Comment of:
Christopher Soghoian
Student Fellow
Berkman Center for Internet & Society
Harvard University
23 Everett Street, Second Floor
Cambridge MA 02138

Represented by:
Phil Malone
Director, Cyberlaw Clinic
Arjun Mehra
Clinical Student, Cyberlaw Clinic
Harvard Law School
Berkman Center for Internet & Society
23 Everett Street, Second Floor
Cambridge MA 02138

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 2, 2008

Re: RM 2008-8 -- Exemptions to Prohibition on Circumvention of Copyright Protection Systems for Defunct DRM and Copy Protection-Based Stores

I. PROPOSED CLASS OF WORKS

We respectfully request an exemption to DMCA §1201(a)(1)(A) for lawfully purchased sound recordings, audiovisual works, and software programs distributed commercially in digital format by online music and media stores and protected by technological measures that depend on the continued availability of authenticating servers, when such authenticating servers cease functioning because the store fails or for other reasons. We also request a separate exemption for the same class of works even prior to the failure of the servers for technologists and researchers studying and documenting how the authenticating servers that effectuate the technological measures function. The technological measures at issue include digital rights management (DRM) technologies and copy protection mechanisms encoded into purchased music, videos, and software, which are sold with a set of permissions and require authentication with remote

servers in order to allow users to fully exercise those purchased rights, including the ability to access the works on other devices, or in some cases, to allow continued access to the works on the same device. When the DRM servers malfunction or are shut down by their operators, consumers lose the rights to engage in the legitimate, non-infringing usage of content that they lawfully purchased and reasonably expected to continue using.

II. SUMMARY OF ARGUMENT

Most online music and media stores, such as Apple's iTunes Store and Microsoft's Zune Marketplace, use digital rights management (DRM) technologies in order to limit consumers' access to the music, videos, and software that they have lawfully purchased. Although DRM technologies differ by store, many require that a user authenticate any purchased works with a remote central server, run by the seller, in order to transfer the works to, and access them on, other computers or portable devices as permitted by the terms of purchase. At least one media store has required authentication when a user simply upgraded his operating system.[1] Another media store required authentication every time a user wished to play one of the purchased works.[2]

During the past decade, several major online music and video stores have ceased operating and stopped, or announced that they would stop, operating their DRM authenticating servers, thus endangering continued customer access to their lawfully purchased content. So far, widespread consumer backlash has forced these stores to either keep their DRM servers alive beyond the initially stated date of server termination, refund their customers the purchase price of all purchased works, or both. While these measures have so far prevented customers from losing complete access to their lawfully purchased works, there is no reason to believe that other companies or services that fail or are shut down in the future will provide similar corrective steps. When this happens, users will be adversely affected in their ability to continue making noninfringing uses of lawfully purchased media due to the DRM measures and §1201(a)'s prohibition on circumvention of those measures.

An exemption granted to the requested class of works would not affect the rights of copyright owners or the value of their works in any meaningful way. Consumers who previously purchased the works would simply be assured of access to the works for which they already have paid and have obtained a legal, noninfringing right to use, thereby maintaining, and perhaps even increasing, the market demand for and value of

---

[1] This was true for the Microsoft MSN music service, which required authentication when upgrading from Microsoft's own Windows XP to Windows Vista. *See* http://arstechnica.com/news.ars/post/20080422-drm-sucks-redux-microsoft-to-nuke-msn-music-drm-keys.html (accessed November 11, 2008).

[2] The now-defunct Google Video Store contained this restriction; the user had to be connected to the internet to view copy-protected videos. *See* http://www.google.com/press/guides/video_overview.pdf (accessed November 28, 2008).

the protected works.

A similar exemption for technologists and researchers studying, evaluating and documenting how the DRM schemes work prior to a DRM-based service's demise or the shutdown or failure of its authenticating servers will ensure that the information regarding the operation of such servers will be available to users in case of service failure, similarly increasing consumer confidence in such purchases.

III. THE SUBMITTING PARTY

Christopher Soghoian is a student fellow at the Berkman Center for Internet and Society at Harvard University and a Ph.D. candidate at the School of Informatics at Indiana University. His research is focused in the areas of computer security, privacy, technology law and policy. In his capacity as a security researcher, he has discovered and reported flaws in software products produced by Google, Yahoo and Facebook.[3] He also discovered and publicized security flaws in a website run by the Transportation Security Administration, which lead to an investigation of TSA's website security by the House Committee for Oversight and Government Reform.[4] He is the primary inventor of four pending patents in the areas of mobile phone authentication, secure digital cash, anti-phishing, and anti-virus system protection. In addition to his work in the field of applied computer security, Soghoian actively engages in legal research and recently published an analysis of legal issues associated with the large-scale reverse engineering and circumvention of DRM in subsidized consumer electronics by end-users. [5]

As a legitimate researcher with the technical skills to engage in the circumvention of defunct DRM, an interest in the public policy issues associated with failed DRM stores and authenticating servers, and sufficient knowledge of the law to appreciate that there are significant risks involved in such circumvention research, Soghoian has found his research activities in this area constrained by the substantial chill of the DMCA's anti-circumvention prohibitions.

---

[3] *See* http://www.securityfocus.com/news/11467 (accessed December 1, 2008); http://blog.wired.com/27bstroke6/2007/05/google_yahoo_fa.html (accessed December 1, 2008).

[4] *See* http://edition.cnn.com/2008/TRAVEL/01/15/tsa.loophole/ (accessed December 1, 2008); http://oversight.house.gov/story.asp?ID=1680 (accessed December 1, 2008).

[5] *See*, Christopher Soghoian, *Caveat Venditor: Technologically Protected Subsidized Goods and the Customers Who Hack Them*, 6 NW. J. TECH. & INTELL. PROP. 46 (2007). Available at http://ssrn.com/abstract=1032225.

IV. DIGITAL RIGHTS MANAGEMENT AND AUTHENTICATING SERVERS

A. Authenticating Server-Controlled DRM

Digital rights management (DRM), technological measures that limit access to, and thus use of, digital copyrighted content, such as music, videos, and software, are frequently employed by copyright owners and hardware and software manufacturers to control, among other things, the number of copies that can be made of a file, the number of times it can be accessed, the length of time that access is allowed, and to which devices the file may be transferred. One of the earliest examples of DRM is the Content Scrambling System (CSS) placed on commercial DVDs since 1996. CSS employs an encryption scheme that only allows authorized DVD players and DVD playback software to access the content on such DVDs. Another older form of DRM is the dongle, a code-containing device that needs to be plugged into a computer in order to allow the use of certain commercial software applications.

Most DRM schemes currently use remote online authentication servers in order to control access to content. The most prevalent form of DRM today, aside from CSS, is DRM encryption on music and videos bought online through various commercial services. However, DRM schemes can also be found in commercial computer software (including games), e-books, and the new Blu-Ray high definition disc format, with corresponding support for the schemes in computer operating systems and electronic hardware.

B. DRM-based Stores Have Failed In the Past

The concern addressed by this requested exemption is both real and substantial. Our short technological history is already littered with the remnants of failed and obsolete technological protection measures that employ authenticating servers. Thus far, when companies have announced the intended decommissioning of servers, a consumer outcry has resulted, demonstrating users' expectations of, and critical reliance on, the continued operation of the service to allow access to the content for which they have paid and gained lawful, noninfringing access. While this backlash heretofore has resulted in some companies delaying the termination of their DRM servers, it is likely that those servers will eventually be shut down. Moreover, there simply is no assurance that users' lawful access to their own content will similarly be continued when these situations arise in the future.

1. Circuit City's Digital Video Express (DIVX) Service

In 1998, Circuit City introduced a DVD rental store called Digital Video Express (or "DIVX"). The service relied on special, stand-alone DIVX-enhanced DVD players that were capable of playing both regular DVDs and DIVX discs. The players cost around $100 more than regular DVD players, while DIVX discs were $4.50 each. Once a customer began playing a DIVX disc, he could watch it as often as he liked for 48 hours, after which the disc became useless. A customer could "recharge" the disc by paying $4.50 for another 48 hours of access, or could pay a higher price to receive unlimited lifetime access to the disc. The entire process was handled by the DIVX player, which

dialed into an automated billing server over a telephone line. DIVX discs, regardless of their status, could be played only on DIVX-enhanced DVD players.

On June 16, 1999, Circuit City announced that it would discontinue making and marketing DIVX players and discs. The company offered all buyers of DIVX-enhanced players a $100 rebate and a full refund for those who had paid to unlock their DIVX discs. It also kept the DIVX billing servers alive until June 30, 2001, after which access to all discs was completely cut off.[6]

2. Google Video Store

In early 2006, Google launched a paid video store as part of its Google Video user-generated video platform. The Google Video Store, as it was called, allowed Windows users to buy or rent certain video content, which would be downloaded and played using Google's video player software. The paid videos were encoded with DRM technology that authenticated the videos, each time they were played based on the user's account information and the Google video player software. Thus, purchased or rented videos were inaccessible unless the user was connected to the Internet and using Google's proprietary playback software, which was available only on Windows PCs.[7]

Approximately a year-and-a-half after launching the video store, Google decided to discontinue it and shut down its authentication servers, which would have completely disabled consumers' access to all previously purchased videos. The company initially offered purchasers a credit towards future online purchases through its Google Checkout service, but after massive customer backlash,[8] the company reversed course and gave all of its Video Store customers a full credit card refund. Google also opted to delay the deactivation of its authentication servers by six months, during which purchased videos continued to be accessible.[9]

3. Microsoft's MSN Music Store

Microsoft launched its own online music store, the MSN Music Store, in

---

[6] *See* http://www.cnn.com/TECH/ptech/9906/16/divx.done; http://www.sfgate.com/cgi-bin/article.cgi%3Ffile=/chronicle/archive/1999/06/18/BU89741.DTL (accessed November 11, 2008).

[7] *See* http://www.google.com/press/guides/video_overview.pdf (accessed November 28, 2008).

[8] *See* http://googleblog.blogspot.com/2007/08/update-on-google-video-feedback.html (accessed December 1, 2008).

[9] *See* http://www.boingboing.net/2006/02/14/google-video-drm-why.html; http://googleblog.blogspot.com/2007/08/update-on-google-video-feedback.html (accessed November 11, 2008).

September 2004.[10] The store was based on Microsoft's PlaysForSure DRM scheme, which required authentication not just to access songs from several different computers, but also when a user upgraded his operating system, as from Windows XP to Windows Vista. In April 2008, after starting a new music service, Zune Marketplace, with a completely different DRM technology, Microsoft announced that that it would discontinue the MSN Music Store and would turn off its music license servers on August 31, 2008.[11]

After many customer complaints, Microsoft changed its stance and declared in June 2008 that it would keep its license servers alive until the end of 2011.[12] PlaysForSure is the same technology employed by several online music services, including RealNetworks' Rhapsody, the legal pay-for-use Napster music service, AOL MusicNow, MTV Urge, Yahoo Music, and Wal-Mart's first music service.[13]

4. Yahoo Music

Yahoo began selling music online in 2005, after it had purchased the Musicmatch service, an established player in the online music retail market. Yahoo's store used Microsoft's PlayForSure DRM technology.[14] After several years of operation, the company announced the termination of its Yahoo Music store in July 2008, stating that its authentication servers would shut down on September 30, 2008.[15] Just two days after its announcement, the company reversed course after receiving a significant number of negative customer complaints, as well as widespread negative coverage in the technology press, by offering a full refund to any customer who had purchased music through its service. However, the company did not extend the date on which it would shut off its DRM authentication servers.[16]

---

[10] *See* http://news.cnet.com/Microsoft-opens-MSN-Music-store/2100-1027_3-5342795.html (accessed November 15, 2008).

[11] *See* http://arstechnica.com/news.ars/post/20080422-drm-sucks-redux-microsoft-to-nuke-msn-music-drm-keys.html (accessed November 15, 2008).

[12] *See* http://blog.wired.com/music/2008/06/microsoft-backt.html (accessed November 15, 2008).

[13] *See* http://news.bbc.co.uk/1/hi/technology/6120272.stm (accessed November 15, 2008).

[14] *See* http://news.cnet.com/Yahoo-readies-iTunes-rival-for-launch/2100-1027_3-5603157.html (accessed November 15, 2008).

[15] *See* http://opinion.latimes.com/bitplayer/2008/07/yahoo-pulls-and.html (accessed November 15, 2008).

[16] *See* http://www.informationweek.com/news/personal_tech/music/showArticle.jhtml?articleID

5. Wal-Mart's Music Store

Wal-Mart first launched its downloadable music store in late 2003, using the Windows Media 9 file format (WMA) and DRM. Customers were able to burn CDs and make back-up copies of music tracks. The technology infrastructure was provided by Liquid Digital Media (formerly Liquid Audio).[17]

In August 2007, Wal-Mart began selling DRM-free MP3 tracks alongside its protected WMA tracks, and six months later, the store was completely DRM-free.[18] In late September 2008, Wal-Mart informed its customers that it would be shutting down its DRM servers on October 9, 2008 and recommended that users burn their DRM-protected tracks to CD for continued use.[19]

As a result of customer complaints, Wal-Mart reversed its policy, and announced on October 10, 2008 that it would keep the servers alive indefinitely. However, it continued to recommend to its customers that they back up their songs onto CDs.[20]

C. Overview of Currently Operating DRM-based Stores

Many currently operating online stores offer media vulnerable to similar loss of usage in the event of a shutdown, breakage or obsolescence of the stores' authenticating servers.

1. Apple's iTunes Store

Apple Inc.'s iTunes Store is the largest and most well known online music and video store. The store launched in April 2003, and five years later, it became the top music vendor in the United States.[21] It offers more than 8 million songs, 3,000 TV shows, 2,500 movies, and 3,000 software applications for use on the company's iPhone and iPod Touch devices.

=209601121 (accessed November 15, 2008).

[17] *See* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/12/19/BUG773QIO71.DTL&type=business (accessed November 15, 2008).

[18] *See* http://blog.wired.com/music/2007/08/wal-mart-announ.html (accessed November 15, 2008).

[19] *See* http://www.boingboing.net/2008/09/26/walmart-shutting-dow.html (accessed November 15, 2008).

[20] *See* http://www.boingboing.net/2008/10/10/walmart-now-says-the.html (accessed November 15, 2008).

[21] *See* http://www.apple.com/pr/library/2008/04/03itunes.html (accessed November 16, 2008).

Most music and nearly all videos offered through the iTunes Store are protected by Apple's FairPlay DRM technology, which is enforced through online communication between the iTunes software application and Apple's FairPlay authentication servers. When FairPlay was first introduced along with the iTunes store, it limited users to burning ten copies of a particular playlist onto a CD and allowed up to three computers to access the purchased songs at one time. Today, those limits are seven copies of a playlist, with authorization allowed for up to seven computers.[22] Apple has not licensed FairPlay to any other hardware or software manufacturers. Thus, FairPlay-protected files can only be played back using Apple's iTunes software or its own hardware devices (like iPod, iPhone, and Apple TV).[23]

In April 2007, the iTunes Store began offering songs and music videos whose copyrights were owned by the music company EMI free of FairPlay protection, albeit for a higher price than the same songs locked with DRM. Five months later, Apple dropped the price of its DRM-free tracks to the same 99-cent price as the DRM-protected songs in its catalog.[24] Apple has since expanded DRM-free sales to several independent music labels.[25] However, music by the other major record labels, as well as most video content in the iTunes store catalog remains DRM-protected.[26]

2. Microsoft's Zune Marketplace

Microsoft's Zune Marketplace is the equivalent of the iTunes Store for Microsoft's Zune music players. Launched in November 2006 along with the Zune hardware player, Zune Marketplace offers millions of songs and thousands of videos for sale. Most of this content is encrypted with Microsoft's Zune DRM scheme, which, although similar to the company's PlaysForSure DRM technology, is not interoperable with PlaysForSure. Thus, only the Zune hardware players and the Zune desktop software application for Windows can play back content protected by the Zune DRM, and the Zune player and software are incapable of playing back files purchased from stores using PlaysForSure (such as Napster, Rhapsody, and even Microsoft's own old MSN Music Store).[27] Although a third of Zune's music selection is offered in the DRM-free MP3

---

[22] *See* http://www.apple.com/legal/itunes/us/service.html (accessed November 28, 2008).

[23] *See* Nicola F. Sharpe and Olufunmilayo Arewa, *Is Apple Playing Fair? Navigating the iPod FairPlay DRM Controversy*, Northwestern Journal of Technology and Intellectual Property, Vol. 5, p. 331, 2007. Available at SSRN: http://ssrn.com/abstract=997159.

[24] See http://arstechnica.com/journals/apple.ars/2007/10/15/itunes-plus-drm-free-tracks-expanding-dropping-to-99-cents (accessed December 2, 2008).

[25] See http://www.digitalmusicnews.com/stories/012009pias (accessed December 2, 2008).

[26] *See id.*

[27] *See* http://news.cnet.com/8301-10784_3-9833174-7.html (accessed November 16, 2008).

format, Zune's DRM-protected content can be shared by up to three computers and three Zune devices.[28]

3. Napster

The second incarnation of Napster, as a legal, subscription-based music store, launched in 2003 with the second-largest collection of online music tracks. The tracks were all encoded using Microsoft's PlaysForSure DRM technology and could be lawfully played back on several authorized hardware players as well as on Microsoft's Windows Media Player software. In May 2008, Napster converted its entire 6-million song collection into DRM-free MP3s. However, it is keeping its PlaysForSure authentication servers online and not exchanging DRM-protected music previously bought through the service for the new DRM-free tracks.[29]

4. Other Stores

In addition to online stores that sell audio and video recordings, many software manufacturers now also use copy protection mechanisms utilizing remote server authentication. For example, the game developer Electronic Arts announced in May 2008 that its Mass Effect and Spore computer games would ship with a version of SecuROM copy protection software, which requires online authentication during installation, as well as re-validation every ten days for continued use of the game. n addition, the copy protection scheme would limit the number of simultaneous installations of the games to three.[30] In response to negative press coverage and customer complaints, Electronic Arts dropped the requirement to re-authenticate Mass Effect every ten days[31] and increased the limit on simultaneous installations of Spore from three to five.[32]

Microsoft also includes server-based copy protection methods in its Windows XP and Windows Vista operating systems. Both instances of Windows include a mandatory Product Activation process, which submits the software license key to a remote server along with a signature for the computer based on the processor type and serial number, the amount of memory, the hard disk and serial number, and the wireless or wired

---

[28] *See* http://support.microsoft.com/kb/928217 (accessed November 28, 2008).

[29] *See* http://news.cnet.com/8301-10784_3-9945987-7.html (accessed November 16, 2008).

[30] *See* http://www.1up.com/do/newsStory?cId=3167711 (accessed November 28, 2008).

[31] *See* http://www.joystiq.com/2008/05/10/bioware-drops-10-day-valdiation-from-mass-effect-pc (accessed November 28, 2008).

[32] *See* http://kotaku.com/5052473/ea-respond-to-drm-complaints (accessed November 28, 2008).

network adaptor.[33] If the user's Windows license key has not been used in the previous 120 days for a device with a different signature, Microsoft's servers will allow for the successful activation of the operating system.[34] If the user does not authenticate her copy of Windows within 30 days of the installation, the operating system will only boot into "Reduced Functionality Mode," which permits the use of Internet Explorer for only 60 minutes, after which the user will be logged out.[35] If significant portions of the computer's hardware change at a later date, the user will be forced to re-activate her copy of Windows, or again be restricted to Reduced Functionality Mode after a 3-day grace period.[36] Microsoft bowed to consumer complaints and did away with the Reduced Functionality Mode in the early 2008 release of Service Pack 1 (SP1) for Windows Vista. That mode was replaced with a "nagging" system that changes the background wallpaper every hour and displays frequent popup boxes, but keeps functionality intact.[37]

There is every reason to expect that this trend toward copy protection mechanisms based on remote server authentication for music, videos, computer games and other software will continue to expand and that greater and greater amounts of lawfully purchased media and software will be vulnerable to disruptions in the applicable authenticating servers.

V. ARGUMENT

The DMCA states that "[n]o person shall circumvent a technological measure that effectively controls access to a [copyrighted] work."[38] However, the DMCA also allows the Librarian of Congress, upon recommendation of the Register of Copyrights, to determine in a rulemaking held every three years whether noninfringing users of certain classes of copyrighted works are or will be adversely affected by the anti-circumvention provision.[39] Upon such a determination, the Librarian shall grant an exemption from the anti-circumvention provision for these users and those specific classes of works, for a period of three years from the time of the rulemaking.[40]

---

[33] *See* http://www.licenturion.com/xp/fully-licensed-wpa.txt (accessed November 28, 2008).

[34] *See* http://www.helpwithwindows.com/WindowsXP/activation.html (accessed November 28, 2008).

[35] *See* http://support.microsoft.com/kb/925582 (accessed November 28, 2008).

[36] *See id.*

[37] *See* http://blogs.zdnet.com/hardware/?p=1253 (accessed November 28, 2008).

[38] 17 U.S.C. §1201(a)(1)(A).

[39] 17 U.S.C. §1201(a)(1)(C).

[40] 17 U.S.C. §1201(a)(1)(D).

The DMCA lays out several factors that the Librarian should examine in conducting the exemption rulemaking.[41] An analysis of these factors strongly suggests that such an exemption should be adopted for lawfully purchased but DRM-protected sound recordings, audiovisual works, and software when the authenticating servers behind the DRM scheme are retired or for any other reason stop functioning.

A. Failed DRM Schemes Prevent Noninfringing Use of the Works They Protect

The first factor that the DMCA asks the Librarian to analyze is "the availability for use of [the affected] copyrighted works."[42] DRM-based stores that cease to operate or abandon their authenticating server system cause their customers to lose full, and often any, access to, and thus use of, their lawfully purchased works. Once an authenticating server goes down, the software and hardware that checks in with the server to verify licensed access to protected works is unable to do so, thus completely preventing whatever access is contingent on that check-in. This loss can take various forms. While it will not necessarily happen immediately after a particular store is discontinued, it does take place once the DRM authentication servers are shut down and a user decides to take any action with respect to the works that requires a connection the servers. The effect of the server shutdown in such a situation is to adversely affect users by denying them the lawful ability, for which they have paid, to access and use purchased content. Consumers' continued access to their lawfully purchased or licensed content even after any shutdown of authenticating servers plainly is, of course, plainly noninfringing.

In the now-defunct DRM-based services mentioned earlier, the companies either shut down the authentication servers and refunded customers for the content they had purchased or decided to continue operating the servers so that customers would not immediately lose access to their purchased works. In either case, however, the authentication servers most likely will eventually be shut down, at which point consumers will lose access to, and use of, the works that they have purchased. In some cases, the user can continue to play their purchased content without checking in with the servers, but if that user decides to transfer her legally purchased content to another device (which she should by law and license be able to do), the mandatory check-in with the authentication server will fail, and she will lose access.

The companies that have operated the failed services so far have been relatively large corporations such as Google, Yahoo, and Microsoft. These firms have deep enough pockets to be able to subsidize the gentle shuttering of their music services, by eventually agreeing to provide refunds to customers and to continue running the authentication servers for some period of time. A smaller company facing the closure of a failed online media store, however, would be unlikely to be able to provide such refunds or continued DRM server access.

---

[41] 17 U.S.C §1201(a)(1)(C)(i)-(v).

[42] 17 U.S.C §1201(a)(1)(C)(i).

Given the proliferation of downloaded content subject to authenticating-server based DRM, and the variety of firms offering such content and servers, the need for this exemption going forward is both real and substantial. In April 2008, Apple announced that its iTunes music store had overtaken WalMart's brick and mortar retail outlets as the top music retailer in the United States. Apple has sold over three billion music tracks since its launch in 2003.[43] In November 2008, Atlantic Records announced that digital sales now accounted for a majority (51%) of its revenue.[44] Finally, industry analysts predict that by 2013, digital downloads will make up more than 41 percent of the music market.[45]

Thus, over the next three years, millions of pieces of music, video, and software will be purchased from DRM stores and be controlled by authenticating servers. It is likely that in that same period at least one DRM-media store and/or its authenticating servers will shut down. The usage rights users obtain with those purchases will be jeopardized if consumers are not assured the ability to circumvent the DRM in the event the stores' central servers are shut down for any reason. Customers will be stranded without legal, noninfringing access to the works that they have lawfully purchased. Moreover, even the large companies that have already terminated their DRM stores but agreed to delay turning off their DRM authentication servers are unlikely to provide consumers with a total guarantee that they will continue to operate their servers for the next three years. In the event that these companies turn off the switch, their users too will lose access to their lawful media.

B. Failed DRM Schemes Prevent the Protected Works From Use for Nonprofit Archival, Preservation, and Educational Purposes

The next factor that the Librarian of Congress must analyze in granting an exemption to the anti-circumvention provision is "the availability for use of [the affected] works for nonprofit archival, preservation, and educational purposes."[46] The problem of inaccessibility for use of content lawfully purchased from failed DRM-based services is at least as serious for nonprofit institutions as for general customers, and most likely even more acute. Entities that lawfully purchase DRM-protected sound recordings, video, or software for archiving, preservation, or educational uses particularly need legal authority to allow long-term access to that material. While most of the DRM-based services described above do not require regular authentication for continued access on an already authorized machine, archival storage does not normally utilize personal computers or

---

[43] See http://www.cbsnews.com/stories/2008/04/04/business/main3993505.shtml (accessed December 2, 2008).

[44] See http://news.cnet.com/Digital-sales-surpass-CDs-at-Atlantic/2100-1027_3-6248057.html (accessed December 2, 2008).

[45] See http://arstechnica.com/news.ars/post/20081202-report-online-to-be-larger-piece-of-shrinking-music-pie.html (accessed December 2, 2008).

[46] 17 U.S.C. §1201(a)(1)(C)(ii).

hard drives. Rather, content is backed up on fixed media, like tape drives, and stored for years or decades before being accessed, most likely on an entirely different machine.

Consider the example of a library that backs up certain DRM-protected electronic files it has lawfully acquired onto a tape drive. If a librarian needed to access one of the files twenty years later, while it would be possible to copy the file onto a computer, he would be denied access to, and use of, the file because there would be no authentication server present to authorize the new machine onto which he tried to load it. That librarian's use of the file, which he had lawfully purchased, clearly would be noninfringing, but it would be impossible in the absence of the authentication server without circumvention of the DRM scheme.

Educational uses are also harmed. If a college music professor wishes to play certain DRM-protected sound recordings for his students in class, she can only do so if the authenticating servers needed to access or transfer the recordings lawfully to the necessary device are functioning. If those servers have been shut down or or are otherwise inoperable, the professor would be unable to access the files for this noninfringing educational use unless he could circumvent the DRM protection on the files.

C. An Exemption for the Proposed Class of Works Will Not Harm the Market For or Value of the Underlying Works

Another factor for the Librarian to consider in deciding whether to grant this exemption is "the effect of circumvention of [the] technological measure[] on the market for or value of [the underlying] copyrighted works."[47] The exemption that we request simply gives consumers the ability to access and lawfully view, use, and copy content that they have already purchased, and only in the event that the authenticating servers that restrict such uses are no longer working. As a result, the exemption will have no effect on the market demand for the work because the only users authorized to take advantage of the circumvention will be those who have already lawfully bought and paid for a license to the affected works.

In fact, the circumvention may even increase demand for DRM-protected content because potential customers of online music, video or software stores can be confident that they will retain access to and use of their acquired works, regardless of their point of purchase and the ultimate success or demise of the store they choose to patronize and its authentication server system.

D. Similarity to Previously Granted Exemptions

1. The Dongle Exemption

In its 2006 rulemaking, the Librarian of Congress approved an exemption to the anti-circumvention procedures of DMCA §1201 for "computer programs protected by

---

[47] 17 U.S.C. §1201(a)(1)(C)(iv).

dongles that prevent access due to malfunction or damage and which are obsolete. A dongle shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace." [48] The exemption requested here is quite similar to the dongle exemption. Dongles are "hardware locks attached to a computer that interact with software to prevent unauthorized access to that software."[49] DRM schemes are simply a software version of this kind of "lock" (or access control mechanism) that apply not only to software, but also to audio and video files. The Register of Copyrights in 2006 found a genuine problem with malfunctioning dongles from "vendors [that] may be unresponsive or have gone out of business."[50] Similarly, our request here is aimed at DRM-based services whose authentication servers have ceased to function.

Indeed, software DRM technology can be seen as the modern version of the dongle. While the cost of a physical dongle restricted such control devices to high-priced software in the past, the relatively low per-user cost of operating an Internet-based DRM authentication scheme has allowed the modern use of DRM protections for purchases as low as 99 cents per track of music. Access controls today are based primarily on remote server authentication rather than hardware controls like dongles. Thus, the important concerns addressed by the dongle exemption also conceptually include the class of works requested for exemption here, and the requested exemption merely seeks to allow similar continued access to content protected by this "new" form of dongle where access is disrupted by "malfunction or damage" to or "obsolete" authenticating server systems.

2. The Exemption for Obsolete Computer Programs

The Librarian in 2006 also approved an exemption for "[c]omputer 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."[51] The requested exemption shares much in common with this granted exemption. Files purchased and downloaded from DRM-based services whose servers are no longer functioning are essentially distributed in a "format[] that [has] become obsolete" and "require the original media or hardware as a condition of access." The DRM authentication server in this case is "the machine or system necessary to render perceptible a work" purchased from the service, and the particular DRM-protected format associated with the service is "no

---

[48] *See* http://www.copyright.gov/1201/2006/index.html (accessed November 21, 2008).

[49] *See* http://www.copyright.gov/fedreg/2006/71fr68472.html (accessed November 21, 2008).

[50] *See id.*

[51] *See id.*

longer manufactured or is no longer reasonably available in the commercial marketplace" once the service and its authentication servers shut down.

While the 2006 exemption applied only to computer programs and video games, we request that the exemption be extended to sound recordings and videos as well because the same deficiency that afflicts obsolete software in the authenticating server context is equally applicable to failed DRM-protected formats audio and video files. Also, we request that the exemption be extended to any use of the files, rather than limited to "preservation or archival reproduction . . . by a library or archive," because the class of works requested are largely bought by consumers for their daily use and it is consumers who most significantly will lose access to these works when authenticating servers are shut down.

E. Other Factors

In addition to the statutory factors described above, the DMCA allows the Librarian of Congress to consider "such other factors as the Librarian considers appropriate."[52] Below are some additional factors that argue in favor of the requested exemption.

1. Consumers Frequently Upgrade, Reinstall, or Replace Their Computers and Portable Media Devices

Several of the DRM and copy protection methods outlined earlier require re-authentication with remote servers when upgrading the operating system or hardware components of a computer, replacing the computer or portable media device, or even re-installing the operating system. Such activities are common, and becoming increasingly so, for consumers of computers and electronics.

For example, a 2007 study by Carnegie Mellon University revealed hard-disk failure and replacement rates of between 2%-4% every year and up to 13% for some systems.[53] Rapid obsolescence rates in consumer technology coupled with lowering costs of electronics mean that even if a user does not replace his system frequently, he is likely to upgrade components of his system that may well trigger the need to re-authenticate his DRM-protected files.[54] The wide prevalence of viruses and other malicious software on the Internet means high rates of infection,[55] particularly for

---

[52] 17 U.S.C. §1201(a)(1)(C)(v).

[53] *See* http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9012066 (accessed November 28, 2008).

[54] Upgrading a computer's motherboard, for instance, requires a brand new Windows license key. *See* http://support.microsoft.com/kb/824125 (accessed November 28, 2008).

[55] By some measures, a Windows PC has a 50% chance of being compromised by a virus or worm within 12 minutes of being connected to the internet.

inexperienced users. For many users, the only viable path to recovery from these crippling software attacks is re-installation of the operating system,[56] which will trigger required re-authentication for files protected by the PlaysForSure DRM scheme. Even portable media devices, like Apple's iPod, will often need to be replaced in less than the three years between anti-circumvention rulemakings,[57] again requiring re-certification by remote authentication servers.

The need for this exemption now is especially clear in light of these frequently occurring scenarios. If a DRM-based service shuts down and deactivates its authentication servers, a user will likely be deprived of access to his lawfully purchased works well before the Librarian of Congress and the Register of Copyrights have a chance to grant the appropriate anti-circumvention exemption in another rulemaking.

2. Creating Audio CDs and Re-copying the Sound Recordings Is Not An Adequate Substitute for This Eemption

Several of the failed DRM-based services mentioned above initially suggested to users that they could maintain access to their DRM-protected audio files by copying the files onto CDs (as Compact Disc Digital Audio, the format for regular CD audio tracks), then "ripping" (or re-copying) the music back onto their computers in a DRM-free audio format, such as MP3 or AAC. Unfortunately, there are several problems with this process that render it far from an adequate substitute for the loss of access sought to be addressed by this request.

First the ability to copy and then rip files into an unprotected format is only available for sound recordings; this method will not work for DRM-encoded videos or software. Second, the option to create an audio CD is only available if a user still has full access to the DRM-protected audio files (and the authenticating server) in the first place. Thus, this avenue is only open when the DRM authentication servers are still functioning. An online store that fails with little notice, or that discontinues its authenticating servers before users are able to take the potentially time consuming and laborious steps needed to rip all their music, makes this solution unworkable. Similarly, a librarian who wants to create an audio CD out of DRM-wrapped files that have been stored on portable media

---

http://www.zdnet.com.au/news/security/soa/The-12-minute-Windows-heist/0,130061744,139200021,00.htm (accessed November 28, 2008).

[56] "[T]he most effective option is to wipe or format the hard drive and reinstall the operating system. Although this corrective action will also result in the loss of all your programs and files, it is the only way to ensure your computer is free from backdoors and intruder modifications." Michael D. Durkota and Will Dorman, *Recovering from a Trojan Horse or Virus*, United States Computer Emergency Readiness Team. Available at http://www.us-cert.gov/reading_room/trojan-recovery.pdf.

[57] iPod and iPhone batteries come with a 1-year warranty, and considering the steep $50-80 cost of a new battery, many users are likely to replace the devices entirely. http://www.apple.com/batteries/replacements.html (accessed November 28, 2008).

for a period of years, after the DRM servers have been disconnected, cannot do so.

Third, while the audio files that result from this process are free of DRM protections, they also are inferior in quality to the original files. This is because many DRM-free audio files and DRM-protected audio files both encode sound recordings in a "lossy" format – that is, some quality is lost when originally encoding these files from the master recordings in return for smaller, downloadable file sizes. CD audio tracks, by contrast, are stored in the lossless CDDA format. When a user converts a DRM-encoded lossy audio file into a CD audio track, the quality of the track is inferior to what the quality would be if the track were recorded directly from a perfect quality master recording. When the user then re-rips the lower quality audio track back into a DRM-free lossy format (like MP3 or AAC), the process further degrades the quality of the track, resulting ultimately in a lower quality file than the DRM-encoded file with which the user started. For users who opted to pay a financial premium for a higher quality audio track, the end of this cumbersome process is a poorer quality recording, plainly an inadequate substitute for the higher-quality access for which they have paid.

Finally, this indirect method takes about four to five minutes to create a 60-minute audio CD from digital files and an equal amount of time to rip the tracks back into a DRM-free format. While the overall time commitment is not tremendous for a few hours of music, the length of the process would be unreasonable and quite burdensome for large audio collections, which many users have and for which they have paid substantial amounts for noninfringing access.

3. The "Analog Hole" Is Not an Adequate Alternative to the Exemption.

One alternative to directly accessing the DRM-protected files through circumvention is recording the analog signals that result from using or playing the digital files. For example, a DRM-encoded audio file, when played on an authorized music playback device, can be connected to a speaker, which plays the sounds of the file out loud. A user could then record these sounds and save them into a DRM-free file format. This aspect DRM technology that allows this digital-to-analog-to-digital circumvention is known as the "analog hole." The analog hole could conceivably be used to obtain access to videos, which could be re-captured by another device once they are displayed on a screen.

Yet, this method is subject to the same access hurdle a user faces when creating an audio CD. In order to re-capture a sound recording or video from a DRM-protected file, the user must have functional access to the file in the first place. Once the DRM authentication servers stop working, a user is completely unable to play the file.

Another problem with exploiting the analog hole for audio and video is that the method described invariably results in lower quality copies, when the user originally paid for high quality versions of the works. Such a solution would therefore be an unwanted and unacceptable form of access to content for customers of failed DRM services. Finally, the analog hole is completely unavailable as an alternative to accessing software, which requires interaction rather than simply listening or viewing.

F. Technologists and Researchers Require a Separate Exemption to Document DRM Schemes Even Prior to Store Failures

Providing an exemption for circumvention of DRM to consumers after the failure of the DRM store authentication servers, as requested above, is necessary to maintain lawful, noninfringing access. By itself, however it is not a fully effective solution to failed DRM systems. Most consumers, of course, will not have the information or technical skills necessary to circumvent a failed DRM scheme even if such circumvention is exempted from §1201's prohibitions. Furthermore, once a DRM service has been turned off, it may be impossible, for both experts and end users, to learn enough about its workings to effectively circumvent the protection. Understanding modern DRM schemes now requires collaboration by teams of technologists and researchers, who require a clear exemption from the DMCA's anti-circumvention provisions in order to study, test, and document the schemes in case they fail in the future.

1. Effective Circumvention of a DRM Scheme After It Fails Requires Good Faith Research and Documentation of the Technology During Its Operation

In general, there are two ways to circumvent a copy protection or DRM scheme. One is to disable the specific portions of the computer code that perform the copy protection check. Another is to allow the check to proceed, but send back false (yet valid-looking) authentication data. For both of these methods of DRM circumvention, researchers must be able to observe the normal operation of the DRM scheme in action. This includes being able to monitor the messages sent back and forth between a customer's computer and the central DRM authentication server, as well as being able to observe the computer instructions that are executed as a song, movie, or piece of software is decrypted and run.

Once the authentication server has been turned off, it is impossible to observe the authentication channel as well as to observe the computer instructions that execute after a successful message has been received. Thus, technologists and researchers require an exemption to be able to study, test, and document authentication server DRM schemes even before the service ceases to operate. Waiting to begin the observation, study and documentation until the server has been turned off will significantly increase the difficulty of the task, perhaps even making it impossible.

It is important to note that many of the strongest contributions to encryption research related to the weakness of technological protection measures have and still continue to come from "amateurs," who may be self-taught, or even highly educated in theoretical or practical computer science, but are not part of the formal DRM research community. Thus, it is vital that the exemption considers the motivation and work performed by the technologist, and does not require an advanced degree, certification, or prior academic publications in the field.

2. This Exemption Is Similar to the Rootkit Exemption Granted In 2006 By the Librarian of Congress

In 2006, the Librarian approved an exemption for "[s]ound 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.[58] The exemption requested for researchers here is similar to that exemption because the purpose of the exemption here is also for "good faith testing, investigating, or correcting" (or reverse engineering and documenting) of currently operating DRM schemes so that adequate information about them is available in the event that their supporting authenticating servers are shut down or become inoperable.

Also like the 2006 exemption, the researcher exemption is necessary because "it is not clear whether [DMCA §1201(j)] extends to such conduct."[59] DMCA §1201(j) states in relevant part that "it is not a violation of [the anti-circumvention provision, DMCA §1201(a)(1)(A),] for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section,"[60] where "security testing," means "accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network."[61] The cases of failed DRM and copy protection systems do not easily fit into the category of "security flaw or vulnerability."

Moreover, the purpose of the researcher exemption, which is to effectuate the general user exemption when circumvention is needed, requires reverse engineering and documentation to proceed even without the permission of the DRM technology owners and operators. Just as Felten and Halderman noted in their 2006 exemption comment, "[b]ecause 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."[62] This equally applies to those who reverse engineer DRM and the

---

[58] *See* http://www.copyright.gov/fedreg/2006/71fr68472.html (emphasis added) (accessed November 29, 2008).

[59] *Id.*

[60] 17 U.S.C. §1201(j)(2).

[61] 17 U.S.C. §1201(j)(1).

[62] Comment of Edward W. Felten at 7, submitted 12/01/05,

working of authenticating servers for the purpose of documenting their workings. It is likely that researchers and technologists will disable or remove some portion of the protection measure in the process of determining how the scheme functions. In order to ensure that legitimate, good-faith researchers are not exposed to legal jeopardy for the task of documentation, these acts of circumvention should be exempted.

3. Waiting for Notice That a DRM-based Service Will Be Shut Down Will Not Provide an Adequate Exemption

Limiting permission for researchers to circumvent DRM systems as soon as the future planned termination of a particular central DRM authentication server has been announced would not be a workable alternative. A company operating a failing DRM-based media store in the future may not provide any or much advance notice to users, unlike the several months of notice that failing DRM stores have given their customers thus far. In such a situation, researchers would have no time to legally analyze and document the failed DRM scheme. Furthermore, were such a limited window of early circumvention to be approved, it may even encourage companies to shutter their DRM services quickly, without providing notice to customers.

VI. CONCLUSION

The first proposed exemption would allow users and consumers of DRM-protected media to continue to access their lawfully purchased and noninfringing content in situations where the authentication servers on which their access relies stop working. The second exemption would allow researchers in good faith to study, analyze and document the protection measures when needed, without fear of jeopardy for any necessary circumvention that is part of the research process. At the same time, each exemption would preserve the interests of copyright owners because each would allow users to access only those files that they have lawfully purchased and to which, in the absence of the failure of the authenticating server, they have lawful, noninfringing access. Moreover, the exemptions would allow such access by circumvention only when the necessary DRM servers have actually failed or are otherwise inoperable. For these and the other foregoing reasons, we respectfully ask that the Copyright Office recommend, and the Librarian of Congress approve, the exemption for the class of works requested.

---

http://www.copyright.gov/1201/2006/comments/mulligan_felten.pdf (accessed December 1, 2008).