Id.*

[6] *See Blizzard Support - Warcraft Installation Passwords*, http://us.blizzard.com/support/article.xml?articleId=20912&categoryId=2611&parentCategoryId=&pageNumber=1 (last visited June 12, 2009) (listing the installation passwords for users who wish to install *Warcraft* but no longer have access to the original game manual).

[7] *See, e.g.*, *Retail CD Keys*, https://support.steampowered.com/kb_article.php?ref=7480-wusf-3601 (last visited June 12, 2009) ("The CD Key is a serial number with a combination of . . . letters and numbers - it can be found on a sticker inside your game's case or printed on the game's quick reference card.").

[8] *See* Tim Fisher, *CD Key Generator - Will a Product Key Generator Find My CD Key?*, ABOUT.COM, http://pcsupport.about.com/od/productkeysactivation/f/cdkeygenerator.htm (last visited June 12, 2009).

technological protection measures, such as SecuROM,[9] SafeDisc,[10] and StarForce.[11] These systems typically provide copyright owners with stronger anti-copying protections. For example, some implementations of SecuROM install a small program that checks to see whether a legitimate copy of the software disc is in the computer every time the user attempts to run the protected program.[12] Although this gives copyright owners greater control in preventing illegal uses of their intellectual property, critics have argued that these technological protection measures place an unreasonable burden on consumers by creating security risks for their computers and potentially preventing them from installing the software that they have purchased.[13] Finally, even these technologically advanced methods of copyright protection are still not immune to circumvention. Despite its SecuROM protection, *Spore* was downloaded approximately 1.7 million times between September and December of 2008, making it the most heavily pirated game of 2008 by more than half a million downloads.[14]

¶4 SecuROM, the DRM system used in *Spore*, is the source of the most recent legal debate about software-based DRM. The two particular legal issues that this iBrief will address are (1) whether SecuROM is substantially similar to the rootkit software that the Federal Trade Commission ("FTC") essentially prohibited in 2007 and (2) whether a product that circumvents SecuROM's technological protection measures could be legal under the Digital Millennium Copyright Act ("DMCA"). Section I of this iBrief outlines the technical details of SecuROM and frames the current legal controversy surrounding the product. Section II discusses the significant distinctions between SecuROM and the rootkit software condemned by the FTC in 2007. Section III evaluates SecuROM in light of the DMCA's anti-circumvention provisions, arguing (1) that certain methods of circumventing SecuROM might not violate the DMCA's anti-circumvention provisions and (2) that an entity seeking an exemption

---

[9] *SecuROM Frequently Asked Questions* at 1.1–1.2, http://www.securom.com/support_faq.asp [hereinafter *SecuROM FAQ*] (last visited June 12, 2009).

[10] Lisa Vaas, *Windows Users Getting Bitten by Macrovision Zero Day*, EWEEK.COM, Nov. 5, 2007, http://www.eweek.com/c/a/Security/Windows-Users-Getting-Bitten-by-Macrovision-Zero-Day; *see also Microsoft Security Advisory*, Nov. 5, 2007, http://www.microsoft.com/technet/security/advisory/944653.mspx.

[11] Nate Anderson, *It's Official: Ubisoft Dumps StarForce*, ARS TECHNICA, Apr. 14, 2006, http://arstechnica.com/old/content/2006/04/6603.ars.

[12] *See, e.g.*, *SecuROM FAQ*, *supra* note 9, at 4.4.

[13] *See* Greenberg, *supra* note 2; *see also infra* notes 32–36, 141–43 and accompanying text.

[14] *Spore at Top of Piracy Charts*, BBC NEWS, Dec. 10, 2008, http://news.bbc.co.uk/1/hi/technology/7772962.stm.

authorizing it to bypass the DMCA's anti-circumvention provisions would almost definitely fail to meet the high evidentiary burden.

I. WHAT IS SECUROM?

A. How SecuROM Works

¶5 SecuROM is a highly customizable DRM system developed and sold by Sony DADC.[15] SecuROM operates using two different components: a hardware component and a software component. The hardware component prevents direct copying of a disc. The software component first requires a user to activate her license in order to install the protected software, and then encrypts the program once it has been installed on the user's computer to prevent further copying.[16]

¶6 When the user inserts a SecuROM-branded disc into her computer, the SecuROM software is installed contemporaneously with the main program on the disc.[17] A copyright owner typically requires a user to activate her license during this installation, unless the copyright owner has chosen to use only the disc-based activation features of SecuROM.[18] The copyright owner can also configure SecuROM to require this online activation only during the initial installation, after a specific number of launches, or after a pre-determined period of time.[19] The number of simultaneously activated copies of the software that a user may have at any given time is entirely at the discretion of the copyright owner.[20] For example, *Spore* permits the user to activate the game up to five times, and these activations can be "revoked" and later re-used by running a special program available directly from Electronic Arts.[21] Another Electronic Arts product, the game *Mass Effect*, only allows users to install the game three times, and these activations cannot be "revoked."[22] According to SecuROM, this feature is highly customizable, with a company conceivably able to limit users to a single, non-revocable activation.[23]

---

[15] *SecuROM FAQ*, *supra* note 9, at 1.1–1.2.
[16] *Id.* at 1.2.
[17] *Id.* at 2.2.
[18] *Id.* at 1.2.
[19] *Id.* at 4.4.
[20] *Id.*
[21] *Spore De-Authorization Tool*, http://www.spore.com/patch/deauthorization (last visited June 12, 2009).
[22] *Official BioWare/Electronic Arts Response to DRM Discussion*, May 9, 2008, http://masseffect.bioware.com/forums/viewtopic.html?topic=629059&forum=125 [hereinafter *BioWare/Electronic Arts Response*].
[23] *See SecuROM FAQ*, *supra* note 9, at 4.4.

¶7 SecuROM's software component has two other important features. First, it can determine whether there have been any hardware changes to the user's computer since the last time the user ran the protected program.[24] Again, the extent to which this feature limits the user is at the discretion of the company employing SecuROM.[25] One company might allow a user to make significant hardware changes without requiring re-activation, whereas another company might require a user to re-activate her software after performing a single, relatively minor change, like upgrading her computer's graphics card.[26] Second, SecuROM can detect whether the user has any emulation software running on her computer, which might enable the user to run a modified version of the protected software that bypasses the activation or authentication requirements.[27] Thus, SecuROM is capable of placing significant limitations on the way in which consumers are able to use their SecuROM-protected products.

B. Controversy and Legal Action

¶8 Electronic Arts initially planned to permit only three installations of *Spore*.[28] This plan was met with significant consumer backlash, causing Electronic Arts to modify the activation limit of SecuROM to permit five installations.[29] The company also developed a software tool that allows users to revoke their activations.[30] Finally, Electronic Arts has repeatedly stated that if users have reached the activation limit and legitimately need additional activations, they can call the company's technical support hotline and the company will grant additional activations on a case-by-case basis.[31] Despite these concessions, on September 22, 2008, an owner of a copy of *Spore* filed a class action lawsuit against Electronic Arts in the United

---

[24] *Id.* at 4.3.
[25] *Id.*
[26] *Id.* The SecuROM FAQ states that "SecuROM can be configured by the publisher to be more lenient or more strict with regards to changes to the system configuration. This means that publishers can configure the tolerance threshold at their own discretion, so there might be applications which do not tolerate a single change and there might be other applications which tolerate many major changes." *Id.*
[27] *Id.* at 2.9.
[28] *Electronic Arts Responds To DRM Complaints*, KOTAKU, Sept. 19, 2008, http://kotaku.com/5052473/ea-respond-to-drm-complaints [hereinafter *Electronic Arts Response*].
[29] *Id.*
[30] *Id.*; *Spore De-Authorization Tool*, *supra* note 21.
[31] *See infra* notes 136–37 and accompanying text.

States District Court for the Northern District of California.[32] The plaintiff alleges that Electronic Arts violated California's consumer protection statute, unfair competition law, and the common law prohibition against trespass to chattels.[33] The law firm representing the plaintiffs in the *Spore* case also represents plaintiffs in two similar lawsuits against Electronic Arts concerning two other SecuROM-protected video games.[34] At least two other similar complaints have been filed against Electronic Arts.[35] One important aspect of these lawsuits is that the plaintiffs allege that their computers were actually damaged by the SecuROM software,[36] although it is still unclear whether there is any evidence to support their claims. In the following two sections, this iBrief will address the legal issues related to (1) the FTC's order in the Sony BMG Music Entertainment ("Sony BMG") rootkit case, and (2) SecuROM as it relates to the DMCA's anti-circumvention provisions.

II. SECUROM AND THE SONY BMG FTC ORDER

A. Sony BMG's DRM and the FTC

¶9 In 2005, a security researcher discovered that Sony BMG's Extended Copy Protection ("XCP") DRM system, which it used on many of its music CDs, installed a program called a rootkit when users inserted these

---

[32] Complaint, Thomas v. Electronic Arts, Inc., Case No. 5:08-cv-04421-PVT (N.D. Cal. Sept. 22, 2008), *available at* http://www.courthousenews.com/2008/09/23/Spore.pdf.

[33] *Id.* at ¶¶ 51, 59, 73.

[34] Complaint, Eldridge v. Electronic Arts, Inc., Case No. 3:08-cv-04733-BZ (N.D. Cal. Oct. 14, 2008) (class action lawsuit based on the use of SecuROM in *Spore Creature Creator*), *available at* http://media.libsyn.com/media/gamepolitics/EA-spore-eldridge-vs-ea.pdf; Complaint, Gardner v. Electronic Arts, Inc., Case No. 5:08-cv-04629-RS (N.D. Cal. Oct. 6, 2008) (class action lawsuit based on the use of SecuROM in *Mass Effect*), *available at* http://www.courthousenews.com/2008/10/08/MassEffect.pdf.

[35] Complaint, McQuown v. Electronic Arts, Inc., Case No. 4:2008cv05373 (N.D. Cal. Nov. 26, 2008) (class action lawsuit based on the use of SecuROM in *Spore Creature Creator*), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/4:2008cv05373/209262/1/; Complaint, Cortez v. Electronic Arts, Inc., Case No. 3:08-cv-04917-SC (N.D. Cal. Oct. 27, 2008) (class action lawsuit based on Electronic Arts' use of SecuROM in several different titles), *available at* http://media.libsyn.com/media/gamepolitics/EA-securom-cortez-vs-ea.pdf.

[36] *See, e.g.*, Complaint, *Thomas*, at ¶ 20.

music CDs into their computers.[37] Rootkits are programs that give a user access to the most privileged level of a computer system, giving the person in control of the program virtually unlimited access to make changes to the computer while "effectively hiding their existence and operation from both a computer's user and the machine's operating system."[38] Because of this level of control, rootkits are often used by hackers to prevent their malicious actions from being detected by other applications running on the computer.[39]

¶10 A program that provides access to a user's entire computer poses a significant security risk to the system.[40] At the same time, Sony BMG was also using another DRM system called MediaMax. MediaMax was also installed when a user inserted the disc into her CD-ROM drive.[41] Although the MediaMax program did not have root access, it created a similar vulnerability in which hackers could gain full administrator privileges over the computer by modifying the MediaMax folder from a less privileged guest account on the computer.[42]

¶11 When a user inserted an XCP-protected Sony BMG CD in the computer's CD-ROM drive, she was greeted by an End User License Agreement ("EULA") informing her that the CD would have to install a small program before the CD could be used to play music or copy files.[43] The CD packaging itself typically contained little information other than a notice that the disc was "Content Protected" and a list of the system requirements necessary for using the disc on a computer. Sony BMG provided the user with negligible advance warning that the DRM software was going to be installed or what the software would actually do.[44] Furthermore, MediaMax partially installed itself as soon as the user inserted the disc, even before she had an opportunity to read and accept the EULA.[45] These undisclosed security vulnerabilities prompted the FTC to file a complaint against Sony BMG for its deceptive practices in using XCP and MediaMax.[46]

---

[37] Deirdre K. Mulligan & Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L.J. 1157, 1159 (Summer, 2007).
[38] *Id.* at 1159–60.
[39] *Id.* at 1160.
[40] *Id.*
[41] *Id.* at 1161.
[42] *Id.* at 1161–62.
[43] *Id.* at 1208.
[44] *Id.* at 1168.
[45] *Id.* at 1163.
[46] *See* Complaint, *In re* Sony BMG Music Entertainment, Docket No. C-4195, *available at* http://www.ftc.gov/os/caselist/0623019/0623019cmp070629.pdf.

¶12 In its complaint against Sony BMG, the FTC emphasized that XCP and MediaMax both exposed users to significant security risks—XCP by enabling root access to a user's computer and MediaMax through its ability to allow hackers to obtain heightened security privileges over a user's system.[47] The FTC further stressed the fact that it was extremely difficult to locate and uninstall XCP and MediaMax.[48] Neither program appeared in the Add/Remove Programs menu on users' computers, and both programs were disguised in a way that made it difficult to manually uninstall them.[49] Ultimately, the FTC and Sony BMG reached a settlement agreement in which the FTC issued an order requiring heightened notice requirements whenever the use of a CD is conditioned on the installation of particular kinds of DRM software.[50] The FTC required Sony BMG to "clearly and prominently" disclose information about the exact nature of the technological protection measures it employs, both on the product packaging and in the EULA.[51] These heightened notice requirements ensure that consumers have adequate information to decide whether they are willing to expose their computers to the potential security risks associated with Sony BMG's technological protection measures.[52]

¶13 The FTC imposed several additional requirements with respect to the use of XCP and MediaMax. First, the FTC stated that Sony BMG "shall not install or cause to be installed on a consumer's computer any content protection software that prevents the consumer from readily locating or removing the software . . . ."[53] The FTC further stated that this type of software may not be disguised by "hiding or cloaking files, folders, or directories,"[54] suggesting that rootkit technologies like XCP necessarily violate the terms of the order.[55] Second, the FTC prohibited Sony BMG from "install[ing] or caus[ing] to be installed on a consumer's computer any content protection software unless [the company] provides a reasonable and effective means for consumers to uninstall the software."[56] Thus, even if Sony BMG provides clear and prominent notice about the DRM systems it

---

[47] *Id.* at ¶¶ 13–14.
[48] *Id.* at ¶¶ 15–16.
[49] *Id.*
[50] *See* Decision and Order at 3–5, *In re* Sony BMG Entertainment, Docket No. C-4195, June 28, 2007, *available at* http://www.ftc.gov/os/caselist/0623019/0623019do070629.pdf; *see also* Mulligan, *supra* note 37, at 1215–16.
[51] Decision and Order, In re *Sony BMG*, at 3–5.
[52] *See* Mulligan, *supra* note 37, at 1217.
[53] Decision and Order, In re *Sony BMG*, at 5.
[54] *Id.*
[55] Mulligan, *supra* note 37, at 1217.
[56] Decision and Order, In re *Sony BMG*, at 6.

employs, consumers have the right to reject the terms of Sony BMG's product installation and uninstall the software at a later date.

B. Distinguishing SecuROM from the Sony BMG Case

¶14 Although there have been allegations that SecuROM poses similar security risks to the technological protection measures in the Sony BMG case,[57] there are a few key differences that may compel the FTC to reach a different result should it choose to investigate Sony DADC. As an initial matter, Sony DADC maintains that SecuROM operates at the normal application level rather than at the more privileged root level.[58] This would mean that it is unlikely to pose the same security risk as XCP, and therefore would not be explicitly barred by the FTC order. Although one of the plaintiffs in the pending lawsuits against Electronic Arts asserts that SecuROM installs itself at the root level,[59] no reliable news outlets have given any indication that SecuROM is installed anywhere other than the normal application level. Further, unlike MediaMax, there have been no reliable reports that SecuROM enables privileged access to a user's computer.

¶15 Also, unlike XCP and MediaMax, SecuROM appears to be fairly easy to uninstall. Users who wish to remove SecuROM can simply visit the company's website, which contains step-by-step instructions for downloading and running a tool that will uninstall the product from the user's computer.[60] Although the SecuROM removal tool leaves some information on users' computers, it only leaves the files that are necessary to determine "whether the consumer has reached the limit of permitted copies of the covered product, or other comparable content protection data,"[61] which is explicitly permitted by the FTC as long as the company gives proper notice and the remaining data does not adversely affect users' computers.[62] Therefore, the FTC is likely to view SecuROM as more innocuous than both of those technologies.

¶16 Furthermore, SecuROM and the companies who use it appear to be far more open in their publicity about the nature of the product. For example, the EULA template currently employed by Electronic Arts states:

> Our Software uses access control and copy protection technology. An internet connection is required to authenticate the Software and verify

---

[57] *See supra* note 36 and accompanying text; *infra* notes 141–43 and accompanying text.
[58] *SecuROM FAQ*, *supra* note 9, at 2.3, 2.14–2.15.
[59] *See, e.g.*, Complaint, *Thomas*, *supra* note 32,at ¶¶ 11–12.
[60] *SecuROM FAQ*, *supra* note 9, at 3.2.
[61] Decision and Order, In re *Sony BMG*, *supra* note 50, at 6.
[62] *Compare id. with SecuROM FAQ*, *supra* note 9 at 3.2–3.3.

> your license. EA reserves the right to validate your license through subsequent online authentication. If your license is not valid you may not be able to use the Software. The first end user of this License can install and authenticate the Software on a set number of machines which may vary by product. The installation of EA Download Manager, the registration of the Software, and the acceptance of additional terms may be required to access online services and download and apply Software updates and patches. Only licensed software can be used to access online services and download and apply updates and patches. If the Software permits access to additional online features, only one copy of the Software may access those features at one time. If you disable or otherwise tamper with the technical protection measures, the Software will not function properly.[63]

¶17 In contrast, Sony BMG's EULA "explicitly disavowed any collection or dissemination of data related to customers or their computers"[64] and "[c]omponents of these [technological protection] measures were installed . . . before customers were confronted with the EULA terms."[65] Thus, not only were the DRM systems potentially harmful to users' computers, but consumers typically had no way of knowing beforehand what was going to be installed when they inserted their newly purchased CDs.

¶18 Electronic Arts in particular has been very willing to disclose the precise nature of SecuROM,[66] again standing in stark contrast to Sony BMG's public disavowals of the true nature of its DRM software.[67] This greater level of openness with consumers represents a further departure from Sony BMG's behavior, and suggests that SecuROM has substantially followed the guidelines in the FTC order. Thus, unless details emerge that reveal that SecuROM poses a greater security risk than Sony DADC has claimed, the relatively innocuous nature of SecuROM and the openness with which Sony DADC and companies like Electronic Arts have treated it would probably compel the FTC to find that the current use of SecuROM does not run afoul of the espoused guidelines in the Sony BMG rootkit order.

---

[63] Electronic Arts, *End User License Agreement*, http://tos.ea.com/legalapp/eula/US/en/PC/ (last visited June 12, 2009).
[64] Mulligan, *supra* note 37, at 1167–68.
[65] *Id.*
[66] *See, e.g.*, *supra* notes 22, 28–31 and accompanying text.
[67] As an example of Sony BMG's public posture while the rootkit story was unfolding, a high-level Sony BMG employee stated at the time that "'most people, I think, don't even know what a rootkit is, so why should they care about it?'" Dan Mitchell, *The Rootkit of All Evil*, N.Y. TIMES, Nov. 19, 2005, at C5.

III. EVALUATING SECUROM UNDER THE DMCA'S ANTI-CIRCUMVENTION PROVISIONS

A. The DMCA's Anti-Circumvention Provisions

¶19 The DMCA, enacted by Congress in 1998 as an overhaul of the U.S. Copyright Act, includes a section discussing circumvention of DRM systems, stating that "[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title."[68] The DMCA also prohibits the manufacturing or distributing of products designed to circumvent technological access controls protecting copyrighted works.[69] The Act further protects against the trafficking of products that circumvent anti-copying controls.[70]

¶20 Three important court decisions interpreting these provisions of the DMCA are *Universal City Studios, Inc. v. Corley*,[71] *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*,[72] and *Storage Technology Corp. v. Custom Hardware Engineering, Inc.*[73] In *Corley*,[74] the defendant Eric Corley operated a website where he published links to other websites where users could download a program called DeCSS.[75] This program enables users to bypass Content Scramble System ("CSS"), the DRM system used to prevent copying and unauthorized viewing of DVDs.[76] Eight major film studios sued Corley, alleging that the use and dissemination of DeCSS violated the DMCA's anti-circumvention and anti-trafficking provisions by enabling users to circumvent CSS, a technological protection measure that effectively controls access to the underlying film on the DVD.[77] The studios alleged that Corley, by providing links to websites where users could find DeCSS, was violating the DMCA's anti-trafficking provision,

---

[68] 17 U.S.C. § 1201(a)(1)(A) (2007); *see generally* U.S. COPYRIGHT OFFICE SUMMARY OF THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998, Dec. 1998, *available at* http://www.copyright.gov/legislation/dmca.pdf (discussing the various provisions of the DMCA and the rationale behind their inclusion in the statute). This provision, and only this provision, is subject to an exemption process. *See infra* notes 124–33 and accompanying text. This process allows groups and individuals who have been, or are likely to be, adversely affected by this provision to seek three-year exemptions to make non-infringing uses of particular classes of protected works. *See id.*

[69] 17 U.S.C. § 1201(a)(2) (2007).

[70] *Id.* at § 1201(b)(1).

[71] 273 F.3d 429 (2d Cir. 2001).

[72] 381 F.3d 1178 (Fed. Cir. 2004).

[73] 421 F.3d 1307 (Fed. Cir. 2005).

[74] 273 F.3d at 429.

[75] *Id.* at 435–36.

[76] *Id.*

[77] *Id.* at 436.

specifically the prohibition on providing or offering of circumvention tools to the public.[78]

¶21 The Second Circuit Court of Appeals decided in favor of the film studios, affirming the decision of the district court.[79] In evaluating the "dual use" aspect of DeCSS, the circuit court favorably quoted the district court judge, who stated:

> Every recipient is capable not only of decrypting and perfectly copying plaintiffs' copyrighted DVDs, but also of retransmitting perfect copies of DeCSS and thus enabling every recipient to do the same. They likewise are capable of transmitting perfect copies of the decrypted DVD. The process potentially is exponential rather than linear.[80]

¶22 Thus, even if DeCSS were capable of certain lawful uses, the fact that it can also be used to facilitate widespread infringement caused the court to find that there is no reasonable way to limit the uses of DeCSS other than issuing injunctions against those who knowingly disseminated the unlawful circumvention software.[81] In holding for the motion picture studios, the court emphasized that "[p]osting DeCSS on [Corley's] web site makes it instantly available at the click of a mouse to any person in the world with access to the Internet,"[82] and that linking to other websites that contained DeCSS "facilitate[d] instantaneous unauthorized access to copyrighted materials by anyone anywhere in the world."[83]

¶23 On the other side of the spectrum, *Chamberlain*[84] and *Storage Technology*[85] suggest that some courts might be willing to find circumvention of a technological protection measure is lawful when the protection measure is not rationally related to protecting the exclusive rights afforded by copyright law.[86] In *Chamberlain*,[87] the plaintiff, Chamberlain

---

[78] *Id.*
[79] *Id.* at 459–60.
[80] *Id.* at 452 (quoting Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 331–32 (S.D.N.Y. 2000)).
[81] *Id.* at 457–58.
[82] *Id.* at 454.
[83] *Id.* at 457.
[84] Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004).
[85] Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., 421 F.3d 1307 (Fed. Cir. 2005).
[86] *See also* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522, 549–50 (6th Cir. 2004) (holding that a company that specialized in aftermarket printer cartridges did not violate the DMCA when it sold printer cartridges that circumvented the printer's embedded software that was designed to prevent users from installing third party cartridges).
[87] 381 F.3d at 1178.

Group, Inc., had developed a new garage door technology known as rolling code technology.[88] This technology was supposedly more secure than previous garage door openers because the opener required the transmitter to submit two codes to open the door: a fixed identification code that was set when the user initially programmed the transmitter and a rolling code that automatically changed every time the user opened the garage door.[89] The system first required users to synchronize their Chamberlain transmitters with their Chamberlain garage door openers, and then the software embedded in the Chamberlain garage door opener would only open the door when it received the programmed codes from the transmitter.[90]

¶24 Skylink Technologies, Inc., a company that specialized in aftermarket garage door transmitters, developed a universal remote control that was capable of operating the Chamberlain garage door opener without using the same rolling code technology.[91] Although Skylink did not use the same technology as Chamberlain's transmitters, the Skylink transmitter could still be synchronized with the Chamberlain garage door opener in order to program the first fixed signal.[92] After programming the Skylink transmitter, every time a user operated the transmitter it would send three signals: a modified fixed signal that identified the transmitter to the garage door opener and attempted to open the door and two additional fixed signals that simulated the effect of the rolling code technology by re-synchronizing the transmitter with the opener.[93] Chamberlain sued Skylink under the DMCA, claiming that the universal transmitter constituted a violation of the DMCA's prohibitions against circumventing access control technologies and distributing the tools necessary to enable such circumvention.[94]

¶25 In ruling for Skylink, the Court of Appeals for the Federal Circuit did not focus on whether the rolling code technology was a technological protection measure that controlled access to the embedded program in Chamberlain's garage door opener, or whether Skylink's transmitter circumvented that technological protection measure.[95] Rather, in distinguishing this case from the district court's decision in *Corley*,[96] the court emphasized the fact that Skylink's "accused products enable only

---

[88] *Id.* at 1183.
[89] *Id.*
[90] *Id.* at 1184.
[91] *Id.* at 1184–85.
[92] *Id.*
[93] *Id.* at 1185.
[94] *Id.* at 1183.
[95] *Id.* at 1191.
[96] *See* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).

legitimate uses of copyrighted software."[97] Therefore, if the court held in favor of Chamberlain and enjoined Skylink from distributing its universal transmitters, the court would have effectively allowed Chamberlain to use the DMCA to "[eliminate] all existing consumer expectations about the public's rights to use purchased products" solely because Chamberlain had employed a technological protection measure to control access to its garage door opener software.[98] The DMCA created no such new property right, but rather gave copyright owners a method of protecting against the circumvention of technological protection measures that were designed to protect the exclusive rights afforded to copyright owners by the Copyright Act.[99] Therefore, the court held that the DMCA "prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners."[100]

¶26 Finally, a Federal Circuit case after *Chamberlain* suggests that the non-infringing nature of circumvention may preclude a plaintiff from succeeding in a DMCA action, even if the circumventing act or tool created the potential for copyright infringement. In *Storage Technology*,[101] the plaintiff, Storage Technology Corp. ("StorageTek"), manufactured data libraries, and the defendant, Custom Hardware Engineering & Consulting, Inc. ("CHE"), was a company that repaired StorageTek data libraries.[102] In order to repair the libraries, CHE had to access the data library control software to ensure that it was properly configured to transmit error messages.[103] In order to access this software, CHE needed to bypass a password system employed by StorageTek to restrict access to the control unit, and CHE used two different tools to accomplish this circumvention.[104] As StorageTek. computer code was protected by copyright,[105] CHE would appear to have "circumvent[ed] a technological measure that effectively controls access to a work protected under [the DMCA]."[106]

¶27 However, the court held for CHE on the DMCA claim for largely the same reasons that it held for Skylink. Although the tools that CHE used to circumvent the technological protection measure gave it access to use StorageTek's copyrighted computer code, these tools did not facilitate

---

[97] *Chamberlain*, 381 F.3d at 1198.
[98] *Id.*
[99] *Id.* at 1202.
[100] *Id.*
[101] Storage Tech. Corp. v. Custom Hardware Eng'g, Inc., 421 F.3d 1307 (Fed. Cir. 2005).
[102] *Id.* at 1309–10.
[103] *Id.* at 1310.
[104] *Id.*
[105] *Id.* at 1309.
[106] 17 U.S.C. § 1201(a)(1)(A) (2007).

copyright infringement because their use did not actually enable the users of those tools to make copies of StorageTek's code or otherwise infringe its copyright.[107] Thus, these tools did not "facilitate" infringement for the purposes of the DMCA, and therefore, "[t]here [was] simply not a sufficient nexus between the rights protected by copyright law and the circumvention of [StorageTek's password system]."[108] The court then held that in order to support a valid DMCA claim, the alleged violation must either "constitute copyright infringement or facilitate copyright infringement."[109]

¶28 On its face, the statutory language of the DMCA's anti-circumvention provisions seems to suggest that it is unlawful to circumvent, or facilitate the circumvention of, any technological protection measure that controls access to or prevents infringement of a copyrighted work. In *Corley*, the Second Circuit appeared to support this proposition by holding that DeCSS was unlawful regardless of its non-infringing, lawful uses. The *Chamberlain* and *Storage Technology* court, on the other hand, tempers this approach by holding that circumvention of a technological protection measure only runs afoul of the DMCA's anti-circumvention provisions if the technological protection measure is rationally related to protecting the copyright owner's intellectual property rights.

B. Is the Targeted Use Plainly Lawful?

¶29 In evaluating SecuROM under the DMCA, it is important to note that as in *Corley*, *Chamberlain*, and *Storage Technology*, there are situations in which SecuROM protection might prevent a consumer from engaging in a plainly lawful use of her purchased software. For example, it is possible that a software publisher could implement a version of SecuROM that does not allow users to "revoke" their activations, and any changes to a user's hardware configuration will require the user to re-activate her software. If this user reaches her maximum number of installations and her operating system then crashes or she upgrades part of her computer, her product may cease to function until she finds some way to re-activate it. Even if this user were able to obtain an additional activation from the publisher, the consumer might wish to avoid the inconvenience of calling the publisher every time she needs to re-install her product, and prefer instead to install her software by using an aftermarket tool that circumvents the activation requirement.

¶30 Thus, using a physical copy of the software disc to reinstall legitimately purchased software for personal use is clearly a lawful use of

---

[107] *Storage Tech.*, 421 F.3d at 1319.
[108] *Id.*
[109] *Id.* at 1318 (citing Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1202 (Fed. Cir. 2004)).

the product.[110] This implementation of SecuROM, however, would prevent the user from engaging in this lawful act. Therefore, like the owner of a Chamberlain garage door opener who merely wants to be able to open her garage door, a user of SecuROM-protected software could have an entirely legitimate, legal reason for wishing to circumvent the SecuROM activation limit.

¶31 This hypothetical situation is certainly plausible, especially given the fact that some implementations of SecuROM already do not allow users to revoke their activations once they have been used.[111] Although there is no indication that Electronic Arts will renege on its commitment to continue supporting access to its titles, it would not be unprecedented for a company that uses DRM to discontinue its support for customers who are no longer able to access the products that they purchased. For example, a DMCA exemption proposal was recently filed with the Copyright Office that requests an anti-circumvention exemption for users who have purchased DRM-protected products from now-defunct service providers.[112] This proposal relies heavily on examples from the music industry, in which many online digital music distribution services have closed their doors and left their customers with no way to authenticate their DRM-protected music files.[113] Similarly, then, it is quite possible that a user will purchase a SecuROM-protected product with limited, server-based activations from a company that will eventually go out of business and leave the user with no method of securing an additional activation for legitimate uses of the software.[114]

¶32 Furthermore, it is plausible that a software tool could be developed solely to allow consumers to engage in this kind of clearly lawful use. As previously discussed, SecuROM has hardware and software measures in place to ensure that the individual using the protected product is an authorized user.[115] Thus, if a tool only permitted a user to circumvent the activation limit, it is unclear how this kind of tool would serve any purpose other than enabling consumers to engage in clearly legal uses of their purchased products.

---

[110] *See, e.g.*, 17 U.S.C. § 117(a)(1) (2007) (permitting users to make a reproduction of a copyrighted program as long as the reproduction "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").
[111] *See supra* note 22 and accompanying text.
[112] *See infra* notes 145–48 and accompanying text.
[113] *Id.*
[114] *Id.*
[115] *See supra* notes 16–27 and accompanying text.

C. Circumvention of SecuROM Under the DMCA

¶33 The facts surrounding circumvention of SecuROM's activation limit appear to fall somewhere between those of the Second Circuit's decision in *Corley* and the Federal Circuit's decisions in *Chamberlain* and *Storage Technology*. Unlike the use of DeCSS in *Corley*, the targeted use of the protected product would be clearly legal because it could only be used to circumvent the activation requirement that is preventing the user from installing her software. In contrast, as the Second Circuit stated in *Corley*, "'the evidence as to the impact of the anti-trafficking provision[s] of the DMCA on prospective fair users is scanty and fails adequately to address the issues,'"[116] suggesting that it might be plausible for users to legally circumvent protected products if there is adequate evidence that users' lawful use rights have been adversely affected. Also, circumventing the activation limit on a SecuROM-protected product would not enable the instant mass distribution that troubled the *Corley* court because the other technological protection measures of SecuROM would still be in place.[117] Thus, in this hypothetical scenario, there would be substantial evidence that the activation limit significantly restricts the ability of users to make non-infringing uses of their software, potentially distinguishing SecuROM from CSS.

¶34 Furthermore, as in *Chamberlain* and *Storage Technology*, a non-revocable activation limit in a SecuROM-protected program could prevent users from engaging in plainly legal uses of their software, such as the ability to reinstall the program after a computer crash or minor hardware upgrade. Thus, it is quite possible that this fact could compel a court to find that a manufacturer in such a case was attempting to use the DMCA to prevent access to the underlying software, rather than to protect the plaintiff's intellectual property rights. It is reasonable for a purchaser of computer software to assume that she will be able to do normal things with the software like reinstalling it. Therefore, if the only way to reinstall a program is to circumvent the SecuROM activation limit, using the DMCA to prohibit circumvention would interfere with the consumer's reasonable expectations in purchasing the software without furthering the goal of protecting the copyright owner's rights under the Copyright Act.

¶35 On the other hand, *Chamberlain* applied to a technological protection measure used to protect embedded software from being accessed by competitors to create aftermarket devices.[118] Sony DADC might argue

---

[116] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 459 (2d Cir. 2001) (quoting Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 338 n.246 (S.D.N.Y. 2000)).

[117] *See supra* notes 16–27 and accompanying text.

[118] *See supra* notes 98–100 and accompanying text.

that SecuROM is more similar to CSS, because companies like Electronic Arts implement SecuROM in order to protect their intellectual property rights, not merely to prevent unauthorized access to the underlying works. Thus, even if the targeted use is clearly legal—such as circumventing the activation limit in order to reinstall a legally purchased program—the technological protection measure may still be considered a reasonable attempt to protect the copyright owner's exclusive intellectual property rights. According to *Corley*, the most important fact was not that consumers could use DeCSS for non-infringing uses, but rather that consumers could use DeCSS to make and distribute perfect digital copies of the plaintiffs' copyrighted work.[119] Certainly, not every use of DeCSS would constitute copyright infringement, but CSS itself is a technological protection measure that was reasonably designed and implemented to protect the legal interests of copyright owners. Likewise, SecuROM's activation limit may create a burden for some individual users, but the interdependent package of all of SecuROM's components may be the only reasonable way for copyright owners to protect their rights.

¶36 However, if users are unable to install their legally purchased software without circumventing SecuROM's activation limit, it seems to be a plausible reading of *Storage Technology* that this circumvention is lawful unless the "access was intertwined with a right protected by the Copyright Act."[120] Thus, even if the activation limit were an interdependent part of the SecuROM system of preventing copyright infringement, circumvention of the activation limit would probably be authorized as long as the access itself did not facilitate or enable infringement of the copyright owner's rights.

¶37 If there is a situation in which users are legally able to circumvent one of SecuROM's components, the DMCA's anti-trafficking provisions will probably not preclude the production and distribution of certain software tools that are necessary for users to engage in legal circumvention. The best-case scenario for a developer of this kind of circumvention tool would involve a product that enables circumvention of the activation limit while leaving the other technological protection measures intact, so that its only function is to allow users to circumvent the activation requirement. As discussed above, SecuROM is capable of using hardware protections on the physical installation disc in order to prevent direct copying of the underlying program, as well as software protections to enable online

---

[119] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 452 (2d Cir. 2001) (quoting Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 331–32 (S.D.N.Y. 2000)).

[120] Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc., 421 F.3d 1307, 1318 (Fed. Cir. 2005).

authentication of the software.[121] *Chamberlain* and *Storage Technology* suggest that some courts might not have so readily affirmed an injunction against linking to DeCSS if the technological protection measure in question had placed a demonstrably significant burden on lawful users without furthering the goal of protecting the plaintiff's intellectual property rights. Thus, if a product could be developed that only circumvented the activation limit, and if it could be demonstrated that the activation limit has created a significant burden on lawful uses of the protected software, then such a tool might avoid the *Corley* problem of needing to prohibit dual-use technologies. Such a program might, then, be considered lawful under the anti-trafficking provisions.

D. Analyzing Whether Users of Products Protected by Highly Restrictive SecuROM Implementations Should Be Exempted from the DMCA

1. The Evidentiary Burden in the Rulemaking Procedure

¶38 Since the enactment of the DMCA in 1998, every three years the Register of Copyrights evaluates applications for exemptions to the DMCA's prohibition against user circumvention of access controls.[122] The Register then makes recommendations to the Librarian of Congress on whether to grant or deny the requested exemptions.[123] In order to qualify for an exemption, the DMCA requires evidence that "persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the [anti-circumvention prohibition] in their ability to make noninfringing uses . . . of a particular class of copyrighted works."[124] The Register of Copyrights approves very few of these applications, suggesting that the evidentiary burden is extremely high.[125]

¶39 In order to obtain an exemption, the entity proposing the exemption has the burden of demonstrating that some kind of actual adverse impact on the ability of users to engage in lawful, non-infringing activities has resulted from the lack of an exemption or that "adverse effects are more likely than

---

[121] *See supra* note 16 and accompanying text.
[122] 17 U.S.C. § 1201(a)(1)(B)–(C) (2007). This exemption process only applies to the anti-circumvention provision of the DMCA, not to either of the anti-trafficking provisions. *Id.*; *see also supra* notes 70–71 and accompanying text.
[123] 17 U.S.C. § 1201(a)(1)(B)–(C) (2007).
[124] *Id.*
[125] *See generally* Marybeth Peters, Register of Copyrights, *2006 Recommendation of the Register of Copyrights*, Nov. 17, 2006, *available at* http://www.copyright.gov/1201/docs/1201_recommendation.pdf (recommending only six exemptions out of seventy-four submitted requests).

not to occur."[126] The most compelling evidence of actual harm comes from first-hand accounts of instances in which users were harmed by the lack of an exemption, and theoretical critiques alone are insufficient to meet the evidentiary burden placed on the proponent of the exemption.[127]

¶40 For example, anti-censorship activist Seth Finkelstein submitted a successful request in 2002 for an exemption to allow circumvention of Internet filtering software applications in order to access the lists of blocked sites used by these applications.[128] In this request, Finkelstein relied heavily on his own first-hand experiences with how the anti-circumvention provisions would prevent him, and in some cases had prevented him, from being able to engage in non-infringing activities.[129] He had previously decrypted several of these "censorware" applications for the purposes of news reporting, education, and criticism of the software companies who developed these programs.[130] He detailed both why these specific actions constituted non-infringing uses, and how the DMCA prevented him from engaging in these lawful uses prior to obtaining an exemption during the 1999 rulemaking session.[131] Thus, he met the burden of proof by showing actual, demonstrable evidence of harm rather than merely speculative or theoretical critiques of the DMCA and its potential effects.[132]

2. Evaluating the Plausibility of an Exemption for SecuROM

¶41 It would be very difficult for an entity seeking an exemption for circumventing SecuROM's activation limit to meet this high evidence threshold. Thus, the Register of Copyrights would almost certainly not recommend such an exemption. The first major hurdle is the requirement that users of SecuROM-protected products be adversely affected or likely to be adversely affected within the next three years.[133] Current implementations of SecuROM are generally not restrictive enough to create a likelihood that users will be adversely affected within three years. The most restrictive example of a SecuROM-branded product comes from *Mass*

---

[126] Notice of Inquiry, 73 Fed. Reg. 58073 (Oct. 6, 2008), *available at* http://www.copyright.gov/fedreg/2008/73fr58073.pdf.
[127] *Id.*
[128] SETH FINKELSTEIN, PLEA FOR A DMCA EXEMPTION DURING 2002 RULEMAKING SESSION, at 2–3, *available at* http://www.copyright.gov/1201/2003/comments/031.pdf (last visited June 12, 2009).
[129] *Id.*
[130] *Id.*
[131] *Id.*
[132] *See* SETH FINKELSTEIN, HOW TO WIN (DMCA) EXEMPTIONS AND INFLUENCE POLICY, http://sethf.com/publications/dmca-guide.php (last visited June 12, 2009).
[133] 17 U.S.C. § 1201(a)(1)(B)–(C) (2007).

Effect.[134] *Mass Effect's* DRM only allows three activations instead of five, and unlike some other Electronic Arts SecuROM-protected products, the user does not receive activation revocations when the game is uninstalled.[135] It is certainly plausible that users will use these three activations rather quickly—for example, by using one installation on a desktop computer, one on a laptop computer, and one reinstallation after an operating system crash. At that point, users would not be able to sell the game, nor would they be able to reinstall it in the event of another computer crash, without contacting Electronic Arts to request an additional activation.[136] The company, however, has repeatedly stressed that it will continue to support its products, and there is no evidence that it will withhold additional activations from users who legitimately need them.[137] Thus, because this burden on users is relatively insignificant, it is highly unlikely that *Mass Effect* will provide sufficient evidence to warrant a DMCA exemption for this type of circumvention during the next rulemaking period.

¶42 Although more highly restrictive implementations of SecuROM might qualify for an exemption once there is evidence that the product has restricted users from engaging in clearly non-infringing uses, there is no evidence that software using a more restrictive version of SecuROM will be released within the next three years. Attempts to implement more restrictive versions of SecuROM's software have been met with significant consumer backlash,[138] and therefore no company has yet released software protected by a version of SecuROM that is much more restrictive than that of *Mass Effect*. Even *Mass Effect* and *Spore* were originally designed to require users to re-authenticate the software online every ten days,[139] a feature that was removed from the SecuROM implementations before the final products were released.[140] Thus, not only have the most restrictive versions of SecuROM not yet been released, but the negative public response against companies that have tried to use more restrictive

---

[134] *BioWare's Mass Effect for PC Now Available in North America*, BUSINESS WIRE, May 28, 2008, *available at* http://findarticles.com/p/articles/mi_m0EIN/is_2008_May_28/ai_n25457226.
[135] *BioWare/Electronic Arts Response*, *supra* note 22.
[136] *Id.*
[137] *See id.*; *Spore DRM FAQ*, http://help.spore.com/cgi-bin/easpore.cfg/php/enduser/std_adp.php?p_sid=i2IjIJlj&p_accessibility=0&p_redirect=&p_faqid=19743 (last visited June 12, 2009) [hereinafter *Spore DRM FAQ*].
[138] *See Electronic Arts Response*, *supra* note 28.
[139] Matt Peckham, *Mass Effect and Spore to Require Online Authentication Every 10 Days*, PCWORLD, May 7, 2008, http://blogs.pcworld.com/gameon/archives/006904.html.
[140] *See BioWare/Electronic Arts Response*, *supra* note 22; *Spore DRM FAQ*, *supra* note 138.

configurations suggests that companies may be unlikely to employ such tactics any time in the near future.

3. Pending Exemptions That May Affect SecuROM

¶43 Finally, it is important to note that on December 3, 2008, two proposed exemptions were submitted to the Copyright Office that may affect the rights of certain users to circumvent SecuROM and other software-based DRM systems. First, J. Alex Halderman, a professor at the University of Michigan whose rootkit circumvention exemption request was granted during the 2006 rulemaking proceedings,[141] has requested an exemption for circumvention of similar technological protection measures that may pose significant security risks to users.[142] The proposed exemption focuses on SecuROM in particular, arguing that (1) security researchers should be allowed to circumvent software like SecuROM to determine whether it poses security risks, and (2) if security researchers are not allowed to circumvent SecuROM for research, individual users should be allowed to circumvent SecuROM and similar DRM systems in order to install legitimately purchased software without exposing themselves to potential security risks.[143]

¶44 Second, Christopher Soghoain, a student fellow at Harvard University, submitted a request for an exemption that would allow users to circumvent server-based DRM access controls.[144] Although the exemption request focuses heavily on several music services that have recently gone out of business, it also discusses the potential problems associated with the online authentication requirements of SecuROM-protected products.[145] If a company implements a version of SecuROM that requires periodic online authentication, as was originally planned with *Spore* and *Mass Effect*,[146] and that company then goes out of business, users could be left without a method of legally authenticating their purchased software.[147]

---

[141] Christopher Soghoain, *DMCA Exemptions Desired to Hack iPhones, DVDs*, CNET NEWS, Dec. 2, 2008, http://news.cnet.com/8301-13739_3-10112046-46.html.

[142] J. ALEX HALDERMAN, EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES, Dec. 2, 2008, *available at* http://www.copyright.gov/1201/2008/comments/halderman-reid.pdf.

[143] *Id.* at 13, 15–16.

[144] CHRISTOPHER SOGHOAIN, EXEMPTIONS TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR DEFUNCT DRM AND COPY PROTECTION-BASED STORES, Dec. 2, 2008, *available at* http://www.copyright.gov/1201/2008/comments/soghoain-christopher.pdf.

[145] *Id.* at 9.

[146] *See supra* notes 140–41 and accompanying text.

[147] Soghoain, *supra* note 145, at 9.

CONCLUSION

¶45 In all of these possible legal challenges to SecuROM, the result will ultimately depend on the evidence. If the plaintiffs in the currently pending cases against Electronic Arts are able to prove that SecuROM actually installs itself at the root level, or otherwise exposes its users to risks similar to those posed by XCP and MediaMax in the Sony BMG case, Sony DADC might see a similar FTC order regarding SecuROM. If, on the other hand, Sony DADC has been accurate and honest in its description of its software and the way that it functions, it would be difficult for a plaintiff to bring a successful challenge against any existing implementations of SecuROM. It would be similarly difficult to obtain a DMCA exemption for circumvention of features like the activation limit.

¶46 However, even if a company does not use the most restrictive version of SecuROM, it is still possible that a tool could be developed that only allows users to circumvent the activation limit without violating the DMCA's anti-circumvention provisions. Like the aftermarket garage door opener in *Chamberlain*, this kind of tool might be developed and distributed freely as long as it only enables consumers to engage in lawful uses of their products. Thus, in a future case involving this hypothetical circumvention tool, the legal analysis must begin by determining whether the technological protection measure at issue bears a rational relationship to preventing infringing uses of the product, not merely whether a technological protection measure has been circumvented. If the court in this hypothetical situation follows the pro-consumer lead of *Chamberlain* and *Storage Technology*, then the court's decision could serve as an important, much-needed tempering of the DMCA's blanket prohibition against the development and distribution of circumvention tools.

¶47 A tempering of the DMCA is especially important given the high evidentiary burden of the DMCA exemption process and the fact that the exemption process only applies to one of the DMCA's three anti-circumvention provisions. Although the process should function as a safeguard against overly burdensome technological protection measures, the stringent evidence requirements and emphasis on imminent harm essentially guarantee that there will not be an exemption for circumventing systems like SecuROM until users are actually being locked out of using their software. Moreover, even if an exemption were granted to allow users to circumvent SecuROM, the anti-trafficking provisions of the DMCA would still be in full effect. Thus, it would be illegal for software developers to create and distribute the tools that are necessary to enable such circumvention. Users, then, would have the legal right to circumvent access controls with no legal way of obtaining the tools to do so. This would be like the *Chamberlain* court allowing consumers to circumvent the access controls on their garage door openers while prohibiting Skylink from

producing and distributing universal remotes. In the future, courts need to look to decisions like *Chamberlain* to ensure that consumers have access to the tools that they need to engage in lawful circumvention.