Christopher Soghoian
Student Fellow
Berkman Center for Internet & Society
Harvard University

Represented by:

Phil Malone
Director, Cyberlaw Clinic

Rachel Gozhansky
Clinical Intern, Cyberlaw Clinic

Harvard Law School
23 Everett Street, Second Floor
Cambridge, MA 02138

Rob Kasunic
Principal Legal Advisor
Office of the General Counsel
United States Copyright Office
101 Independence Ave SE
Washington, DC
20559-6000

July 10, 2009

Dear Mr. Kasunic,

Thank you for the opportunity to provide additional information regarding our exemption requests and to respond to the follow-up questions posed in your letter dated June 22, 2009. We describe a critical new development regarding DRM servers in Section I, and then in Sections II and III, we provide our detailed responses to each of the questions raised in your letter (your questions are in italics).

I. Recent Events Clearly Establish That There is a Real Need for These Exemptions and That Consumers Are Likely to Suffer Substantial Adverse Effects Without Them

During the May 6, 2009 §1201 Rulemaking Hearing for Exemptions 10A and 10B, Christopher Soghoian was asked, "Is there any evidence to suggest that this [an authentication server going down and consumers being left without access or a refund or

other appropriate remedy] is in fact likely on any kind of—any kind of significant scale during the next three-year period?"[1]

Parties seeking Digital Millennium Copyright Act (DMCA) exemptions need only show that the Act's prohibitions have or are likely to have a substantial adverse effect on non-infringing uses of a class of works.[2] Mr. Soghoian's response to this question at the hearing, and the arguments in our original request fully meet this requirement. In his testimony, Mr. Soghoian pointed to a strong likelihood of such consumer harm based on the current state of the economy and the fact that over the last several years, various media companies have shut down their authentication servers with increasing regularity and have only been inclined to provide, reluctantly, remedies for customers after considerable public and media outcry.

Specifically, Mr. Soghoian pointed to the fact that after Wal-Mart announced that it intended to shut down its authentication servers in September 2008, the outcry from consumers was so strong that the company ended up retracting its statement and saying it would continue to support the servers indefinitely. As Mr. Soghoian remarked at the hearing, however, Wal-Mart "clearly has no intention to run that server forever, so at some point they are going to turn it off."[3]

That point in time has now come. Just three weeks after the hearing, on June 1, 2009, Wal-Mart announced that as of October 9, 2009, it will shut down the authentication servers supporting the DRM-protected music purchased by its customers.[4] Wal-Mart is not providing its customers with a refund or any other remedy but instead has suggested that its customers should make do with burning their music to CDs. As our original exemption request to the Copyright Office noted at length, this is an inferior solution that will permanently reduce the audio quality of the products legally purchased by Wal-Mart's customers, products to which the customers should be entitled to have full and continuing access.

Wal-Mart's latest actions provide ample evidence that the issue of DRM abandonware is not a hypothetical concern and that the market cannot be counted on to provide consumers with an adequate remedy. As long as the ability to circumvent the DRM on lawfully acquired music is barred by the DMCA, consumers will suffer direct and substantial adverse effects. The recent Wal-Mart news also demonstrates quite clearly that, even in those instances where companies might initially promise to continue to run their authentication servers in response to consumer backlash, the hand that giveth can (and will) later taketh away. Without these exemptions, consumers will be harmed.

---

[1] Transcript of §1201 Rulemaking Hearing before the United States Copyright Office at 53:19-22 (May 6, 2009).
[2] See Digital Millennium Copyright Act, 17 U.S.C. §1201a(1)(B) (1999)
[3] Transcript of §1201 Rulemaking Hearing at 53:2-4 (May 6, 2009).
[4] Mark Hefflinger, *Walmart to End Support for DRM-Wrapped Songs in October*, Digital Media Wire, (June 1, 2009) http://www.dmwmedia.com/news/2009/06/01/walmart-end-support-drm-wrapped-songs-october.

II. Copyright Office Follow-up Question 1

Assume that we will conclude that a case has been made for the proposed Exemption 10B. Please provide your reaction to the following limitation: "…when the information obtained by the technologists and researchers is used only to provide access to works protected by the technological measures that depend on the continued availability of an authenticating server when [1] access is provided only to persons to whom access had been provided by the authentication server prior to its failure, [2] the authentication server has permanently ceased functioning, and [3] the provider of the service has neither made alternatives means of access to the works available nor provided a refund for the loss of access to the purchased copies of the works."

A. General Response

We assume that you intend these proposed limitations to ensure that any study and documentation of DRM server systems done by researchers and technologists is limited to legitimate purposes in the abandoned-DRM context and is not abused for other, improper purposes. Although we understand these concerns as a general matter, the proposed limitations, as currently phrased, would create a set of impossible hurdles that no researcher or technologist could meet. These limitations would effectively require researchers to know the unknowable and to predict the unpredictable far in advance in order to begin their DRM study and documentation, prior to the failure of the servers and any response by the server operator.

In order for researchers to be exempt from potential DMCA liability for their work, the language proposed in your letter would require them to know – up front – that the information developed by their work would be "used only to provide access to works" where three future conditions are met: (1) the subsequent access will only be by people who had lawful access under the working DRM server; (2) a particular authentication server will cease functioning in the future, and (3) the provider will fail to make alternative means of access or refunds available to customers. Thus, this phrasing requires researchers to possess foresight regarding how other persons, well into the future, may make use of their research and documentation, as well as what will happen to particular DRM servers and what steps the providing companies will or will not take to provide alternative access or refunds to consumers. These are things that legitimate researchers, acting in good faith, prior to a failure, wanting to study and document how authenticating servers function, simply cannot know.

In order to be meaningful, Exemption 10B needs to ensure that researchers and technologists who, in good faith, undertake the study and documentation of how authenticating servers function are protected from the risk of DMCA liability or frivolous lawsuits if, months or years later, the DRM servers remain operational, or, if the servers are abandoned, the service provider chooses to provide an alternative means of access or a refund for the loss of access. The exemption also must protect researchers and

technologists from legal liability for any improper actions later performed by other persons who, without the researchers' advance knowledge or complicity, use the researchers' documentation for illegitimate and illegal purposes not within the scope of Exemption 10A.

In fact, it is likely that the researchers and technologists who reverse engineer an authentication server-based DRM scheme for the purpose of documenting its functions will not be the same persons who, months or years later, after the DRM servers have been disabled, will make use of that information. Just as it does not make sense to punish a security researcher based on the later actions of a cyber-criminal who uses the researcher's good faith discovery and responsible disclosure of a software vulnerability to write a virus, it does not make sense to punish researchers who work to document the functionality of DRM schemes for the later, illegal actions of others in which the researchers did not participate.

To punish the researcher for the subsequent and impossible-to-predict actions of other companies or persons would be inappropriate and would chill legitimate researchers from making use of the exemption and thereby wholly undermine the purpose of the exemption: ensuring that consumers have the information necessary to maintain continued access to their lawfully acquired content.

Consequently, it is vital that any limitation imposed on Exemption 10B to prevent possible abuse focus on the actions and motivations of the researcher rather than on unforeseeable future actions of individuals or companies. Looking to the good faith acts or intent of the researcher at the time of the research is not only the best way to protect against possible abuse, but is also consistent with other recent approaches in copyright law. The DMCA itself already utilizes this approach, as discussed below in Section III of our response. In addition, in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, the Supreme Court, in finding Grokster's peer-to-peer file sharing network liable of copyright infringement, focused in part on Groksters's objectives in making their software available.[5] The Court held that "one who distributes a device with the **object of promoting its use** to infringe copyright" is liable for the resulting acts of infringement by third parties.[6] Thus, focusing on the ex ante good faith actions of researchers, in the context of the purpose of this exemption, rather than focusing on the unpredictable ex post actions of others or market developments, will achieve the exemption's goals while fully ensuring that Exemption 10B is not misused by bad actors for purposes outside those legitimate goals.

To accomplish what we understand to be the goal of your proposed limitation without chilling legitimate research or creating an impossible burden for researchers, we propose the following alternative language to limit the exemption:

[5] 545 US 913 (2005).
[6] *Id*. at 919 (emphasis added).

> 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, prior to the failure of the authenticating servers for technologists and researchers studying and documenting how the authenticating servers that effectuate the technological measures function, **unless such study and documentation was not performed in good faith**.

B. The Copyright Office's Proposed Approach is Better Suited to Exemption 10A:

We have explained that the proposed, numbered limitations quoted above are not workable or appropriate to add to Exemption 10B. To the extent the Copyright Office continues to believe that the elements of those limitations are necessary to narrow our request, we submit that they are far more suitable and practical, in a slightly modified form, as limitations to Exemption 10A, for the general public's circumvention of abandoned DRM to access lawfully acquired works.

If you feel further limits are essential, we would not object to appropriately limiting Exemption 10A with the following modifications (explained in sections C-E, below):

> 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, only when [1] access **is gained by** persons **who previously had lawful access to both the works and** the authentication servers prior to their failure, [2] such authenticating servers **become effectively unavailable for a significant period of time**, and [3] the provider of the service has neither made **available** alternative means of access to the works that **are substantially equivalent in functionality to the original means of access and offered at no additional cost to the consumer**, nor provided a **full** refund for the loss of access to the purchased copies of the works.

C. Discussion of Your Proposed Limitation [1]: *"access is provided only to persons to whom access had been provided by the authentication server prior to its failure"*

First, this limitation should be applied to Exemption 10A, not 10B, for the reasons explained above.

Second, there is no reason why Exemption 10A should not be limited both to lawfully purchased works (which was in our original exemption) as well as only to persons who were legally permitted to make use of those purchased works and the authentication server prior to the shuttering of the authentication server. We have modified the proposed limitation text to reflect this, as seen above under Section II.B of our response.

D. Discussion of Your Proposed Limitation [2]: *"the authentication server has permanently ceased functioning"*

Again, this limitation should be applied to Exemption 10A, not 10B, for the reasons explained above.

With regard to this limitation, we are concerned by the proposed insertion of the word "permanent." While we do not believe that consumers should be free to circumvent the DRM in the event of brief or transitory interruptions, such as a temporary power failure at the data center in which the authentication servers are hosted or a one- or two-day-long software glitch on the servers, we are extremely concerned that requiring "permanent" shutdown goes much too far in the other direction. For one thing, "permanent" would be very difficult for consumers to know or establish up front before they began to circumvent DRM to regain access to music or other content they had lawfully purchased. They would not know whether they needed to wait a month to see if the servers were turned back on, or six months, or a year, or more.

Moreover, a "permanent" requirement would permit companies to utilize ambiguous announcements or strategies, deliberately or inadvertently, to avoid triggering this section of the exemption. For example, a company might announce that, out of a desire to cut costs, it was going to turn off its authentication servers for 11 out of 12 months of the year or was going to turn the servers off for an indefinite period but with a statement that it would reactivate them at some unspecified future point. Similarly, a company might announce the termination of its servers without mention of a duration for the shutdown, turn them off, and then some months later turn the servers back on again, at which time consumers might fear exposure to a DMCA circumvention suit if they had utilized the exemption in the interim.

These and possible similar actions would clearly and substantially harm consumers and deprive them of access to their lawful content but might not be seen as enough to trigger the protective circumvention provisions of Exemption 10A if a "permanent" limit were included.

For this reason, we propose modifying the text of your proposed limitation as follows:

> … such authenticating, servers **become effectively unavailable for a significant period of time**, and …

E. Discussions of Your Proposed Limitation [3]: *"the provider of the service has neither made alternative means of access to the works available nor provided a refund for the loss of access to the purchased copies of the works."*

Once again, this limitation should be applied to Exemption 10A, not 10B, for the reasons explained above.

We are concerned that the term "alternative means" is too broad and indefinite and might allow a media store to provide alternative solutions that are limited in quality or scope, or limited to the number or types of customers, or limited in some other way, to the substantial adverse effect for consumers. For example, a vendor might propose (as Wal-Mart recently has) that, even though its DRM servers were being shut down, consumers could burn their music to CDs, a clearly inferior option that would leave consumers with significant reductions in the quality of their content compared with what they legally purchased (and what they could regain by circumventing the DRM pursuant to this exemption). Or a music provider whose DRM-secured works were accessible on Microsoft, Apple, and Linux based computer systems might shut down its authentication server and attempt to offer customers an alternative means to access their lawful music through a third party provider whose DRM software only supported Windows computer systems. In that case, any customer with an Apple or Linux based computer system who purchased the music with the legitimate expectation that it would play on their computer could no longer access the works they had paid for. Moreover, they would be unable to make use of Exemption 10A because the vendor could claim it had made "alternative means of access" available.

Under your proposed phrasing, it is also possible that a service provider might use the shutdown of DRM servers as a final opportunity to extract additional revenue from its soon-to-be-former customers. For example, currently Apple's iTunes allows customers to upgrade their DRM music to non-DRM versions by paying an additional $.30 per song. If Apple were to shut down its iTunes authentication servers, it might demand that its customers pay the additional $.30 to strip the DRM from their music collection or risk losing access to the music. While this might be seen as an "alternative means of access" to those works, it would be one that harmed consumers and deprived them of access to works for which they had already paid in full.

Finally, the current phrasing of the proposed limitation could permit vendors to attempt to make partial refunds and to claim that they had avoided invoking the exemption. The language needs to clearly specify that refunds must be full and complete.

To address the above concerns and prevent any ambiguity that might allow such scenarios to occur, we propose modifying the limitation text:

> … the provider of the service has neither made **available** alternative means of access to the works that **are substantially equivalent in functionality to the original means of access and are offered at no additional cost to the consumer**, nor provided a **full** refund for the loss of access to the purchased copies of the works.

F. Applying the Copyright Office's Proposed Limitation Text to 10B:

As detailed in Section II.B above, it would be both unnecessary and counterproductive to impose the proposed limitations [1]-[3] on Exemption 10B. However, if the Copyright Office remains committed to limiting the researcher exemption

beyond what we suggest in Section II.A, at a minimum the specific limitations in your Question 1 first must be modified in the same ways we propose for Exemption 10A in Sections II.C, D and E, above.

In addition, we feel it is vital that the focus of any such limitations be on the actions and motivations of the researcher rather than on the unforeseeable future uses, as addressed above in Section II.A and below in Section III. With this goal in mind, the limitation should be edited to include language that includes the up front, "good faith" approach.

If the Copyright Office feels it is essential to further limit Exemption 10B, we propose the following modifications:

> 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, prior to the failure of the authenticating servers for technologists and researchers studying and documenting how the authenticating servers that effectuate the technological measures function, **with the intent that the** information obtained by the technologists and researchers **will be used to** provide access to works protected by the technological measures that depend on the continued availability of an authenticating server when [1] access is **provided to** persons **who had lawful access to both the works and** the authentication servers prior to their failure, [2] such authenticating servers **become effectively unavailable for a significant period of time**, and [3] the provider of the service has neither made **available** alternative means of access to the works that **are equivalent in functionality to the original means of access and are offered at no additional cost to the consumer**, nor provided a **full** refund for the loss of access to the purchased copies of the works, **unless such study and documentation was not performed in good faith**.

III. Copyright Office Follow-up Question 2

> *Would it be appropriate to limit the persons who would be eligible to invoke Exemption 10B? Why? If you believe it would be appropriate to limit the persons eligible for Exemption 10B, what criteria could be used?*

We believe that it is both inappropriate and unnecessary to limit the application of Exemption 10B to particular persons based on criteria such as having professional or formal academic training, or being employed in a university or industry research setting or similar security profession, or the like. First, any attempt to define a qualified "class" of technologists and researchers would be artificial and under-inclusive. In reality, many discoveries and innovations made by the security and computer science community have come from laypersons, tinkerers and hobbyists who do not necessarily have formal "credentials." For example, Linus Torvalds was not an established academic researcher or a professional working in the field of operating systems when he began developing the

Linux operating system, which he initially pursued as a hobby.[7] Yet the success and impact of his work with Linux have been profound.

Second, limiting the application of Exemption 10B is unnecessary to achieve the intended purposes of the exemption or to avoid any risks of overbroad application of the exemption. To ensure that the researchers protected by this exemption genuinely study and document how DRM-authenticating servers work, we believe it is more appropriate to focus on the nature of the specific research actions and the intent and purpose of that research rather than to focus, artificially, on the formal qualifications of the particular technologist or researcher.

In fact, this is the approach repeatedly taken by the DMCA that includes various references to "good faith" acts and efforts by "persons" rather than a special class of researcher. For example:

> 1201(g)(2) **Permissible acts** of encryption research. — Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for **a person** to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of **an act of good faith** encryption research if —[8]
>
> > (C) **the person** made **a good faith effort** to obtain authorization before the circumvention; and[9]
>
> * * * * *
>
> 1201(g)(4) Use of technological means for research activities. — Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for **a person** to —[10]
>
> > (A) develop and employ technological means to circumvent a technological measure for the sole purpose of **that person performing the acts of good faith** encryption research described in paragraph (2); and[11]

---

[7] "I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones." *See* Email from Linus Benedict Torvalds to comp.os.minix newsgroup (August 26, 1991) *available at* http://groups.google.co.uk/group/comp.os.minix/browse_thread/thread/76536d1fb451ac60/b813d52cbc5a044b; Linus Torvalds & David Diamond, *Just for Fun: The Story of an Accidental Revolutionary* (HarperCollins 2001).

[8] 17 U.S.C. §1201g(2) (emphasis added).

[9] 17 U.S.C. §1201g(2)(C) (emphasis added).

[10] 17 U.S.C. §1201g(4) (emphasis added).

[11] 17 U.S.C. §1201g(4)(A) (emphasis added).

> (B) provide the technological means to **another person** with whom he or she is working collaboratively for the purpose of conducting the **acts of good faith** encryption research described in paragraph (2) or for the purpose of having that **other person** verify his or her **acts of good faith** encryption research described in paragraph (2).[12] [13]

The DMCA is not alone in this sensible approach. For example, the anti RFID-skimming statute recently adopted by California states that:

> Subdivisions (a) and (d) shall not apply to the reading, storage, use, or disclosure to a third party of a person's identification document, or information derived therefrom, in the course of **an act of good faith** security research, experimentation, or scientific inquiry, including, but not limited to, activities useful in identifying and analyzing security flaws and vulnerabilities.[14]

Any concerns that an otherwise unlimited Exemption 10B would allow "bad actors" to attempt to "break" DRM authentication server systems for improper purposes rather than the lawful, legitimate purposes covered by Exemption 10 can be fully resolved by our proposed limitation language for 10B described above: "technologists and researchers who are studying and documenting how the authenticating servers that effectuate the technological measures function . . . , **unless such study and documentation was not performed in good faith**." This focus on the good faith actions and intent of the researchers in the context of the purpose of this exemption ensures that the Exemption cannot be misused by bad actors to escape liability under the DMCA.[15]

---

[12] 17 U.S.C. §1201g(4)(B) (emphasis added).

[13] While we recognize that 17 U.S.C. §1201g(3)(B) does provide, in determining whether a person qualifies for exemption §1201g, some reference to the individual's background, specifically "whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced in the field of encryption technology," this provision is quite broad and, by its terms, covers a wide range of training and experience. If the Copyright Office feels it is necessary to limit the persons eligible for Exemption 10B, we recommend adopting similar language, as discussed below.

[14] Cal. Civ. Code §1798.79 (2009) *available at* http://www.dmv.ca.gov/pubs/vctop/appndxa/civil/civ1798_79.htm (emphasis added).

[15] Our placement of the burden of showing lack of good faith upon those bringing DMCA suits will still fully prevent bad actors from improperly shielding their abuse with the exemption, since their bad faith and lack of proper intent can be readily established. At the same time, our approach will ensure that legitimate research will not be chilled by the risk of costly and burdensome litigation before the researchers are able to establish their good faith at an advanced stage of the litigation. This chilling effect would be substantially greater if the burden were on the researchers to prove good faith. Since there is often a significant disparity in resources between large plaintiffs and small, independent researchers, the public interest is best served by ensuring that researchers are able to resolve the good faith issue at the early stages of a case.

However, if at the end of the day the Copyright Office still believes that some additional limits are needed on the particular persons who are eligible to invoke Exemption 10B, we suggest that the most straightforward limitation would be to adopt language similar to that already used in 17 U.S.C. §1201(g)(3)(B) cited above. We propose adding the clause, "…who are engaged in a legitimate course of study, are employed, are appropriately trained, self-taught or otherwise experienced in computer science, …" so that the relevant part of the exemption would read:

> … technologists and researchers **who are engaged in a legitimate course of study, are employed, are appropriately trained, self-taught or otherwise experienced in computer science and who are acting in good faith, to study and document** how the authenticating servers that effectuate the technological measures function, **unless such study and documentation was not performed in good faith**.

We hope these responses fully address your questions. If you have any additional concerns or follow-up inquiries, we would welcome the opportunity to address them.

Sincerely,

/s/

Christopher Soghoian,
Student Fellow,
Berkman Center for Internet & Society

Represented by:

Phil Malone
Director, Cyberlaw Clinic
Berkman Center for Internet & Society

Rachel Gozhansky
Clinical Student, Cyberlaw Clinic
Berkman Center for Internet & Society