BEFORE THE COPYRIGHT OFFICE OF THE LIBRARY OF CONGRESS

IN THE MATTER OF
EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES

Docket No. RM 2008-8

Comment of:
J. Alex Halderman
Assistant Professor of Electrical Engineering and Computer Science
--
University of Michigan
CSE Building
2260 Hayward Avenue
Ann Arbor, MI 48109-2121

Represented by:
Blake E. Reid, Clinician and Juris Doctor Candidate
Paul K. Ohm, Associate Professor of Law
Harry A. Surden, Associate Professor of Law
J. Brad Bernthal, Associate Clinical Professor of Law
--
Samuelson-Glushko Technology Law & Policy Clinic
University of Colorado School of Law
105R Wolf Law Building, 401 UCB
Boulder, CO 80309-0401

December 2, 2008

Pursuant to the Notice of Inquiry of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies[1] ("NOI") and 17 U.S.C. § 1201(a)(1)(C), we respectfully request that the Librarian of Congress grant an exemption to 17 U.S.C. § 1201(a)(1)(A) for (1) literary works, sound recordings, and audiovisual works accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities, or, in the alternative, for (2) video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.

---

[1] 70 Fed. Reg. 73, 58073 (Oct. 6, 2008) [hereinafter *NOI*].

I. Submitting Party

J. Alex Halderman is a noted computer security and privacy researcher and an assistant professor of electric engineering and computer science at the University of Michigan.[2] His research focuses particularly on the threats introduced by access and copy-protection measures. In particular, he published in 2003 an academic paper on SunnComm's MediaMax copy-protection system[3]. In response, SunnComm first threatened a lawsuit under the Digital Millennium Copyright Act ("DMCA")[4], then subsequently retracted the lawsuit, citing the "chilling effect on [computer security] research."[5]

Partially in response, Professor Halderman proposed, as part of the third iteration of this rulemaking process (along with Princeton Professor Edward W. Felten), an exemption to the DMCA anti-circumvention measures to address the chilling effect of the statute on computer security researchers in the context of insecure technological protection measures ("TPMs") on compact discs containing audio recordings and the unfair access limits that the statute placed on consumers.[6] As a result, the Librarian of Congress exempted the following class of works from the anti-circumvention measures (hereinafter "Sound Recordings Exemption"):

> *Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.*[7]

---

[2] http://www.cse.umich.edu/~jhalderm/.
[3] J. Alex. Halderman, *Analysis of the MediaMax CD3 Copy-Prevention System*, PRINCETON UNIVERSITY COMPUTER SCIENCE TECHNICAL REPORTS TR-679-03, *available at* http://www.cs.princeton.edu/research/techreps/TR-679-03.
[4] Fred Locklear, *Press "Shift" to Initiate Lawsuit*, ARS TECHNICA (Oct. 9, 2003), *available at* http://arstechnica.com/archive/news/1065755223.html.
[5] Fred Locklear, *SunnComm Shifts Stance, Backs Away from Lawsuit*, ARS TECHNICA (Oct. 10, 2003), *available at* http://arstechnica.com/archive/news/1065816462.html.
[6] Edward W. Felten and J. Alex Halderman, Re: RM 2005-11 – Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Dec. 1, 2005), *available at* http://www.copyright.gov/1201/2006/comments/mulligan_felten.pdf.
[7] Final Rule of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 71 Fed. Reg. 227, 68477 [hereinafter "FR"].

II. Proposed Classes of Works

In this rulemaking, we request that the following class of works (hereinafter "Class 1") be exempted from the anti-circumvention measures:

> *Literary works, sound recordings, and audiovisual works accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.*

In the alternative, we request that the following class of works (hereinafter "Class 2") be exempted instead:

> *Video games accessible on personal computers and protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.*

In the proposed classes of works, we have tracked very closely the language adopted by the Librarian during the third rulemaking in granting the Sound Recordings Exemption, merely replacing "[s]ound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format" with "[l]iterary works, sound recordings, and audiovisual works accessible on personal computers" in Class 1, and "[v]ideo games accessible on personal computers" in Class 2, and thereby maintaining the proposed classes of works as limited subsets of the categories of authorship enumerated in 17 U.S.C. § 102(a), further limited to particular uses, as required for an exemption under the NOI.[8]

In particular, the starting points of Class 1 are literary works, sound recordings, and audiovisual works, each a copyrightable category of authorship under 17 U.S.C. § 102(a). Indeed, each category was a starting point of another exemption granted by the Librarian during the third rulemaking.[9]

---

[8] *See NOI*, *supra* note 1 at 58077.

[9] *(1)* ***Audiovisual works*** *included in the educational library of a college or university's film or media studies department, when circumvention is accomplished for the purpose of making compilations of portions of those works for educational use in the classroom by media studies or film professors . . .*
(4) ***Literary works*** *distributed in ebook format when all existing*

The starting point of Class 2 is video games. Video games are a subset of computer programs, which are themselves a subset of literary works under 17 U.S.C. § 102(a)[10]. Video games may further embody literary works, audiovisual works, and sound recordings, all copyrightable categories of authorship under Section 102(a). Accordingly, Class 2 forms a narrow subset of Class 1. Video games were also embraced as part of the class of works of another exemption granted by the Librarian during the third rulemaking.[11]

Furthermore, both proposed classes are limited to works protected by TPMs that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers ("PCs"). Finally, both classes are limited to circumvention "accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."

As discussed in the following sections, these limitations narrowly focus the proposed classes to remedy the evidence of present and likely harm while preserving protection for copyright holders in other classes as required under the NOI.[12]

> *ebook editions of the work (including digital text editions made available by authorized entities) contain access controls that prevent the enabling either of the book's read–aloud function or of screen readers that render the text into a specialized format . . . [, or]*
> *(6)* ***Sound recordings****, and* ***audiovisual works*** *associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."*

FR, *supra* note 7 at 68480 (emphasis added).

[10] *Dun & Bradstreet Software Services, Inc. v. Grace Consulting, Inc.*, 307 F.3d 197, 206 (3d Cir. 2002) (citing *Whelan Assoc. v. Jaslow Dental Lab.*, 797 F.2d 1222, 1234 (3d Cir. 1986)).

[11] > *(2) Computer programs and* ***video games*** *distributed in formats that have become obsolete and that require the original media or hardware as a condition of access, when circumvention is accomplished for the purpose of preservation or archival reproduction of published digital works by a library or archive. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.*

FR, *supra* note 7 at 68480 (emphasis added).

[12] *See NOI*, *supra* note 1 at 58077.

III. Summary of Argument

Beginning in 2005, over *half a million* PCs were afflicted with serious security vulnerabilities as a side effect of copy-protection software, known as a "rootkit," distributed on audio compact discs ("CDs") by Sony.[13] Though the company initially professed ignorance over the rootkit fiasco[14], public outcry and legal advocacy later led to a partial recall of rootkit-equipped CDs[15], abandonment of the rootkit[16], and the aforementioned Sound Recordings Exemption.

Since the third rulemaking, evidence has been uncovered indicating that security flaws in TPMs affecting works *outside* the scope of the Sound Recordings Exemption have created similar security vulnerabilities in many more PCs. A flaw uncovered last year in Macrovision's SafeDisc software[17], one of the most widely used copy-protection systems for PC-accessible video games[18], exposed PCs to attacks similar to but even more dangerous than those enabled by the Sony rootkit.[19] Because SafeDisc shipped preinstalled on nearly every copy of the Microsoft Windows XP and Windows 2003 operating systems, the vulnerability affected nearly *one billion PCs*, two thousand times more than the rootkit.[20]

---

[13] Paul F. Roberts, *Sonys [sic] Rootkit Is on 500,000 Systems, Expert Says*, EWEEK.COM (Nov. 15, 2005), *available at* http://www.eweek.com/c/a/Security/Sonys-Rootkit-Is-on-500000-Systems-Expert-Says/.

[14] Andrew Orlowski, *Sony Digital Boss – Rootkit Ignorance is Bliss*, THE REGISTER (Nov. 9, 2005), *available at* http://www.theregister.co.uk/2005/11/09/sony_drm_who_cares/.

[15] John Borland, *Sony Recalls Risky 'Rootkit' CDs*, CNET (Nov. 15, 2005), *available at* http://news.cnet.com/Sony-recalls-risky-rootkit-CDs/2100-7349_3-5954154.html.

[16] Amy Phillips, *Sony Discontinues Controversial Anti-Piracy Software*, PITCHFORK MEDIA (Nov. 15, 2005), *available at* http://www.pitchforkmedia.com/article/news/35490-sony-discontinues-controversial-anti-piracy-software.

[17] Microsoft, *Security Bulletin MS07-067– Important: Vulnerability in Macrovision Driver Could Allow Local Elevation of Privilege* (Dec. 11, 2007), *available at* http://www.microsoft.com/technet/security/Bulletin/MS07-067.mspx.

[18] *See Macrovision Announces SafeDisc DVD-ROM Copy Protection*, EMEDIALIVE.COM (May 16, 2003), *available at* http://www.emedialive.com/Articles/ReadArticle.aspx?ArticleID=7594.

[19] Both the Sony rootkit and the flawed SafeDisc software are so-called "device drivers." Device drivers have effectively unrestricted access to PC hardware and software, so attackers can often leverage security flaws in the drivers to bypass other security mechanisms on the PC. The flaw in the Sony rootkit grants attackers only the limited power to conceal their own files and programs; the SafeDisc flaw is much more dangerous, allowing attackers to execute unrestricted "kernel-level" code and read or write any area of the hard disk or memory of the PC, thus facilitating the complete compromise of the security of the PC. The flaws in both the rootkit and SafeDisc are exploited by so-called "privilege escalation attacks" and require the attacker to first gain *some* access to the PC.

[20] *See* Joel Hruska, *Windows Install Base to Break One Billion in 2008*, ARS TECHNICA (Jul. 28, 2007), *available at* http://arstechnica.com/journals/microsoft.ars/2007/07/28/windows-install-base-to-break-one-billion-in-2008.

Serving as another prominent example of this kind of TPM is Sony's SecuROM software, utilized by dozens of high-profile video game publishers including Atari, Bethesda Softworks, Capcom, Eidos, Electronic Arts, Konami, LucasArts, Microsoft, Sega, and Ubisoft.[21] PC-accessible video games utilizing SecuROM automatically install copy-protection software, often without the consumer's knowledge. Independent security experts have not yet rigorously studied SecuROM; in the absence of a definitive analysis, anecdotal contentions of harm, speculation about causes, and contradictory assessments of risk have run wild on the Internet. While Sony maintains that the TPM is safe[22], some users report that it disables critical system security functionality including firewalls and antivirus software, opening their PCs to a variety of viruses, spyware, and other malware.[23] Three class action lawsuits have been filed against Electronic Arts on behalf of those allegedly negatively affected by the inclusion of SecuROM in the popular video games *Mass Effect*[24], *Spore*[25], and *Spore Creature Creator*[26].

Whether or not SecuROM causes actual security vulnerabilities, the uncertainty about its risks has created an environment of suspicion where consumers fear the worst.[27] Given the immense stakes that users hold in the security of their PCs – private communications, valuable data, and even financial assets vulnerable to theft and fraud – the presumption that SecuROM is insecure may be a rational decision to err on the side of caution. Yet, consumers who bought SecuROM-encumbered games unaware of the potential risks are now placed between a rock and a hard place, forced to choose between accepting the indeterminate risks posed by SecuROM and abandoning access to their lawfully obtained video games. This is an unacceptable proposition for consumers.

Furthermore, the SafeDisc and SecuROM fiascos showcase the very real chilling effect of the DMCA anti-circumvention measures on security research related to these TPMs. Even though SafeDisc exposed hundreds of millions of PCs to a serious security vulnerability, over six years passed after the release of the TPM until anyone but attackers knew about the vulnerability, which was not publicly documented until a security

---

[21] *Securom [sic] Affected Games*, RECLAIM YOUR GAME! (Nov. 11, 2008), *available at* http://reclaimyourgame.com/index.php?option=com_content&view=article&id=45&Itemid=11.
[22] *See SecuROM™ Frequently Asked Questions*, *available at* http://www.securom.com/support_faq.asp ("SecuROM™ does not damage a computer in any way. Great care has been taken to make sure the SecuROM™ system is sound and compatible.")
[23] *See Thomas v. Electronic Arts, Inc.* fn. 1 (N.D. Cal., Sept. 22, 2008), *available at* http://www.courthousenews.com/2008/09/23/Spore.pdf.
[24] *Gardner v. Electronic Arts, Inc.* (N.D. Cal., Oct. 6, 2008), *available at* http://www.courthousenews.com/2008/10/08/MassEffect.pdf.
[25] *Thomas*, *supra* note 22.
[26] *Eldridge v. Electronic Arts, Inc.* (N.D. Cal., Oct. 14, 2008), *available at* http://docs.justia.com/cases/federal/district-courts/california/candce/3:2008cv04733/208019/1/.
[27] *See* anonymous user "Faceless Clock," *Anti-DRM Revolt Strikes Amazon Reviews*, BLOGCRITICS MAGAZINE (Nov. 12, 2008), *available at* http://blogcritics.org/archives/2008/11/12/183314.php.

researcher observed a piece of malware exploiting it[28]. And the ongoing uncertainty over SecuROM's safety could probably be settled by a single definitive scientific study; instead, a regime of panic, protests, and litigation has taken hold over what may turn out to be nonexistent or easily reparable faults.

Despite the high stakes, security researchers have clearly avoided addressing these problems, and the chilling effect of the DMCA anti-circumvention provisions is at least partially to blame. Security researchers remain the last defense against dangerous security flaws caused by TPMs, and discouraging their intervention is completely undesirable. Accordingly, an exemption to the anti-circumvention measures is needed to allow security researchers to investigate and fix security flaws caused by TPMs on PC-accessible video games, and for consumers to apply those fixes to access their lawfully obtained games.

A growing body of evidence suggests an inherent tension between digital rights management ("DRM") technology embodied by these TPMs and user security[29]. Accordingly, we can confidently predict that the Sony rootkit, SafeDisc, and SecuROM will not be the last TPMs to cause collateral security harm. The exemption of Class 2 from the anti-circumvention measures should be adequate to mitigate the harms caused by TPMs that control access to PC-accessible video games because it will remove the chilling effect of the anti-circumvention measures, thereby encouraging independent researchers to investigate and correct security flaws in these TPMs and allowing users to stay informed and take appropriate measures to protect themselves.

However, potentially dangerous TPMs will likely be used on many other PC-accessible works between now and the next rulemaking procedure in 2012. To wit, TPMs are being used (or are planned for use) on ebooks[30] and digitally distributed multimedia content[31]. The continued use of flawed TPMs in the aftermath of the Sony rootkit fiasco indicates that the risk of harming consumers is unlikely to provide the content industry with sufficient incentive to be diligent about security, and those consumers should not be forced to wait years to gain secure access to their lawfully obtained works. Accordingly, an

---

[28] Elia Florio, *Privilege Escalation Exploit in the Wild*, SYMANTEC FORUMS (October 16, 2007), available at https://forums.symantec.com/syment/blog/article?message.uid=305541.

[29] *See* discussion *infra* Part IV(B).

[30] Adobe plans to establish a de facto industry standard for ebook DRM. Bill McCoy, *Point-Counterpoint: Digital Book DRM, the Least Worst Solution*, O'REILLY TOC (Nov. 24, 2008), *available at* http://toc.oreilly.com/2008/11/an-industry-standard-digital-b.html.

[31] Netflix is using Microsoft Silverlight digital rights management (DRM) technology to protect its video streams. Joshua Topolsky, *Netflix Finally Brings 'Watch Instantly' to Macs Via Silverlight*, ENGADGET (Oct. 26, 2008), *available at* http://www.engadget.com/2008/10/26/netflix-finally-brings-watch-instantly-to-macs-via-silverlight/. YouTube and Hulu use Adobe Flash technology, which is now capable of encrypting video streams, thus bringing security research thereof under the purview of the DMCA. Kevin Towes, *Encryption and Streaming Media Protection to Adobe Flash*, FLASH MEDIA BLOG (Sept. 28, 2008), *available at* http://blogs.adobe.com/ktowes/2008/09/encryption_and_streaming_media_1.html.

exemption of Class 1 from the anti-circumvention measures is needed to prospectively allow security researches to discover and fix security flaws in other PC-accessible works before attackers find and exploit these flaws against consumers.

IV. Nature and Operation of the Access-Controlling Technological Measures

This section describes the technological measures that control access to the proposed classes of works and the manner of operation of the measures.

A. PC-accessible Video Games (Class 2)

Over the history of PC video games, publishers have relied extensively on the use of access controls to prevent unauthorized copying. Early video games contained simple serial numbers in the packaging that needed to be entered in order to install the games; many contained gameplay-based puzzles unsolvable without information in the included user manual[32]. With the rise of the Internet and the growth of sophisticated hacking techniques, these controls were considered no longer sufficient to control access to the games; serial numbers and information from user manuals could simply be distributed over the network, or internal protection measures could simply be bypassed. Publishers responded with video games that "phoned home," checking with a server operated by the publisher to ensure that the software was licensed, as well as controls to prevent discs from being copied. These controls were quickly and widely circumvented as well.

Frustrated by these technological changes, the video game industry has followed Sony's rootkit lead, responding with new, more aggressive TPMs to control access to their games. These TPMs, of which SafeDisc and SecuROM are well-known examples, tend to operate approximately as follows: When a user attempts to install a video game, a hidden computer program is surreptitiously installed along with the game.[33] The program is installed with elevated privileges, giving it unfettered access to the rest of the PC[34] to carry out DRM tasks such as authenticating discs, enforcing access policies, and taking countermeasures against circumvention tools.

TPMs like these may prevent users from accessing their games in ways that are unquestionably legal under (and largely unregulated by) the Copyright Act.[35] Even worse, these TPMs may cause problems with other subsystems of the user's PC. For example, SecuROM reportedly may interfere with the operation of a PC's CD and DVD burners and

---

[32] A famous example is found in *The Secret of Monkey Island*, the seminal 1990 LucasArts adventure game that halts the adventures of the winsome pirate Guybrush Threepwood until the user enters the correct code from the enclosed "*Dial-A-Pirate"* code wheel included in the game box. *See The Secret of Monkey Island*, THE MONKEY ISLAND SCUMM BAR, *available at* http://www.scummbar.com/games/index.php?game=1&sub=media&todo=7; *see also* image *infra* at Ex. A, Fig. 1.

[33] *See Eldridge* at 10 ¶ 13.

[34] *Id.* at 10 ¶ 14.

[35] *See infra* Part V(A)(2).

several software programs[36]; some users even claim that SecuROM can even interfere with virus and firewall protection software[37], opening a serious hole in the defenses of the PC.

Unfortunately, the video game publishers using these TPMs profess ignorance about the security risks posed by the TPMs.[38] Ironically mimicking a Sony officer's initial comments about the rootkit fiasco[39], Electronic Arts CEO John Riccitiello confidently claimed that "99.8% percent of users *wouldn't notice* [the TPMs]," [40] a statement that, if true, *highlights* the need for independent security researchers to act quickly to inform and protect innocent, unknowing, and at-risk consumers, most of whom are ill-equipped to defend against the security risks posed by the TPMs. Even when acknowledging problems with the TPMs, video game publishers have merely loosened usability restrictions[41] and failed to address security risks.

While it is impossible to predict what vulnerabilities will be discovered next in PC video games, the continued adoption of TPMs like SafeDisc and SecuROM makes it inevitable that new vulnerabilities *will* be discovered over the present rulemaking period[42]. Less certain is who will discover these vulnerabilities first. Without the exemption of either of the proposed classes, it is likely to be malicious attackers unconcerned with potential suit under the DMCA, and not legitimate security researchers chilled by the anti-circumvention measures. Accordingly, the proposed exemption of Class 2 is the bare minimum necessary to both cure present, ongoing problems and prevent future harms with video games, as required by the NOI.[43] However, the proposed exemption of Class 1, described in the following subsection, would better enable the noninfringing uses described hereinafter.

---

[36] *See Eldridge* at 13-15 ¶¶ 20-22.
[37] *See Thomas* fn. 1.
[38] *See SecuROM™ Frequently Asked Questions*, *available at* http://www.securom.com/support_faq.asp ("SecuROM™ does not damage a computer in any way. Great care has been taken to make sure the SecuROM™ system is sound and compatible.") (hereinafter "SecuROM FAQ").
[39] Then-Sony BMG Global Digital Business Division President Thomas Hesse pondered, "Most people, I think, don't even know what a rootkit is, so why should they care about it?" Orlowski, *supra* note 14.
[40] David Kaplan, *EA's Ricciteliello: Last Year for 'Offline-Only' Games*, YAHOO! FINANCE (Oct. 14, 2008), *available at* http://biz.yahoo.com/paidcontent/081014/1_328572_id.html?.v=1
[41] *E.g.*, Eric Caoili, *EA Loosens Spore's DRM, Account Restrictions*, GAMASUTRA (Sept. 19, 2008), *available at http://www.gamasutra.com/php-bin/news_index.php?story=20322*.
[42] For example, Blizzard, the creator of the popular *World of Warcraft* series, intends to use SecuROM-esque measures in several upcoming games. *See* Earnest Cavalli, *Q&A: Blizzard CEO Mike Morhaime on DRM, WoW and the Next MMO,* WIRED BLOG NETWORK (October 16, 2008), *available at* http://blog.wired.com/games/2008/10/qa-blizzard-ceo.html.
[43] *See NOI*, *supra* note 1 at 58077.

B. PC-accessible Literary Works, Sound Recordings, and Audiovisual Works (Class 1)

As detailed in the previous subsection and in the initial comment preceding the Sound Recordings Exemption[44], TPMs such as the Sony rootkit and SafeDisc have caused extensive security risks to consumers, and the content industry seems to show little hesitation toward the continued adoption of DRM technologies[45] embodied by these TPMs. However, many security researchers now believe that the Sony rootkit and SafeDisc fiascos are just the tip of the iceberg, merely highlighting security issues that are endemic to all DRM technology.

Researchers have already begun to document the fact that DRM inherently tends to give rise to security vulnerabilities. According to noted security expert Bruce Schneier, "[t]here is an inherent insecurity to technologies that try to own people's computers: [t]hey allow individuals other than the computers' legitimate owners to enforce policy on those machines. These systems invite attackers to assume the role of the third party and turn a user's device against him."[46] This is neither a tentative nor uncertain conclusion in the security field; for example, Schneier's academic colleagues Joan Feigenbaum, Michael Freedman, Tomas Sander, and Adam Shostack pointed out that, "[a]t the risk of stating the obvious, . . . there can be inherent tension between the copyright-enforcement goals of owners and distributors who deploy DRM systems and the privacy goals of users."[47]

The security problems surrounding DRM technology stem from its inherent complexity. Computer scientist Steve Bellovin notes that while "DRM may not be evil[, i]t is, however, very, very complex, and, historically, complexity has led to insecurity."[48] Risky software engineering practices behind DRM technology are also to blame. Programmer Ken Johnson states that "[m]ost DRM technologies tend to use unsupported and/or 'fringe' techniques to make themselves difficult to understand and debug. However, more often than not, the DRM authors often get little things wrong with their anti-debug/anti-hack implementations, and when you're running in a privileged space, 'little things wrong' can translate into a security vulnerability. . ."[49]

---

[44] Edward W. Felten and J. Alex Halderman, *Comment Re: RM 2005-11* (Dec. 1, 2005), *available at* http://www.copyright.gov/1201/2006/comments/mulligan_felten.pdf [hereinafter *Sony Rootkit Comment*].

[45] *See infra* note 23.

[46] *Everyone Wants to 'Own' Your PC*, WIRED (May 4, 2006), *available at* http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70802.

[47] *Privacy Engineering for Digital Rights Management Systems* (2001), *available at* http://www.cs.yale.edu/homes/jf/FFSS.pdf.

[48] *DRM, Complexity, and Correctness*, IEEE SECURITY AND PRIVACY 80 (Feb. 2007), *available at* http://www.cs.columbia.edu/~smb/papers/04085601.pdf.

[49] *Invasive DRM Systems are Dangerous from a Security Perspective*, NYNAEVE: ADVENTURES IN WINDOWS DEBUGGING AND REVERSE ENGINEERING (Nov. 6, 2007), *available at* http://www.nynaeve.net/?p=193. Johnson concludes that "This is one of the reasons why I personally am extremely wary of playing games that require administrative privileges or install administrative 'helper services' for non-administrative users, because games have a

The inherent connection between DRM and security vulnerabilities is a centerpiece of Professor Halderman's research, and indeed, is one of the most significant themes developed in his dissertation. For example, his investigation into the Sony rootkit fiasco led him to conclude that "[b]y looking carefully at CD copy-protection as a technical problem, we can see why DRM designers are drawn to spyware tactics as their best hope of halting copying. . . . From a nontechnical viewpoint, Sony-BMG's experience has much to teach the music industry. The most important lesson is that DRM can have serious side effects, especially relating to security and privacy."[50] In another paper, Professor Halderman noted that "there can be an inverse relation between the efficacy of DRM and the user's ability to defend her computer from unrelated security and privacy risks. The user's best defense is rooted in understanding and controlling which software is installed, but many DRM systems rely on undermining this understanding and control."[51]

Despite the inherent connection between DRM and security vulnerabilities, we are quite sensitive to the rights of copyright owners under the DMCA to protect their copyrighted works with TPMs, and respect the Librarian's necessarily narrow interpretation of his rulemaking authority. Accordingly, and although we would prefer to see a blanket security research exemption to the DMCA,[52] we have limited Class 1 to focus narrowly on the circumstances in which the connections between DRM and security vulnerabilities are best documented.

We have narrowed the scope of Class 1 in two critical ways. First, Class 1 includes only works accessible on personal computers. By personal computers, we mean *general purpose* personal computers, and exclude dedicated and specialized hardware like stand-alone video game playing machines, dedicated eBook readers, and non-PC CD and DVD players, as security vulnerabilities are worst when they infect general-purpose, generative machines like PCs[53].

Second, Class 1 is restricted to three specific categories of copyrighted works: literary works, sound recordings, and audiovisual works. Thus, the proposed exemption

---

high incidence of including low quality anti-cheat/anti-hack/anti-copying system nowadays. I simply don't trust the people behind these systems to get their code right enough to be comfortable with it running with full privileges on my box." *Id.*

[50] Edward W. Felten and J. Alex Halderman, *Digital Rights Management, Spyware, and Security*, IEEE SECURITY AND PRIVACY 21-22 (Feb. 2006), *available at* http://www.cse.umich.edu/~jhalderm/pub/papers/drm-sp06.pdf.

[51] J. Alex Halderman and Edward W. Felten, *Lessons from the Sony CD DRM Episode* (2006), *available at* http://www.cse.umich.edu/~jhalderm/pub/papers/rootkit-sec06.pdf.

[52] Of course, 17 U.S.C. § 1201(j) provides a security exemption of questionable applicability, as discussed extensively during the third rulemaking. For the reasons articulated during those discussions, 1201(j) may provide insufficient protection for security researchers.

[53] *See generally* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008) (defining and discussing generativity).

would not apply to TPMs that restrict access solely to choreographic works[54], pictorial, graphic, and sculptural works[55], or architectural works[56], for example.[57] This reflects the fact that the past evidence of harm has been encountered with TPMs regulating access to literary works (such as computer programs), audiovisual works (video games[58]), and sound recordings (audio CDs).

While it is again impossible, as with PC video games, to predict what vulnerabilities will be discovered next in PC-accessible literary works, sound recordings, and audiovisual works, it is inevitable that new vulnerabilities *will* be discovered over the present rulemaking period, and certain that the DMCA will chill security researchers from discovering them without the exemption of Class 1. Accordingly, and although the proposed exemption of Class 2 would be welcomed and appreciated, the proposed exemption of Class 1 is necessary to both cure present, ongoing problems and prevent future harms with the aforementioned PC-accessible works, as required by the NOI.[59]

V. Legal Arguments in Support of the Requested Exemption

This section first describes the noninfringing uses at issue, then analyzes the proposed classes in the context of the statutory considerations enumerated in 17 U.S.C. § 1201(a)(1)(C).

A. The Prevented Noninfringing Activities

In the third rulemaking, the Register of Copyrights refined her approach to defining acceptable classes of works. Inspired by a proposal narrowly tailored to film and media studies professors, the Register recommended, and the Librarian ruled, that classes of works may be tailored to "particular uses or users."[60] We agree that this rule is sound, in particular because it ensures that proposed exemptions do not swallow the DMCA or exceed the Librarian's rulemaking authority. For this reason, we have narrowed our proposed classes precisely as the Register did in the last round with respect to sound recordings, limiting them to circumvention "accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."

Accordingly, we enumerate in this section two noninfringing uses of the proposed classes of works adversely affected by the previously described TPMs: (1) engaging in good

---

[54] 17 U.S.C. § 102(a)(4).
[55] 17 U.S.C. § 102(a)(5).
[56] 17 U.S.C. § 102(a)(8).
[57] Class 1 would, however, apply to TPMs restricting access to literary works, audiovisual works, and sound recordings that also embody other works (such as choreographic works, pictorial, graphic, and sculptural works, or architectural works).
[58] As previously mentioned, video games may also embody literary works, audiovisual works, and sound recordings.
[59] *See NOI*, *supra* note 1 at 58077.
[60] *FR*, *supra* note 7 at 68474.

faith computer security research, and (2) installing and utilizing the works. Furthermore, each use requires the access-protected copy of the work, an essential element for an exemption under the NOI[61], because alternative, unprotected formats are either unavailable, insufficiently functional to serve as substitutes, or inherently incapable of facilitating the use. These uses are the same or substantially similar for both proposed classes of works, except as noted otherwise.

1. Engaging in Good Faith Computer Security Research

The chilling effects of the DMCA prevent legitimate security researchers from circumventing the TPMs placed on PC-accessible literary works (including video games), sound recordings, and audiovisual works to discover, document, and fix security flaws in good faith. This increases the likelihood that attackers will find flaws first and leaves consumer protection to anonymous researchers who are forced to release their work under the digital cover of darkness, depriving many consumers of the full value of the fixes and preventing legitimate academic publication and discussion of the flaws. This is not merely a concern for academic researchers, as an entire industry of professional security researchers, including those who work for antivirus and anti-spyware firms and specialize in finding and correcting vulnerabilities, is similarly chilled from investigating these TPMs.

Engaging in security research on the proposed classes of works is a noninfringing use under copyright law. Much of the research involves the same activities required to install and use the works, which, as discussed below, do not implicate any of the copyright holder's reproduction or adaptation rights of copyright holders under 17 U.S.C. 106(1)-(2) and, alternatively, are licensed by the game publishers and also explicitly allowed under 17 U.S.C. § 117(a)(1).

Even when unlicensed, this type of security research is almost certain to constitute a legal fair use under 17 U.S.C. § 107. Section 107 enumerates four nonexclusive factors for determining whether a particular use is fair: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.

a. PURPOSE AND CHARACTER OF THE USE

The purposes of the intended use in question are research, scholarship, and teaching, all listed as model fair uses in the preamble to Section 107.[62] Furthermore, the discovery and disclosure of security vulnerabilities is closely analogous to criticism and commentary, two other model fair uses listed in the preamble. The listing of a use in the

[61] *See NOI*, *supra* note 1 at 58077.
[62] The Supreme Court noted that a fair use analysis "may be guided by the examples given in the preamble of § 107. . . ." *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 578 (1994).

preamble to Section 107 weighs the first factor heavily in favor of a determination of fair use.[63]

b. NATURE OF THE WORKS

The nature of the works in question runs the gamut from purely factual (e.g., nonfictional ebooks) to purely creative (e.g., video games); thus, a generalized analysis under the second factor is impossible to perform.[64] However, several courts have held computer programs and video games to be entitled to a lower degree of protection than more traditional literary works because they generally "contain unprotected aspects that cannot be examined without copying."[65] Therefore, the second factor is likely weighted toward a determination of fair use.

c. AMOUNT AND SUBSTANTIALITY OF THE USE

Although security researchers often must install the works in question in their entirety in order to test them for vulnerabilities, such installation is usually licensed and therefore irrelevant to the third factor. More relevant is the amount and substantiality of the copyrighted work *used* by the security researcher which, in most cases, is little to none. Security researchers generally focus their attention on the TPM, not the underlying protected work. In other words, researchers dissect, scrutinize, and manipulate the lock, not what is protected by the lock. Accordingly, the third factor is likely weighted toward a determination of fair use.

d. MARKET EFFECT OF THE USE

As discussed further below[66], successful security research is likely to *increase* market demand for a work by ameliorating consumer uncertainty surrounding the security of the work. Likewise, the detection and responsible mitigation of a security vulnerability in a work will likely give consumers an ongoing confidence in the publisher of the work, further enhancing the market attractiveness of the work. The revelation of security flaws research may have a negative effect on the market for the work if the publisher refuses to fix the flaws. However, this market effect of security research is directly analogous to that of a vicious parody or successful criticism and thus irrelevant to the fourth factor.[67]

---

[63] *See, e.g.*, *Marcus v. Rowley*, 695 F.2d 1171, 1175 (9th Cir. 1983).
[64] The Supreme Court has held that, "[i]n general, fair use is more likely to be found in factual works than in fictional works." *Stewart v. Abend*, 495 U.S. 207, 237 (1990).
[65] *E.g., Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 603 (9th Cir. 2000); *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510, 1526 (9th Cir. 1992).
[66] *See* discussion *infra* Part V(B)(4).
[67] *See Campbell*, 510 U.S. at 591-92 ("[W]hen a lethal parody, like a scathing theater review, kills demand for the original, it does not produce a harm cognizable under the Copyright Act. . . . 'Parody may quite legitimately aim at garroting the original, destroying it commercially as well as artistically . . . .'" (quoting BENJAMIN KAPLAN, AN UNHURRIED VIEW OF COPYRIGHT 69 (1967)).

Because each of the factors enumerated under Section 107 is weighted in favor of fair use, a determination of fair use is almost certain.

Finally, security research inherently requires the use of the access-controlled works, as any security flaws in the access-controlled works may not be present on any alternate formats, if any such formats even exist. Accordingly, no alternate means exists to engage in this noninfringing use.

2. Installation and Utilization

In the present-day security ecosystem, the publishers of PC-accessible works cannot, practically speaking, eliminate all exploitable security flaws from their products. Thus, PC users must rely on academic and industrial security researchers to root out, publicize, and fix security vulnerabilities. However, research on an entire class of vulnerabilities (those associated with TPMs that effectively control access to copyrighted works) has been rendered much riskier and more difficult by the DMCA. With researchers turning their attention elsewhere, the ecosystem has broken down, leaving PCs less reliable and less secure.

As the content industry continues to embrace TPMs laden with security vulnerabilities, and as researchers continue to be chilled from investigating them, consumers have begun to trust content less. In the extreme, a consumer will choose not to install (if necessary) and use a lawfully obtained, TPM-protected work on her PC because of security risks (whether actual or potential). Thus, the TPM will indirectly interfere with her right to install and utilize the content.

There is ample proof that this has already happened in the context of the SafeDisc and Sony rootkit[68] fiascos, and that it is happening now with SecuROM[69]. Without the proposed exemptions, PC users will continue to be stuck with the unpalatable decision of either risking the security of their PCs or being denied access to use their lawfully obtained content.

Furthermore, the installation and ordinary use of lawfully obtained PC-accessible literary works (including video games), sound recordings, and audiovisual works constitute a noninfringing use of the works under copyright law. Copying files and code underlying a work to a user's random-access memory ("RAM") and hard drive as necessary to install and utilize the work does not implicate any of the copyright holder's reproduction or adaptation rights under 17 U.S.C. § 106(1)-(2), and even assuming *arguendo* that it does,

---

[68] *See generally Sony Rootkit Comment*, *supra* note 43.

[69] *See* Staci D. Kramer, *EA Admits Spore Launched Botched by DRM; Still, Financial Damage Already Done*, THE WASHINGTON POST VIA PAIDCONTENT.ORG (September 19, 2008), *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/09/19/AR2008091900129.html ("Buyers worry that [Spore's] SecuROM software is actually installing spyware on their machines.").

making of new copies or adaptations of the works as necessary to install and utilize them is usually licensed by their publishers and also explicitly permitted under 17 U.S.C. § 117(a)(1). Furthermore, no other exclusive rights under section 106 are implicated: in particular, no other copies are made or disturbed; no other derivative works are prepared; and no works are publicly performed, displayed, or transmitted.

The access-protected copies of the works provide the only way for most consumers to engage in the installation and utilization of the works. Many works protected with technological measures such as SecuROM are distributed solely in a format exclusively compatible with the Microsoft Windows operating system. While some works may be available in alternate formats, such as those compatible with other PC operating systems, cellular telephones, or television video game systems, these alternate formats tend to vary widely from the original format in terms of functionality and reliability[70], and may force the consumer to invest hundreds or even thousands of dollars in a new PC, operating system, or video game system and compatible television simply to install and use a comparatively inexpensive work. Accordingly, an alternate means of engaging in this noninfringing use either does not exist or is an insufficient substitute for accomplishing the use due to lack of functionality or prohibitive expense, depending on the particular work.

B. Statutory Considerations

17 U.S.C. § 1201(a)(C) requires the Librarian to consider 1) the availability for use of copyrighted works; 2) the availability for use of works for nonprofit archival, preservation, and educational purposes; 3) the impact that the prohibition has on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; 4) the effect of circumvention of technological measures on the market for or value of copyrighted works; and 5) such other factors as the Librarian considers important. In this section, we address each factor in turn as applied to the proposed classes. Except where noted, the factors apply in the same or substantially similar ways to both proposed classes; while examples are given primarily in the context of Class 2, we believe it is clear that, based on the aforementioned trend toward the broad adoption of TPMs with security flaws, similar examples will arise in the wider context of Class 1.

1. Availability for Use of Copyrighted Works

The proposed exemption will likely have a positive effect on the availability of the copyrighted works at issue. Despite critical acclaim for the works at issue[71], a significant

---

[70] *See, e.g.*, David Clayman, *Head-to-Head: Fallout 3*, IMAGINE GAMES NETWORK (Nov. 3, 2008), *available at* http://xbox360.ign.com/articles/926/926646p1.html (in *seven* pages, detailing the differences between the four versions of Fallout 3, a Bethesda Softworks game, the PC version of which is encumbered with SecuROM).

[71] See Spore; METACRITIC.COM, available at http://www.metacritic.com/games/platforms/pc/spore?q=spore ("84[/100]," "Generally favorable reviews"); Mass Effect, METACRITIC.COM, available

number of consumers have been dissuaded from purchasing the works because of the aforementioned security risks[72]. In other words, the technological measure has the effect of lowering legitimate sales, as opposed to its intended effect of lowering piracy.[73]

If the proposed exemption is passed, security researchers are likely to devote considerable time and resources toward investigating SecuROM and similar TPMs, identifying security flaws and devising solutions as they did for the Sony rootkit. Careful study of TPM security flaws may reveal causative or contributory factors common to all TPMs that could help their designers eliminate future problems. Moreover, the transparent environment would incentivize content publishers to fund the creation of TPMs that respect the security interests of consumers while protecting copyright interests. Eventually, researchers could certify the security of TPMs, thus helping to convince consumers of the safety of those works encumbered with TPMs and thereby increasing the potential for legitimate sales.

2. Availability for Use of Works for Non-Profit Archival, Preservation, and Educational Purposes

After a TPM-encumbered, PC-accessible work is released, security risks are likely to increase over time as new problems are found. Unfortunately, the motivation of the publisher of the work to mitigate the risks is based primarily on the economic return of selling more copies of the work. As soon as the cost of fixing security flaws exceeds the potential profits of increased sales, the publisher is likely to stop releasing fixes. Alternatively, the publisher could simply go out of business. However, the unfixed security flaws leave consumers still using the work vulnerable to attack. Thus, using such a work safely in the long run will require some unofficial method of correcting security flaws. Without an exemption to the DMCA to allow security researchers to continue to investigate works that are no longer supported by their publishers yet still prevalent in the wild, the use of older works will become increasingly fraught with security risks.

---

athttp://www.metacritic.com/games/platforms/pc/masseffect?q=mass%20effect ("89[/100]," "Generally favorable reviews").

[72] One estimate puts Electronic Arts' lost sales revenue on Spore due to SecuROM as high as $25 million, which equates to approximately 500,000 users. *See* Kramer, *supra* note 68.

[73] Some commentators argue that TPMs like SecuROM actually *increases* piracy. *How EA and Spore Are Causing Piracy, the DasmX86Dll Issues, Removing SecuROM and Some Great DRM Free [sic] Alternatives*, ARSGEEK (Sept. 9, 2008), *available at* http://www.arsgeek.com/2008/09/09/how-to-remove-securom-spore-dasmx86dll-issues-and-some-great-drm-free-alternatives/. To wit, some DRM-free games appear to suffer from slightly lower piracy rates than their encumbered bretheren. *See* Seán Byrne, *DRM-free Games No Worse Off With Piracy*, CDFREAKS.COM (Nov. 18, 2008), *available at* http://www.cdfreaks.com/news/15216-DRM-free-games-no-worse-off-with-piracy.html.

3. Impact That the Prohibition Has on the Circumvention of Technological Measures Applied to Copyrighted Works Has On Criticism, Comment, News Reporting, Teaching, Scholarship, or Research

Research directed towards exposing security flaws created by TPMs like SafeDisc, SecuROM, and the Sony rootkit often involves activities that could expose the researchers to the threat of suit under the DMCA. This potential exposure has a chilling effect on the pace and scope of research in this field, without which the identification and mitigation of security risks and related debate, discussion, and scholarship will not occur.

Professor Halderman experienced first hand knowledge of this chilling effect on research and criticism when the manufacturer of insecure technological measures threatened him with a lawsuit prior to the third rulemaking. As was discussed extensively during the hearing, it is unclear that existing statutory preventions[74] provide the legal cover needed by security researchers to perform necessary research without the threat of suit. The time of security researchers would be better spent discovering and fixing security flaws than discussing potential DMCA liability issues with their lawyers.

The prohibition on the circumvention of TPMs on PC-accessible works (including video games) has also adversely impacted teaching. Many university computer science departments offer or are considering offering security courses covering DRM design and operation. Ideally, these courses could train future software engineers to build safer TPMs through immersive, hands-on laboratory components working with TPMs and traditional techniques used by attackers. However, the use of real-world examples of TPMs could give rise to lawsuits or threats thereof under the DMCA. The chilling effect on this important type of teaching and learning is precisely the kind of effect that Congress intended the present rulemaking to alleviate.

4. The Effect of Circumvention of the Technological Measures on the Market For or Value of Copyrighted Works

As under the availability factor, the circumvention of TPMs such as SecuROM is likely to have a *positive* effect on the value of the copyrighted works. For example, much of the criticism of *Spore* was directed not at the artistic merit of the game, but toward SecuROM.[75] In other words, the security risks caused by the TPMs (and the uncertainty about the magnitude of those risks) are likely to have a negative effect on the market for and value of the works. Accordingly, legalizing the good faith investigation and mitigation of those risks is likely to lead to better-informed consumers, fewer TPMs with security flaws, and, accordingly, a positive effect on the market for and value of the works.

Although some copyright owners may believe that TPMs such as SafeDisc, SecuROM, and the Sony rootkit are necessary to profitably distribute PC-accessible works, TPMs

[74] *See* 17 U.S.C. § 1201(i)-(j).
[75] *See, e.g.*, Kris Pigna, *Amazon Users Lash Out Against Spore DRM*, 1UP.COM (Sept. 8, 2008), *available at* http://www.1up.com/do/newsStory?cId=3169804.

laden with security flaws are likely to devalue both the TPMs themselves and the protected works by shaking consumer confidence in the security of the works, particularly when attacks that exploit the flaws are publicized. Because the proposed exemption will increase information about and fixes for security flaws in the TPMs, discourage further use of TPMs with security flaws, and decrease uncertainty about all PC-accessible works, whether or not they are plagued by TPM-enabled security vulnerabilities, the exemption is likely to positively affect the market for and value of video games by restoring consumer confidence in the security of those works.

5. Factors the Librarian May Consider Appropriate

TPMs that protect PC-accessible works pose serious threats to the PCs of consumers. While consumers have been warned for years about the dangers of downloading strange files from the Internet, they did not, until now, have particular reason to fear that content from established publishers could subvert the security of their PCs. Yet, the DMCA casts doubt on the legality of the good faith attempts of security researchers and consumers to rectify the situation. Surely Congress cannot have intended such a result. The DMCA was passed to help protect *legitimate* interests of copyright holders, not to hold security researchers and consumers hostage to security risks. Because of SecuROM and similar TPMs, informed consumers must either forsake access to their lawfully purchased works or face an uncertain level of security risk; uninformed consumers may unknowingly sacrifice security to gain access. This is an untenable predicament.

VI. Conclusion

The proposed classes would allow security researchers and consumers to collectively undertake the necessary measures to maintain both access and security. During the third rulemaking, the Department of Homeland Security laid out a strict edict to the music industry:

> *"It's very important to remember that it's your intellectual property – it's not your computer. And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days."*[76]

It is essential for the content industry to hear the same call – and to allow independent security researchers to ensure that its teachings are respected by the industry. Thus, we respectfully request that that the Register recommend and the Librarian grant an exemption for Class 1, or, in the alternative, Class 2, from the DMCA anti-circumvention measures.

---

[76] Michael Geist, *Sony's Long-term Rootkit CD Woes*, BBC NEWS (Nov. 21, 2005), *available at* http://news.bbc.co.uk/2/hi/technology/4456970.stm (quoting Stewart Baker, then-assistant secretary of policy for the U.S. Department of Homeland Security).

Sincerely,

/s/

J. Alex Halderman • Blake E. Reid • Paul Ohm • Harry Surden • J. Brad Bernthal

Exhibit A

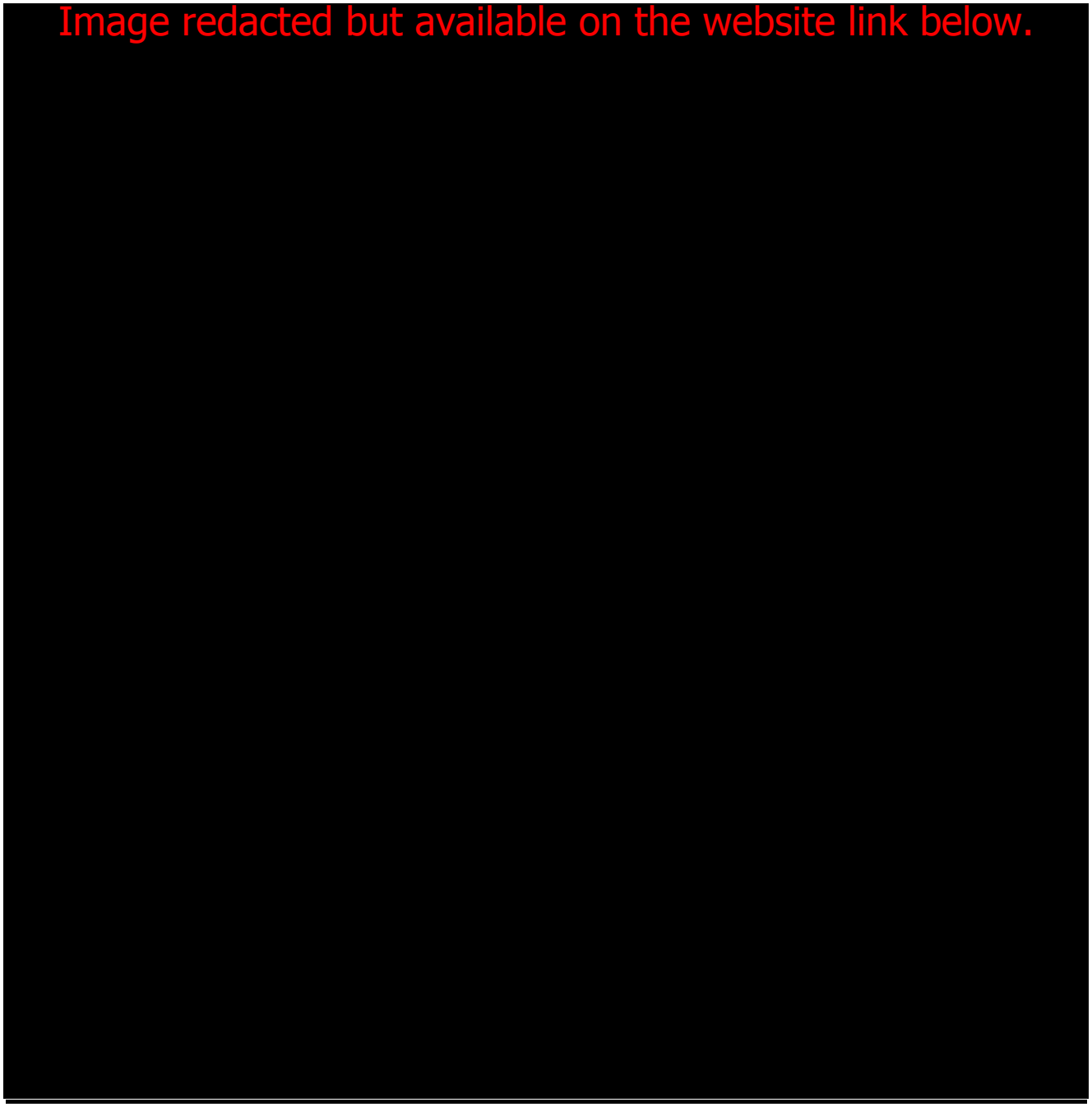

Fig. 1 – The Secret of Monkey Island "Dial-A-Pirate" Code Wheel[77]

[77] *Available at* http://www.scummbar.com/imageviewer/imageviewer.php?useimage=/games/media/mi12/mi1codewheel.jpg.