Comment of:
Edward W. Felten
Professor of Computer Science and Public Affairs
J. Alex Halderman
Department of Computer Science
35 Olden Street
Princeton, NJ 08544
Princeton University

Represented by:
Deirdre K. Mulligan
Director
Aaron Perzanowski
Law Clinic Intern
Samuelson Law, Technology & Public Policy Clinic
Boalt Hall
University of California
346 North Addition
Berkeley, CA 94720-7200

Office of the General Counsel
U.S. Copyright Office
James Madison Memorial Building, Room LM-401
101 Independence Avenue, SE.
Washington, DC 20559-6000

December 1, 2005

**Re: RM 2005-11 – Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies**

## I. Proposed Class Of Works

We respectfully request an exemption to § 1201(A)(1)(a) for sound recordings and audiovisual works distributed in compact disc format and protected by technological measures that impede access to lawfully purchased works by creating or exploiting security vulnerabilities that compromise the security of personal computers. The creation of security vulnerabilities includes running or installing rootkits or other software code that jeopardize the security of a computer or the data it contains. The exploitation of security vulnerabilities includes running or installing software protection measures without conspicuous notice and explicit consent and failing to provide a permanent and complete method of uninstalling or disabling the technological measure.

## II. Summary of Argument

Technological measures protecting works distributed on Compact Discs have been found to pose unreasonable security risks to consumers' personal computers, corporate and government networks and the information infrastructure as a whole. Vulnerabilities inherent in widely distributed CD protection measures create the potential for a frightening range of abuses. Viruses and Trojan horses are already leveraging these technologies to hide from antivirus programs and system administrators. Exacerbating the unacceptable risks posed by these technological protection measures, is that fact that the uninstallers provided to remove these measures pose additional security risks allowing a malicious web site to hijack a consumer's computer.

Security holes of this sort are regularly exploited by criminals. They may be used to turn the computer against its owner by sniffing passwords (including login information for financial sites), stealing business secrets and confidential data, and even holding the data on the PC for ransom. Such weaknesses also serve as launching points for attacks on third parties. Attackers can use such holes to penetrate otherwise secure home or corporate networks. Criminals can use them to enlist thousands of machines, unbeknownst to their owners, into massive "botnets"—armies of so called "zombie" computers—which are directed to relay spam (including pornographic messages) or conduct crippling distributed denial of service (DDOS) attacks. Past targets have included corporations and national security assets, including the infrastructure of the Internet itself. Zombies may also be used to relay anonymous messages and hide the activities of cyber criminals, including terrorist organizations, from law enforcement.

The security holes created by these protection measures force consumers to choose between two equally unappealing options: to accept intolerable security risks in order to access lawfully purchased CDs[1] or to circumvent the protection measures in order to gain lawful access *and* maintain a safe computing environment. This is a Faustian bargain. If consumers choose to listen they open their own systems as well as the broader Internet to countless security risks. The proposed exemption would allow users to take steps to ensure the security of their computers while enjoying access to the CDs they purchase without fear of liability under the DMCA for circumventing protection measures that undermine computer security.

[1] In addition to creating security risks, these technical protection measures interfere with lawful and customary uses of audiovisual works, limiting the ability of lawful purchasers to shift formats, choose listening platforms, and "shuffle" music tracks in order of their liking. Some of these programs invade privacy by actively collecting data about the in-home use of copyrighted works.

## III. The Submitting Parties

Edward W. Felten is a Professor of Computer Science and Public Affairs at Princeton University. Professor Felten's groundbreaking computer security research has established him as one of the field's leading experts, and his ongoing technology policy research addresses developing concerns regarding the legal regulation of technology and innovation. The DMCA has played a particularly important role in Professor Felten's research activities. In 2000, he and a team of researchers, after accepting a challenge from the Secure Digital Music Initiative (SDMI), succeeded in breaking SDMI's digital audio watermark. After facing legal threats under the DMCA, Professor Felten filed for declaratory judgment seeking a determination that his research did not violate the DMCA. Only after the RIAA disavowed any intent to file suit was that action dismissed.

J. Alex Halderman is a computer science Ph. D. candidate and researcher at Princeton University. His computer security and privacy research encompasses a variety of topics, but focuses particularly on the threats introduced by access and copy protection measures. In 2003, he published an academic paper discussing his research on SunnComm's MediaMax protection measure. Shortly thereafter, SunnComm threatened Halderman with legal action for his academic publication. After scathing criticism of its attempt to silence legitimate research, SunnComm publicly retracted this threat.

## IV. The Technological Protection Measures

For most of their twenty-five year history, audio Compact Discs (CDs) have been freely accessed and used by consumers who legally purchase them. Increasingly, however, record labels have sought to exercise greater control over consumers' access and post-sale uses of CDs. Although the particular protection measures employed to control access and use vary between labels and even between titles, these measures can be broadly categorized as either passive or active. Passive protection measures rely on changes to the structure of the data contained on the CD, such as inaccurate Tables of Contents, to assure compatibility with traditional audio CD players while preventing access and controlling use of the same CDs on many personal computers. In contrast, active protection measures, the focus of this comment, rely on the installation of software on the consumer's computer to prevent certain forms of access and use of audio files.

The current breed of active technological protection measures rely almost invariably on the AutoRun feature of the Windows operating system for initial installation. AutoRun allows software code contained on removable media like CDs to run automatically when inserted into a computer. Using AutoRun a CD can automatically install software on a computer without the knowledge or consent of its owner. In the context of CD protection measures, the software installed using AutoRun often includes a device driver that limits the functionality of the consumer's CD-ROM drive, preventing consumers from playing or copying their CD and creating the security risks described above. The current active technological protection measures exploit this aspect of AutoRun, because most consumers would prefer the freedom to make personal backup copies, listen to tracks in order of their preference, or transfer CDs to iPods or other

portable media players and are therefore reluctant to install software that would limit these lawful activities. Absent the installation of the this software, the CD format by nature allows consumers to freely access and use CD audio files.[2]

Once the consumer's CD-ROM drive has been altered, these protection measures typically present an End User License Agreement (EULA) detailing the permitted and prohibited uses of the CD. If the consumer "accepts" the EULA terms, these protection measures install software that the consumer may use to play the CD and copy DRM-protected Windows Media files. These files, unlike MP3 files, cannot be copied to portable media players like Apple's iPod. Most importantly the acceptance of the EULA and installation of this software introduces gaping holes in system security leaving the personal computer, and the networks it can be triggered to attack, open to a range of malicious activity. If instead, the consumer refuses the terms of the EULA, the disc is ejected and she is left unable to listen to her lawfully purchased CD on her computer.[3]

These protection measures have created serious threats to the security of personal computers, private and public networks, and the Internet generally, forcing consumers to choose between lawfully accessing the CDs they purchase and risking a hostile takeover of their computers. A protection measure called XCP developed by First4Internet and included in several million CDs distributed by Sony BMG included a rootkit, a software tool, the use of which is virtually unheard of in legitimate software development, designed to hide processes and files from computer users. Not only did this rootkit hide other components of Sony BMG's protection measure (ostensibly to render their removal more difficult), but it also created a serious security risk easily exploited by malicious hackers. Within days of the discovery of the rootkit, malicious code that took advantage of the rootkit's cloaking capabilities were being spread across the Internet.[4] Since millions of the CDs had been installed on some 500,000 computer networks[5] (including military, government, and business networks), the rootkit resulted in a major security threat to both individual consumers' personal computers and the nation's information infrastructure.

---

[2] Protected CDs often include "bonus" or "enhanced" multimedia content, such as music videos, in addition to audio content. We argue that the audiovisual works contained on CDs should fall within the exempted class of works as well.

[3] Although no court has determined that the active protection measures employed by protected CDs "effectively control access" to the discs' contents, this comment assumes—solely for the purpose of this rulemaking—that, at least for those users of the Windows operating system who have enabled the AutoRun feature, the protection measures described above are effective in controlling access to the audio files contained on those CDs.

[4] *Backdoor. Ryknos*, http://securityresponse.symantec.com/avcenter/venc/data/backdoor.ryknos.html.

[5] Paul F.Roberts, *Sony's 'Rootkit' Is on 500,000 Systems, Expert Says*, http://www.eweek.com/article2/0,1895,1887181,00.asp (Nov. 15, 2005).

Nearly a month after it first learned of the dangers posed by its rootkit,[6] and only after unrelenting pressure from consumers, security researchers, and the press, Sony BMG provided a program to uninstall the XCP rootkit. Unfortunately this uninstaller was fraught with security flaws even more dangerous than the original rootkit technology, allowing any webpage a user visits to secretly install or run code on her computer.[7] Subsequently, Sony BMG announced a recall of the effected CDs and, in recognition of the valuable contribution of security researchers, promised to forego potential DMCA claims against those engaged in legitimate research on its protection measures.[8] Despite the recall several organizations, among them the Electronic Frontier Foundation, filed class action lawsuits against Sony.[9] Finally, Texas Attorney General Greg Abbott filed suit against Sony BMG for violations of that state's anti-spyware legislation.[10]

Other measures that protect releases by Sony BMG and other labels, including SunnComm's MediaMax technology, permanently install software despite the consumer's explicit rejection of the software EULA.[11] This same protection measure collects and transmits data about consumers despite statements in both the software EULA and SunnComm's website denying any such behavior.[12] Not only must users fear surreptitious installation of software that compromises security and privacy, they must also fear deliberate disregard of their choice not to install unwanted software. Simply by placing a CD in their computer, consumers are exposed to potential security breaches even if they refuse to install the protection measures necessary to access their lawfully purchased CDs.

Sony BMG's rootkit and SunnComm's MediaMax software demonstrate the dangers of irresponsible attempts to protect copyrighted content. Software that sacrifices the security of consumers' computers and ignores their explicit refusal to install such software in order to increase control over the uses of CDs made by lawful purchasers creates unnecessary and unacceptable risks. These risks are compounded by software that installs without conspicuous notice and explicit consent, particularly when that software does not include a safe and effective method of permanent uninstallation. Unless

---

[6] See Steve Hamm, *Sony BMG's Costly Silence,* http://www.businessweek.com/technology/content/nov2005/tc20051129_938966.htm (Nov. 29, 2005).

[7] Ed Felten and J. Alex Halderman, *Sony's Web-Based Uninstaller Opens a Big Security Hole; Sony to Recall Discs*, http://www.freedom-to-tinker.com/?p=927 (Nov. 15, 2005).

[8] Letter from Jeffrey P. Cunard to Robert S. Green, Nov. 18, 2005, http://www.eff.org/IP/DRM/Sony-BMG/sony_response.pdf.

[9] Matt Hines, *EFF Takes Action Against Sony BMG*, http://www.eweek.com/article2/0,1895,1891843,00.asp (Nov. 21, 2005).

[10] *Attorney General Abbott Brings First Enforcement Action In Nation Against Sony BMG For Spyware Violations*, http://www.oag.state.tx.us/oagnews/release.php?id=1266&PHPSESSID=m0af3v583ms482pstg39o16lq6 (Nov. 21, 2005).

[11] J. Alex Halerman, *MediaMax Permanently Installs and Runs Unwanted Software, Even If User Declines EULA*, http://www.freedom-to-tinker.com/?p=936 (Nov. 28, 2005).

[12] Congress explicitly allowed the circumvention of technological measures that exhibit this sort of privacy–invasive behavior in 17 USC § 1201(i).

consumers are permitted to circumvent technological measures that create such risks, they will be forced to choose between maintaining the security of their computers and enjoying their lawfully purchased CDs.

## V. The Adversely Affected Non-Infringing Activity

The technological measures described above adversely affect at least four varieties of non-infringing uses: (1) listening, (2) engaging in security research, (3) device and format shifting, and (4) creating backups.

### A. Listening

The act of listening to a CD on a personal computer is lawful under any reading of the Copyright Act. Playing a CD on a computer for one's personal enjoyment implicates none of the exclusive rights granted to copyright holders under § 106. No copies are made or distributed; no derivative works are prepared; and no works are publicly performed. Nonetheless, without an exemption rational consumers would be dissuaded from engaging in this unquestionably lawful activity in light of the security risks posed by protection measures that are a barrier to access.

Without the proposed exemption, millions of computer users will be forced to risk the potential security threats created by protection measures like Sony BMG's rootkit in order to simply listen to their lawfully purchased CDs. For the millions of Windows users who have not opted to disable the default-enabled AutoRun feature,
playing their CDs on their computers requires the installation of technological protection measures. In order to access their lawfully purchased CDs, these consumers must endure potentially crippling security breaches like those created by Sony BMG's rootkit, that allow malicious code authored by third parties to run imperceptibly on consumers' computers or risk other equally dangerous undiscovered threats.

### B. Engaging in Security Research

Without the efforts of security researchers who discover and publicize risks such as those created by Sony BMG's rootkit, consumers would be nearly universally uninformed about the security threats they face. As Sony BMG's month-long delay in responding to the revelation of the dangers created by its rootkit demonstrate, consumers cannot rely on copyright holders to react with speed in providing information about the dangers of the software they foist on consumers. Thomas Hesse, Sony BMG's President of Global Digital Business appears to have summed up the attitude of copyright holders when he asked, "Most people, I think, don't even know what a rootkit is, so why should they care about it?" The vast majority of computer users lack the expertise to discover these threats independently. As a result, consumers must either rely on the research conducted by security experts or blindly trust software developers and content owners to exercise restraint in designing protection measures that respect consumers' security interests.

Unfortunately, the DMCA's anti-circumvention provision chills the efforts of security researchers. Because of the narrow scope of the DMCA's research exemption, the security researchers who are best situated to discover and disclose serious threats to personal computers face uncertain liability for their activities. In their efforts to determine the security threats posed by these protection measures, these researchers are likely to disable or remove some portion or the entirety of the protection measure, and thus potentially run afoul of the DMCA.

Researchers like Professor Edward Felten and Alex Halderman waste valuable research time consulting attorneys due to concerns about liability under the DMCA. They must consult not only with their own attorneys but with the general counsel of their academic institutions as well. Unavoidably, the legal uncertainty surrounding their research leads to delays and lost opportunities. In the case of the CDs at issue, Halderman and Felten were aware of problems with the XCP software almost a month before the news became public, but they delayed publication in order to consult with counsel about legal concerns. This delay left millions of consumers at risk for weeks longer than necessary.

Engaging in such research does not constitute copyright infringement. Security researchers are interested in the manner in which protection measures function and the security threats they may pose; they have no interest in the copyrighted content those measures are meant to protect. Copying of the CD audio files is often not even necessary to conduct their research.[13]

With no potential violations of § 106, the DMCA's ban on circumvention simply functions as a barrier to legitimate and publicly valuable research. As the ongoing spyware crisis has demonstrated, the efforts of independent researchers are crucial to maintaining a safe computing environment. An exemption for the above-described class of works would enable research that would help to ensure the security of consumers' personal computers.

**C. Device and Format Shifting**

While we recognize that the purpose of this rulemaking is to consider exemptions to the DMCA's prohibition against circumvention of access controls, the dual function of the protection measures at issue requires consideration of their affect on lawful copying as well. The active protection measures used on CDs typically control both access and use, including copying, of audio content. Because of the dual function of these protection measures, many consumers are prevented from creating lawful copies of their CDs despite the absence of a prohibition against circumventing copy controls in the DMCA. As a result, consumers are unable to create personal copies of their CDs in the format of their choice. Instead, they are typically permitted only to access compressed and DRM-protected Windows Media (WMA) files.

[13] When such copying is necessary, it should be deemed a fair use.

This limitation on consumer choice is problematic for a number of reasons. First, the Windows Media files are incompatible with the Apple iPod, the dominant portable media player. As complaints lodged on Amazon.com demonstrate, the inability to transfer lawfully purchased music to an iPod, which supports only the MP3 and AAC audio formats, is a pressing concern among consumers. Second, many users object to their inability to access an uncompressed digital copy of their purchased music. These audiophiles prefer to convert the Compact Disc Digital Audio (CDDA) files contained on their CDs to the WAV, SHN, or FLAC formats that, unlike lossy compressed standards like WMA and MP3, retain the highest digital fidelity.

Even for those consumers satisfied with the Windows Media file format, the presence of protection measures that satisfy the definition set out above interfere unreasonably with consumers' fair use rights to transfer CDs to other devices and convert them to other formats. Because the protection measures jeopardize security, many users will be unwilling to copy their CDs with the supplied software out of a justified fear of compromising the security of their computers.

Converting lawfully purchased CDs to other formats and transferring the resulting copies to another device are unquestionably fair uses. Even the record industry itself admits that both of these activities are lawful. Before the Supreme Court of the United States during the oral argument in Metro-Goldwyn-Mayer v. Grokster, counsel for the copyright holders explained, "The record companies, my clients, have said, for some time now, and it's been on their Website for some time now, that it's perfectly lawful to take a CD that you've purchased, upload it onto your computer, put it onto your iPod. There is a very, very significant lawful commercial use for that device, going forward."

Analysis of the four fair use factors supports this conclusion. First, the character of the use, while not transformative, is non-commercial. Consumers who transfer CDs to their iPods do so for their own enjoyment and not for any commercial gain. Similarly, the court in *Sony v. Universal Studios* determined that this first factor weighed in favor of fair use when considering non-commercial time shifting of over the air television broadcasts by VCR owners. The second factor, the nature of the copyrighted work, weighs against fair use because the sound recordings at issue here are entitled to full protection of copyright law. The third factor, too, weighs against fair use since consumers typically copy the entire work when format and device shifting. However, factors two and three are typically given relatively little weight in the overall fair use analysis. Finally, the fourth factor supports a finding of fair use. As portable electronic devices continue to displace traditional means of listening to music, the value of a copyrighted work increases as it becomes easier to use on a variety of platforms. From the perspective of consumers, music that cannot be played on the device of their choice is less valuable. In recognition of this fact, record labels and artists routinely instruct users on how to circumvent their own protection measures to convert CDs to other formats. Given the relative weight of the first and fourth factor, the analysis heavily favors fair use.

### D. Creating Backups

Just as the protection measures on CDs prevent many users from creating copies of audio content in other formats, they can also preclude consumers from creating backup copies of their CDs. Backup copies allow consumers to guard against damage, theft, or loss of the original CD media. True backup copies offer consumers functionality equivalent to the original media.

Although some protection measures allow consumers to copy CDs, these measures ensure that copies are of limited utility. These copies cannot be used to create additional backup copies in the event the original disc is damaged. Nor can these copies be used to copy DRM-protected files to the consumer's computer or portable player. As a result of the technological protection measure, these copies do not serve the same purpose as backup copies.

The creation of backup copies is lawful under copyright's fair use doctrine. Again, just as in *Sony*, the non-transformative non-commercial nature of backup copies supports a finding of fair use. Although both the nature of the copyrighted work and the amount copied weigh against fair use, these factors typically contribute little to the overall balancing of the fair use factors. Finally, the fourth factor weighs in favor if fair use. While record labels would undoubtedly appreciate the opportunity to sell consumers another copy of a CD should their original be damaged or stolen, the creation of personal archival copies is unlikely to harm the value of or market for the copyrighted works in question since the consumers in question have already purchased the CDs they hope to back up.

In addition, § 117 of the Copyright Act explicitly permits copying of the software contained on the CDs—the very software that restricts consumers' ability to access and copy their CDs. Consumers who purchase CDs are in lawful possession of the computer programs that serve as protection measures. Therefore, they are entitled under § 117(a)(2) to create archival copies of those programs.

Since copying the audio and other media files contained on the CDs constitutes a fair use and copying the software programs is permitted under § 117, creating backup copies of protected CDs in their entirety is a non-infringing activity.

## VI. Statutory Considerations

As detailed below, consideration of each of the factors described in § 1201(a)(1)(C) supports exempting the above-described class of works from the DMCA's anti-circumvention provision.

### A. Such factors as the Librarian considers appropriate

Because the primary concerns driving our request for this exemption do not fit easily within the other statutory considerations, we address § 1201(a)(1)(C)(v) first.

Protection measures like Sony BMG's rootkit pose a genuine threat to the security of both individual computer users and the network environment. Without providing notice or obtaining consent, Sony BMG installed software on the computers of millions of consumers that, unbeknownst to them, would enable any virus writer or computer hacker on the planet to secretly run programs on those consumers' machines. While consumers may expect this sort of behavior from spyware vendors, they did not — prior to this incident—expect the simple act of listening to a CD to result in effectively ceding control of their computers to the authors of malicious code.

By any objective evaluation of their characteristics, the XCP rootkit and SunnComm MediaMax protection measures would qualify as spyware. Both are installed without notification or consent, and both collect and transmit information about consumer usage without consent. In fact the primary distinction between these software programs and typical spyware applications is that, because of the DMCA, consumers and researchers may be legally prevented from removing and disabling dangerous and unwanted software. Such an outcome cannot be squared with Congressional intent in passing the DMCA. The DMCA was passed to protect the legitimate interests of copyright holders, not to prevent consumers from taking reasonable and necessary steps to ensure their own computing security. Because of the dangers posed by these protection measures, informed consumers must sacrifice lawful access to the works they purchase in order to secure their computing environment. Meanwhile less informed consumers will likely sacrifice both security and access by inadvertently installing these dangerous and restrictive protection measures.

**B. Availability for use of copyrighted works**

The proposed exemption will have no negative effect on the availability of copyrighted works. Instead, the exemption would likely increase the availability of those works.

The CD titles sold in protected format are typically unavailable in unprotected format in the United States. However, there is no reason to suspect that the CDs sold in protected formats would not be produced or sold if protection measures that create serious security risks to consumers could be circumvented. The vast majority of CDs sold contain no copy or access protection measures at all. Clearly the presence of protection measures is not a prerequisite for distributing a CD. Moreover, if protection measures were deemed a necessity for some titles, the proposed exemption would provide an incentive for the creation of protection measures that respect the security of consumers' computers while protecting the interests of the record labels.

The Sony BMG rootkit fiasco offers a telling example of the affect dangerous protection measures can have on the availability of copyrighted works. After public outcry forced a recall of several million CDs, the works of many artists are simply unavailable in most markets. During the busiest shopping season of the year, consumers are unable to purchase these CDs. By mitigating the damage suffered by consumers and

encouraging the development of safe protection measures, the proposed exemption would likely increase the availability of copyrighted works.

Given that consumers increasingly use computers and portable media players, rather than traditional Compact Disc players, to listen to the music they purchase, the proposed exemption would increase the availability of copyrighted works for high-demand uses. Many consumers purchase CDs primarily to convert them to compressed formats and transfer those files to portable devices like the iPod. To the extent the proposed exemption would enable such uses, more copyrighted works will be available for the uses that matter most to consumers. Without fear of security risks introduced by unwanted and unknown protection measures, these lawful uses are likely to become even more prevalent. By providing a disincentive to distribute dangerous protection measures, the proposed exemption would ensure the safety of purchasing and listening to music. Moreover, by allowing circumvention of these dangerous measures, the exemption would clarify the legality consumers' self-help efforts to ensure their security while enjoying their CDs. The added security, both technical and legal, provided by this exemption would likely spur an increase in the demand for and availability of copyrighted works distributed in CD format.

**C. Availability for use of works for nonprofit archival, preservation, and educational purposes**

The proprietary file formats and DRM schemes employed by the current breed of protected CDs face obsolescence in the future, some in the immediate future. Without the ability to archive the contents of CDs in the format of their choice, archivists risk the creation of stockpiles of data that may prove unreadable in a decade. An exemption would enable archivists to preserve protected CDs that fall within the class in the format of their choice.

Perhaps more importantly, an exemption would free archivists from the security risks posed by these protection measures. Archivists, because of the volume of material they process, face an increased likelihood of exposure to a variety of security risks introduced by security-compromising protection measures. These security risks are perhaps of even greater significance in the archival context since technologies like Sony BMG's rootkit could endanger the entire archive. An exemption would permit archivists to continue their efforts to preserve digital artifacts without risking the deleterious effects of security breaches.

**D. Impact of the prohibition on the circumvention has on criticism, comment, news reporting, teaching, scholarship, and research**

Research of the sort likely to expose security flaws created by protection measures like Sony BMG's rootkit often involves activities that could give rise to anti-circumvention claims under the DMCA. As a result, the pace and scope of research in this field has suffered. Absent research that first identifies security risks, debate and criticism of the tactics of copyright holders is necessarily stifled. The DMCA's ban on

circumvention functions as an effective barrier to research that would otherwise lead to increased consumer and industry awareness of serious security risks posed by certain software-based protection measures.

The authors of this comment have first hand knowledge of the chilling effect of potential liability under the DMCA on research and criticism. If the exemption we propose had been law just a few months ago, the discovery and disclosure of Sony BMG's rootkit technology would have undoubtedly come much sooner. The public outcry, expert discussion, and industry reaction likewise would have proceeded on a shorter timeline. Given the potentially dire consequences of mass-distributed malware such as Sony BMG's rootkit, research delays created by uncertain legal liability should be minimized. In short, researchers should busy themselves with discovering and disclosing security threats and not with engaging in protracted discussions of the DMCA with their attorneys.

**E. Effect of circumvention of technological measures on the market for or value of copyrighted works.**

Circumvention of technological measures protecting the above-described class are unlikely to prove detrimental to the market for or value of copyrighted works. Copyright holders derive little if any additional value from the presence of these protection measures. In fact, the real and perceived dangers of protection measures like Sony BMG's rootkit are likely to substantially detract from the value of those works. Perhaps most importantly, since the proposed exemption includes only those protection measures that create or exploit security risks or ignore consumers' decisions not to install the protection measure, the impact of the exemption could be easily avoided by the creation of protection measures that do not pose these threats to consumers.

As the software developers and record labels that create CD protection measures admit, they are intended to function merely as "speed bumps." While they cannot prevent all unlicensed copying of the audio content of CDs, they may sometimes succeed in restricting the uses that unsophisticated computer users can make of copyrighted works. But the utility of these protection measures is severely limited under a variety of circumstances. For Mac and Linux users, these protection measures are often entirely inoperative. Even on Windows, the effectiveness of these measures depends in large part on the easily disabled AutoRun feature. Regardless of their usefulness for the average computer user, for determined pirates, these technological measures create little if any "speed bump" affect. Preliminary data shows that protected CDs are just as widely available on peer-to-peer networks as their unprotected counterparts.[14]

Moreover, any added value to copyrighted works gained by these protection measures is already significantly undermined by copyright holders' own policies. The

[14] Of course, even if an exemption is granted copyright law still prohibits infringing distribution of the content of these CDs. Just as copyright's exclusive rights—coupled with secondary liability under *Sony* and *Grokster*—have proven sufficient to protect the market for and value of unprotected CDs, they will offer protection for works under this proposed exemption.

labels and the artists they represent have gone to great lengths to inform unsatisfied customers of methods by which they can create DRM-free digital copies of their CDs. Posts on artists' and labels' websites as well as technical support emails from the labels offer step by step instructions that undercut any beneficial effects on the value of or market for these works. While the conciliatory efforts of artists and record labels demonstrate the limited necessity and value of these protection measures, consumers should not be forced to rely on the discretionary good faith efforts of copyright holders in order to engage in lawful activity free from the fear of security threats.

Not only is the proposed exemption unlikely to detract from the value of the copyrighted works within the above-described class, it would likely increase the value of those works to both the copyright holders and the public. Even if some copyright holders believe, protection measures are necessary to profitable distribution of music, protection measures that compromise security only serve to devalue both their DRM systems and the works they are meant to protect. The public controversy surrounding the Sony rootkit debacle has shaken consumer confidence in the safety of Sony BMG's products and CD protection measures generally. The proposed exemption would help to restore confidence that lawfully purchased CDs will not harm consumers' computers. An exemption would help ensure that such measures are less likely to be employed in the future and that if they are, they can be discovered removed without fear of liability. The restored consumer confidence and increased CD sales resulting from the proposed exemption would help rather than harm the value of these works.

**VII. Conclusion**

As the Department of Homeland Security cautioned copyright holders in reaction to Sony BMG's rootkit, "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."[15] The proposed exemption, in keeping with the Congressional intent underlying the DMCA, would allow consumers to undertake the sort of self-help measures necessary to access and lawfully use the CDs they purchase without accepting unnecessary risks created by carelessly designed protection measures. For these reasons, we respectfully request that the Copyright Office recommend this proposed exemption.

[15] Michael Geist, *Sony's long-term rootkit CD woes*, http://news.bbc.co.uk/2/hi/technology/4456970.stm (Nov. 21, 2005).