Before the
U.S. Copyright Office
Library of Congress
Washington, DC

In the Matter of **Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies**	))))	Docket No. 2014–07

Reply Comment on Proposed Class 25: Security Research

of

Dr. Matthew D. Green

Dr. Matthew D. Green, PhD
Assistant Research Professor
Department of Computer Science
Johns Hopkins Information Security Institute
Johns Hopkins University

mgreen@cs.jhu.edu • 410-861-0344

spar.isi.jhu.edu/~mgreen/

3400 N. Charles Street, 209 Maryland Hall,
Baltimore, MD 21218

Samuelson-Glushko Technology Law & Policy Clinic (TLPC)

Counsel to Prof. Green

Chelsea E. Brooks, Student Attorney
Joseph N. de Raismes, Student Attorney
Andy J. Sayler, Student Technologist
Prof. Blake E. Reid, Director

blake.reid@colorado.edu • 303-492-0548

Colorado Law
Robert & Laura Hill Clinical Suite • 404 UCB
Boulder, CO 80309-0404

Table of Contents

Introduction

We respectfully submit this reply comment in response to comments on the proposed exemption and related exemptions in Class 25.[1] Our initial comment requests exemption from the anti-circumvention measures of the DMCA for good faith security research on behalf of Professor Matthew D. Green. Professor Green is a noted cryptography researcher and an assistant research professor at Johns Hopkins University, where he focuses on applied cryptography and cryptographic engineering. Additionally, he investigates how cryptography can enhance end-user privacy. The student attorneys and technologists at the Samuelson-Glushko Technology Law & Policy Clinic (TLPC) at Colorado Law advocate for the public interest in important public policy and legal matters with technological dimensions.

Granting our proposed exemption is necessary to allow for good faith security research. Comments filed in opposition demonstrate the willingness of companies to raise claims unrelated to copyright infringement under Section 1201, which is itself evidence of the adverse effects Section 1201 has on security researchers. Most of the claims raised by objectors address medical or environmental policy and speculative loss of consumer confidence stemming from criticism, none of which are relevant to copyright infringement. Even where objectors do focus on concerns related to copyright infringement, they fail to demonstrate that security research poses any serious risk of copyright infringement. Section 1201's existing statutory exemptions are inadequate to provide good faith security researchers with the assurance that they will not be held liable for non-infringing research. The Register should not recommend disclosure standards in this proceeding because setting disclosure standards is outside the scope of this rulemaking. In light of these facts, the Register should recommend the proposed exemption.

Discussion

I. The record establishes that granting a security research exemption is necessary to avoid chilling good faith security research.

Our initial comments in this proceeding describe substantial adverse effects Section 1201 imposes on researchers' ability to conduct good faith security research and the need for the proposed exemption to avoid those effects.[2] The subsequent record supports the same result. Numerous commenters support an exemption for good faith security research, and the concerns raised by the few objectors do not justify a contrary result.[3]

[1] Long Comment of Dr. Matthew D. Green Regarding a Proposed Exemption at 11-17 ("Green

[2] *See* Green Comment at 17-22.

[3] *Compare* Green Comment, Long Comment of Security Researchers ("Security Researchers"); Long Comment of Stallman, Erik et al. ("Stallman"); Short Comment of the Free Software Foundation ("FSF"); Short Comment of the Verified Voting Foundation ("VVF"); Short Comment of the U.S. Public Policy Council of the Association for Computing Machinery ("ACM"); Short Comment of Dr. Salvatore J. Stolfo ("Stolfo"); Short Comment of Mark Stanislav ("Stanislav") *with* Comments of General Motors LLC ("GM"); Long Comment of Advanced Medical Technology Ass'n & Medical Imaging and Technology Alliance
(continued…)

Most of the concerns raised by objectors are focused on automotive and medical software, while it is largely undisputed that the Register should recommend an exemption for security research on non-medical, non-automotive software. Moreover, the concerns raised over automotive and medical software are largely unrelated to the protection of copyrighted works and therefore do not provide any basis to deny an exemption for medical or automotive software either. The willingness of objectors to invoke Section 1201 to address non-copyright concerns in this proceeding exemplifies their willingness to do so in litigation to chill real-world security research. This underscores the significant likelihood of continuing—and worsening—adverse effects if the exemption is not granted. To whatever extent concerns over automotive and medical software are legitimate, the triennial review is not the appropriate forum in which to address the contours of automotive and medical policy.

A. There is little dispute that the Register should recommend a security research exemption for non-medical, non-automotive software.

While several commenters raise concerns over the application of a security research exemption to software on medical devices and automobile engine control units (ECUs), the record is largely devoid of similar concerns about applying a security research exemption to other types of software.[4] Indeed, the record is replete with support for a security research exemption for general purpose software and the devices that run it, including operating systems, voting machines and software, Internet of Things (IoT) devices such as appliances, control systems, surveillance systems, and entertainment systems, embedded devices, networking devices, communication devices, and many related systems.[5]

Thus, the record demonstrates that the Register should recommend an exemption for good faith security research on non-medical, non-automotive software. While we do not believe the concerns over automotive and medical device software warrant different treatment, the record demonstrates that the Register should recommend, at the very least, a general security research exemption with a narrow limitation pertaining to automotive and medical device software.

B. The Register should not credit concerns unrelated to copyright infringement in this proceeding.

While objectors raise concerns over the discovery or disclosure of security vulnerabilities, they are not primarily concerned that such discovery or disclosure will result in copyright infringement.[6] Instead, they appear primarily concerned that the inability to invoke Section 1201

("AdvaMed"); Short Comment of The Alliance of Automobile Manufacturers ("Auto Alliance"); Long Comment of BSA The Software Alliance ("BSA"); Comment of Intellectual Property Owners Ass'n ("IPOA"); Long Comment of LifeScience Alley ("LifeScience"); Short Comment of Medical Device Innovation, Safety and Security Consortium ("MDISS"); Short Comment of Software & Information Industry Ass'n ("SIIA").

[4] *See* GM at 5-6; AdvaMed at 2; LifeScience at 2; Auto Alliance; BSA; IPOA; MDISS.

[5] *See* Green Comment; Security Researchers; Stallman; FSF; VVF; ACM; Stolfo; Stanislav.

[6] *See* GM at 6*;* AdvaMed at 6; IPO at 1; LifeScience at 4.

to prevent such discovery and disclosure will lead to increased public transparency about dangerous security vulnerabilities in widely available software and devices and potentially harm the sales of those software and devices as a result.[7] For example:

- GM argues that circumvention of technological protection measures ("TPMs") for good faith security research would weaken consumer's faith in GM vehicles because consumers might become aware of serious security flaws in their vehicles;[8]
- The Advance Medical Technology Association (AdvaMed) claims that publicity related to security vulnerabilities into medical devices can lead to "patient panic;"[9]
- LifeScience notes that the proposed exemption may expose medical device manufacturers to liability for flaws in their products;[10]
- BSA references potential adverse effects stemming from research related to industrial applications concerning critical infrastructure.[11]

These concerns do not form a cognizable basis for the Register to deny the proposed exemption because they are wholly unrelated to the purpose of Section 1201—to protect against copyright infringement.[12] As the Register has previously recognized, Section 1201 is not intended to protect business practices that rely on the existence of technological protection measures.[13] Where there is no legitimate risk of copyright infringement from circumvention, Section 1201 cannot be legitimately invoked as a basis to deny an exemption.

Even if Section 1201 legitimately could be invoked to prevent the circumvention of TPMs in contexts where no copyright infringement was at issue, doing so in this context would be contrary to sound public policy. Effective security practice requires external validation of the security of critical software by third-party researchers like Prof. Green and other proponents of a security research exemption. Moreover, the discovery of vulnerabilities that render products unsafe—particularly in life-critical systems like automobiles and medical devices—often requires public disclosure of such vulnerabilities. Such disclosure is necessary to warn consumers of potentially life-threatening risks, especially when companies have strong financial incentives to avoid recalling products or disclosing problems.

Indeed, the claims by some commenters that internal security processes are sufficient to address security concerns are contravened by real-world examples.[14] GM, which argues that Original Equipment Manufacturers (OEMs) "are highly responsive when it comes to fixing

[7] *See* GM at 6; AdvaMed at 6; LifeScience at 4.

[8] *See* GM at 6.

[9] *See* AdvaMed at 6.

[10] *See* LifeScience at 4.

[11] *See* BSA at 3.

[12] *See generally* Bill D. Herman & Oscar H. Gandy, Jr., *Catch 1201: A Legislative History and Content Analysis of the DMCA Exemption Proceedings*, 24 Cardozo Arts & Ent. L.J. 121 (2006).

[13] *Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies*, Final Rule, 75 Fed. Reg. 43,831 (July 27 2010) ("2010 Recommendation of the Register of Copyrights").

[14] *See* GM at 19.

software glitches and providing pertinent software updates," recently failed to disclose a dangerous flaw in the ignition switches of nearly 28 million cars that resulted in at least 80 deaths.[15] Such lack of disclosure in the face of safety-related product flaws demonstrates the importance of the kinds of independent third party review facilitated by the proposed exemption. Denying the proposed exemption would allow Section 1201 to serve as a roadblock for security researchers to discover and disclose similar vulnerabilities, putting the safety of consumers at risk.

C. The willingness of objectors to argue that Section 1201 should prevent non-infringing security research establishes the likelihood of adverse effects.

The concerns raised by objectors over security research on automotive and medical device software fail to establish a cognizable basis for opposing the proposed exemption. These concerns also fail to accord with sound public policy, and demonstrate that Section 1201 will adversely affect security researchers in the absence of an exemption.

As we noted in our initial comment, security researchers routinely face threats from companies asserting that the discovery and disclosure of serious security vulnerabilities violates Section 1201.[16] The comments filed by objectors in this proceeding conclusively demonstrate that these concerns are not merely hypothetical. In opposing this exemption, several of the world's leading manufacturers and trade groups in automobile, medical device, software, and related industries have publicly asserted their belief that performing computer security research as described in our initial comment may constitute a violation of Section 1201.[17]

Not only do we disagree with objectors' assertions for the reasons discussed throughout this filing, their arguments that security research violates Section 1201 in this context evinces a willingness to make similar claims in litigation in order to threaten security researchers and chill security research. The assertion that a non-infringing activity like security research violates Section 1201 is proof of the likelihood that Section 1201 will be used to adversely affect those who wish to engage in that activity, and underscores the need for the Register to recommend the proposed exemption.

D. The triennial review is not an appropriate forum to address the broader contours of environmental or medical policy.

Objectors further invite the Register to deny the proposed exemption because of its potential impact on environmental and medical policy. For example, LifeScience Alley and AdvaMed both argue that granting the proposed exemption might run afoul of Food and Drug Administration (FDA) regulations, while GM argues that security research on automotive

[15] *Compare* GM at 19 *with* David Shepardson, *GM ignition death toll rises to 80*, The Detroit News, Apr. 6, 2015, http://www.detroitnews.com/story/business/autos/general-motors/2015/04/06/gm-ignition-death-toll-rises/25354619/.

[16] Green Comment at 17-18.

[17] *See* AdvaMed; LifeScience; IPOA; GM; SIIA; BSA.

software might implicate the emission regulations of the Environmental Protection Agency (EPA).[18]

We urge the Register to decline objectors' invitation to encroach on medical and environmental policy issues. At the outset, it is unclear that many of the activities underpinning objectors' environmental or medical concerns are even within the scope of the proposed exemption. For example, we do not believe that the proposed exemption, which is limited to circumvention for the purpose of good faith security research, would encompass activities like modifying ECUs on production automobiles for the purpose of tuning engine performance or circumventing access controls on medical devices already implanted in patients.[19]

Nor is it clear that any of the activities at issue actually implicate environmental or medical law or policy. For example, previous automobile-related security research has been limited to testing cars for short periods of time in highly controlled environments such as test tracks, closed parking lots, or wheel blocks, and have primarily focused on communication, braking, lighting, locking, and similar systems—not engine, exhaust, or other EPA-regulated automobile components.[20]

Regardless, to whatever extent security research activities might implicate environmental or medical policy, the triennial review process is not the appropriate forum in which to address the contours of that policy, nor is the Copyright Office the appropriate agency to do so. Environmental and medical policy issues are not copyright policy issues. Whatever narrow intersections between security research activities and environmental or medical policy might exist can be addressed by policymakers at the FDA, EPA, and other appropriate agencies. In the hypothetical circumstance that security research might violate an applicable environmental or medical law or regulation—a circumstance not established in any of the objectors' comments—remedies under that law or regulation would remain available. There is no reason to expect that exempting an activity under Section 1201 would preclude policymakers from proscribing it if it raised legitimate concerns.

None of the hypothetical environmental or medical concerns raised by objectors address copyright policy or the relevant considerations for exemptions spelled out by Section 1201. Accordingly, the Register should decline the objectors' invitation to transform the triennial review into a medical or environmental policymaking exercise and leave those issues, to whatever extent they exist, for resolution by the FDA and EPA.

E. The triennial review is not an appropriate forum to address the contours of the CFAA.

As with the laws administered by the FDA and EPA, the Computer Fraud and Abuse Act (CFAA) is not aimed at preventing copyright infringement, and should not be incorporated by

[18] *See* LifeScience at 2; AdvaMed at 2; See GM at 6.

[19] *See* AdvaMed at 2; GM at 6.

[20] *E.g.*, Stephen Checkoway, et al. *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, 20th Usenix Security Symposium, 2011.

reference in the proposed exemption—notwithstanding BSA's arguments to the contrary.[21] The Register should decline to incorporate the CFAA by reference into the proposed exemption to avoid importing ambiguities and increasing the uncertainty a researcher faces when dealing with unsettled areas of the law like the CFAA. Doing so would contravene the basic goal of increasing certainty embodied of the proposed exemption.[22]

II. Security research is not copyright infringement.

As we noted in our initial comment, good faith security research does not constitute copyright infringement. [23] In many cases, the act of performing security research does not involve copying a protected work at all. In the few cases where copying a protected work is required, it falls within the well-established fair use exceptions to copyright protection. Because security research is not copyright infringement, Section 1201, a statute intended for the narrow purpose of protecting against copyright infringement, should not be used to prevent security researchers from engaging in this non-infringing activity.

A. Security research does not generally raise concerns over copyright infringement.

Most objectors do not seriously contend that good faith security research constitutes copyright infringement. Auto Alliance, Intellectual Property Owners Association (IPOA), and Medical Device Innovation, Safety, and Security Consortium (MDISS) all cite safety as the primary basis of their objections and do not dispute that good faith security research does not infringe on their copyrights or the copyrights of those they represent.[24]

LifeScience Alley and AdvaMed assert that copyright research may reveal trade secrets, which Section 1201 does not cover.[25] Trade secret protection generally does not encompass reverse engineering and any revelation of trade secrets that might result in the course of good faith security research would not constitute copyright infringement—or, in most cases, trade secret infringement.[26] Section 1201 applies only to TPMs that protect copyrighted works, so the hypothetical possibility that circumvention could result in the discovery of trade secrets is not a cognizable basis upon which the Register may deny the proposed exemption.[27]

Finally, BSA complains that the proposed exemption is not limited to activities that do not constitute copyright infringement.[28] However, the plain language of Section 1201(a)(1)(B) limits exemptions by its basic operation to non-infringing uses of works, since copyright owners retain

[21] 18 U.S.C § 1030; BSA at 5.

[22] Green Comment at 19-22.

[23] Green Comment at 11-17.

[24] *See* Auto Alliance at 1, IPOA at 2, MDISS at 1.

[25] *See* LifeScience Alley at 5; AdvaMed at 5.

[26] *See* Chicago Lock Co. v. Fanberg, 676 F.2d 400, 405 (9th Cir 1982).

[27] *See* Chamberlain Grp., Inc. v. Skylink Technologies, Inc., 381 F.3d 1178, 1197 (Fed. Cir. 2004); 17 U.S.C. § 1201.

[28] BSA at 2.

their rights under copyright law even in the case of an exemption to section 1201. Thus, we assume the proposed exemption should, by definition, only be applicable in cases where the proposed use is non-infringing.[29] Any invocation of the exemption for infringing copyright would fail. If the Register nevertheless would prefer to make this point explicit, we would not object to the inclusion of language in the exemption that makes clear the exemption is limited to research activities that do not infringe copyright law.

B. Previous exemptions establish that security research is a non-infringing use.

In previous iterations of this proceeding, the Copyright Office has acknowledged that good faith security research does not constitute copyright infringement and is thus eligible for exemptions to Section 1201. In 2006 the Register recommended an exemption for "good faith testing, investigating, or correcting such security flaws or vulnerabilities" within the class of sound recordings and audiovisual works.[30] Similarly, in 2010, the Register recommended an exemption "for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities" within the class of audiovisual works limited to video games.[31] The Register declared that "researchers in lawful possession of copies of games are engaged in non-infringing uses when they seek solely to research and investigate whether a video game, or the technological measure protecting it, creates security vulnerabilities or flaws".[32]

Both of these cases demonstrate the widespread understanding that good faith security research is a non-infringing use. This proposition remains true under the proposed exemption since the core use case, good faith security research, has not changed. All that differs from previous granted exemptions is the scope of the current exemption to encompass the wider range of software and computing devices that must be necessarily considered when performing security research today due to the diverse and rapidly changing computing landscape.

Indeed, Congress has implicitly recognized security research as a non-infringing use by codifying statutory support for reverse engineering, encryption research, and security testing in Section 1201(f), (g), and (j).[33] These exemptions would be meaningless if the underlying acts of reverse engineering, encryption research, and security testing were treated as copyright infringement; their inclusion indicates Congress's understanding of the common sense proposition that security research does not implicate legitimate concerns over infringement. Furthermore, the inclusion of such exemptions shows that Congress does not deem security research to pose a security threat or violation of related computer security laws. Unfortunately, as outlined in the Section III, *infra*, the statuary exemptions are inadequate to ensure the

[29] 17 U.S.C. § 1201(a)(1)(B).

[30] *Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies*, Final Rule, 71 Fed. Reg. 68,477 (Nov. 27 2006) ("2006 Recommendation of the Register of Copyrights").

[31] *See* 2010 Recommendation of the Register of Copyrights, 75 Fed. Reg. at 43,832.

[32] *Id.*

[33] 17 U.S.C. 1201(f), (g), (j)

unhindered and regular practice of security research—hence the need for the proposed exemption.

C. Security research is fair use.

As our initial comment argues, to whatever extent it might otherwise implicate concerns over copyright infringement, security research is a fair use. Only one commenter, GM, disagrees.[34] GM's arguments, however, are inconsistent with well-established case law and Copyright Office precedent.

First, the purpose and character of the intended uses of our proposed exemption weigh in favor of a fair use determination. As we explained in our initial comment, whether or not a work is transformative depends on, "whether the new work merely supersedes the objects of the original creation, or instead adds something new, with a further purpose or different character, altering the first with new expression, meaning or message."[35] GM argues that security research somehow is not transformative because the dissemination of sensitive information about how a car's ECU or TPMs operate increases the potential risk that individuals might access and modify their vehicle software in a manner that decreases security and safety. But, as discussed in Section I(D), *supra*, GM misconstrues the activities encompassed by the scope of our exemption. While we express no opinions as to the merits of the other automotive exemption proposals, tuning and modification for non-security purposes is not within the scope of our exemption. As our initial comment explains in detail, good faith security research is primarily aimed at archetypically transformative purposes, including research, criticism, commentary, and teaching.[36]

Second, the nature of the copyrighted work used in security research weighs in favor of a fair use determination. While GM argues that the copyrighted computer code used in automobiles is creative, there are significant practical rules and conventions that limit the creativity involved in such software.[37] To the extent such highly functional code is protectable, it is more analogous to a non-fictional work than a fictional one. Thus, the nature of the copyrighted work weights in favor of fair use.

Third, the amount and substantiality of copyrighted software used in security research weighs in favor of a fair use determination. GM argues even where a small portion of the work is copied, it will not be fair use if that portion contains the essence or essential part of the copyrighted work. However, security research by its very nature generally utilizes few or no copyrighted portions of a work at all. To the extent that researchers must duplicate or redistribute pieces of the original work, only the minimal amount of the work necessary for commentary is involved, plainly weighing the amount and substantiality in favor of fair use. Additionally, copying creative aspects of code in order to access key functional elements has been found non-infringing.[38]

[34] GM at 9-12.

[35] Green Comment at 15.

[36] Green Comment at 15-16.

[37] *See* Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 599 (9th Cir. 2000).

[38] *Id.*

Finally, the market for the copyrighted work related to security research weighs in favor of a fair use determination. GM argues that allowing security research on copyrighted works will affect the value of copyrighted works because if the public knows something is unsafe, they will not purchase it.[39] However, to whatever extent the value of copyrighted software might be decreased by revealing that it contains serious security vulnerabilities, that decrease in value is not due to copyright infringement, but is instead a direct result of criticism of and commentary on the software. As the Supreme Court has noted, "there is no protectable derivative market for criticism. . . . . [W]hile a scathing parody may destroy the market for the original work, its destruction stems from criticism, not usurpation by acting as a substitute."[40] Truthful criticism of security failures in a copyrighted work that harms the sales of the work—i.e., in this case, cars—is at the core of fair use and is strongly protected by the First Amendment. Just as consumers may choose not to see badly-reviewed movies, consumers may choose not to buy unsafe cars, and manufacturers who make unsafe cars should not be able to invoke Section 1201 to hide vulnerabilities from the public.

III. Existing statutory exemptions are inadequate to facilitate good faith security research.

Objectors suggest that the existing exemptions are adequate for the proposed research.[41] Although Congress included three exemptions in Section 1201—Section 1201(f) for reverse engineering, Section 1201(g) for encryption research, and Section 1201(j) for security research—the lack of clarity and breadth in the existing statutory framework, and the burdens imposed by such a framework, necessitate granting our exemption.[42] We are hopeful that in many instances, subsections (f), (g), and (j) will exempt security research activities. However, we are concerned for the reasons outlined in our initial comment that the existing exemptions do not provide sufficient clarity or breadth for many uses, a concern repeatedly recognized by the Copyright Office over the past seven years.[43]

A. The Register has routinely recommended exemptions to mitigate uncertainty about the scope of Section 1201's statutory exemptions.

During the 2006 rulemaking, the Librarian designated a class of works exempt from the prohibition on circumvention, when circumvention is accomplished "solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities."[44] This class specifically targeted the rootkit that had been shipped with certain Sony CDs.[45] The Register

[39] *See* GM at 17.

[40] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 592, 114 S. Ct. 1164, 1178, 127 L. Ed. 2d 500 (1994).

[41] *See* SIIA; BSA at 2;

[42] 17 U.S.C. §§ 1201(f), (g), and (j).

[43] *See* Green Comment at 19.

[44] 2006 Recommendation of the Register of Copyrights, 71 Fed. Reg. at 68,477.

[45] 2006 Final Rule at 68477.

reasoned that "it is not clear whether Section 1201(j) extends to such conduct" and that "in light of that uncertainty and the seriousness of the problem, the Register recommends that the Librarian designate a class of works" consisting of sound recordings etc., when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities.[46]

During the 2010 rulemaking, the Librarian granted an exemption for video games protected by access controls, when circumvention is done for the purpose of good faith testing for, investigating, or correcting security flaws or vulnerabilities.[47] The Register again concluded that it is unclear whether Section 1201(j) applies in cases where the person engaging in security testing is not seeking to gain access to, in the words of Section 1201(j), "a computer, computer system, or computer network."[48]

The 2006 and 2010 exemptions were granted because the Register found that Section 1201 chilled important security research, and found the existing exemptions to be sufficiently uncertain that it was necessary to grant a new exemption.[49] As described in our initial comment, Section 1201 is still chilling important security research and is still, as the Register stated, "a serious issue."[50] In addition to Prof. Green, researchers stifled by Section 1201 include individuals from Princeton, Rice, and many other students, teachers, and researchers.[51]

B. Section 1201's statutory exemptions are still inadequate today.

The exemptions granted in 2006 and 2010 underscore the ongoing need for exemptions that are not covered under the existing statute. However, some opposition comments state that the existing statutory framework of Section 1201 covers our proposed exemption.

BSA contends that "although the Register and the Librarian have at times granted exemptions that closely relate to activities that are already addressed by existing statutory exceptions to Section 1201's anti-circumvention prohibitions . . . , previous exemptions related to security testing have incorporated aspects of section 1201(j) to preserve the spirit of Congress' efforts to avoid exacerbating risks rather than reducing them."[52] Software & Information Industry Association (SIIA) similarly argues that the concerns raised by comments relating to this class were considered by Congress when it enacted the DMCA and that Congress carved out exemptions to the Section 1201 anti-circumvention prohibition for security testing (Section 1201 (j)), reverse engineering (Section 1201(f)), and encryption research (Section 1201(g)).

[46] *Id.*

[47] Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies, 75 Fed. Reg. 43,825 (July 27, 2010) (codified at 37 C.F.R. pt. 201) ("2010 Final Rule").

[48] 2010 Final Rule at 43832; 17 U.S.C. § 1201(j).

[49] 2006 Final Rule at 68477.

[50] Green Comment at 18; 2006 Final Rule.

[51] Green Comment at 18; *See* Security Researchers at 6-7; Stallman, et al. at 1.

[52] BSA at 2-3.

While "Section 1201(j) is evidence of Congress's general concern to permit circumvention under appropriate circumstances for purposes of security testing," the fact that exemptions closely related to 1201(j) have been granted in the past, shows that the limitations in the statutory exemptions should not limit the grant of a triennial exemption.[53] The limitations are merely reflective of the technical specifics that existed in 1998, and there is no indication that Congress intended the exemptions to fall behind changing technology.

IV. The Register should recommend an exemption that allows security research into vulnerabilities in copyrighted works and not just TPMs.

Both BSA and SIIA make arguments based on mistaken understandings of the scope of allowable exemptions. BSA argues that in contrast with the targeted security testing exemptions previously recognized by the Register, the proposed exemption relates not to vulnerabilities caused by access controls, but instead to all software products that might contain vulnerabilities and that happen to be protected by access controls.[54] In doing so, BSA invites the Copyright Office to read an unwritten and unprincipled limitation into Section 1201(a)(1)(C). This restriction would preclude any exemption that would allow circumventing TPMs to access other software with security vulnerabilities.

No such limitation exists in the statute. The 2006 exemption was granted for circumvention for the purpose of engaging in good faith testing, investigating, or correcting of security flaws or vulnerabilities—language taken directly from Section 1201(j)—and was only limited to vulnerabilities in access controls because the nature of the vulnerabilities at issue happened to be centered in the TPMs themselves, and not the underlying copyrighted works.[55] There is no evidence that the Register intended to limit future security research exemptions in the same way, nor would Section 1201 require doing so. Indeed, in 2010 the Register recommended an exemption both for video games and the measures that protect them, not just the protection measures alone.[56] Because the landscape of security vulnerabilities has changed to encompass both vulnerabilities in TPMs themselves and underlying copyrighted works, Section 1201 and sound public policy dictate that the Register recommend an exemption that encompasses both types of vulnerabilities.

V. Vulnerability disclosure standards are outside of the scope of the exemption process and the Copyright Office should not endorse a specific standard in granting the proposed exemption.

Several other petitioners, as well as a number of objectors, have raised the issue of the responsible and coordinated disclosure of identified vulnerabilities.[57] Such practices refer to the manner in which a researcher notifies the effected parties, the responsible parties, and the public

[53] 2010 Final Rule 75 Fed. Reg. at 43,833.

[54] BSA at 3.

[55] 2006 Final Rule at 68477.

[56] 2010 Final Rule at 43832.

[57] *See, e.g.*, Long Comment of Security Researchers at 1; BSA at 4.

at large of a security-related issue they discover.[58] Disclosure practices vary widely across the industry, but generally seek to ensure that both manufactures and the public are kept appraised of vulnerabilities in the software they make, distribute, or use so that they make take mitigating actions to avoid and correct such flaws. Proper disclosure practices balance the importance of notifying a responsible party capable of addressing a security flaw, so that they may fix such a flaw before it becomes widely known, against the importance of informing the effected parties and general public of flaws in the software and devices they use—flaws which such parties may wish to mitigate by modifying or ceasing their use of such software or devices.

The means by which researchers disclose, and vendors fix, security vulnerabilities is a complex, multi-faceted issue with substantial implications for cybersecurity and many other areas of national policy that have little to do with copyright law. It is beyond the scope of this proceeding to consider, much less address, the serious ramifications of disclosure policy, and we urge the Copyright Office to avoid conditioning liability under Section 1201 on adherence to particular disclosure standards. We agree with the BSA's comment that "the endorsement of specific security-related standards is far from the Copyright Office's mission and expertise and this proceeding is not designed for a full debate on such topics."[59] Such standards are difficult to calibrate, may not adequately anticipate all situations, and are ineffective in preventing exploits by bad actors. Furthermore, good faith security researchers already follow a range of similar disclosure best-practices when disseminating the results of their work.

A. Coordinated disclosure practices are complex and varied, and imposing an inflexible disclosure standard would not serve the public interest.

In general, good faith security researchers make every attempt to disclose any found vulnerability to a party capable of fixing it prior to the public disclosure of the vulnerability. Such advanced disclosure practices—for example, those proposed by Google[60]—help ensure that manufactures and vendors have an opportunity to fix security flaws before they become public. Good faith security researchers already follow best-practice guidelines for responsible and coordinated disclosure of the flaws they find.[61] For example, Prof. Green was instrumental in coordinating the disclosure of the FREAK SSL vulnerability, even going so far as to personally contact critical end-users such as the Federal Bureau of Investigations (FBI) to inform them of the flaw before its public disclosure.[62] Indeed, not following such practices would likely preempt such

[58] Microsoft, *Coordinated Vulnerability Disclosure*, Security TechCenter, 2015.

[59] BSA at 4.

[60] Google, *Rebooting Responsible Disclosure: a focus on protecting end users*, http://googleonlinesecurity.blogspot.com/2010/07/rebooting-responsible-disclosure-focus.html

[61] Danny Yadron. *After Heartbleed Bug, a Race to Plug Internet Hole*, The Wall Street Journal, April 9, 2014; Ben Grubb, *Heartbleed disclosure timeline: who knew what and when*, The Sydney Morning Herald. April 15, 2014.

[62] *Tracking the FREAK Attack*. https://freakattack.com/ (last visited May 1, 2015); Matthew Green. *Attack of the week: FREAK (or 'factoring the NSA for fun and profit')*, A Few Thoughts on Cryptographic Engineering, March 3, 2015.

research from being qualified as having been undertaken in "good faith" under the meaning of the exemption.

However, advanced disclosure is not always possible or desirable. In some cases, concurrent disclosure is preferable to advanced disclosure. For example, security researchers often discover security flaws that are already known to various bad actors, and that are thus already being exploited to harm users. In such cases, notifying the manufacturer prior to notifying the targeted user or the general public has little benefit, since bad actors are already aware of the flaw and are actively using it to attack users– as is the case with many Internet viruses and worms.[63] Notifying the end-users and the public concurrently with the manufacturer allows users to take mitigating actions such as discontinued use of a service or device until the manufacture has an opportunity to fix the flaw.

Similarly, there are cases where notifying a manufacturer of a flaw is simply not possible. For example, in a case where a manufacturer has gone out of business and is no longer providing support for a product. In such cases, there is no active manufacturer or other "responsible party" to notify, and instead the public at large must be informed of the flaw so that they may make an informed decision about whether or not they wish to continue using a vulnerable and unsupported product. Such cases may also arise in situations where manufacturers have stated that they are unwilling or unable to fix security vulnerabilities in their products—for example, in the case of TrueCrypt, where the developers have publicly stated that they are no longer supporting their disk encryption product and that users should only continue to use it at their own risk.[64] Again, in such situations, notifying the public of vulnerabilities so that they may make informed decisions about the use of specific products outweighs the usefulness of providing notification to a manufacture who has no interest or ability to fix the discovered flaws.

There are also complex cases such as the Heartbleed vulnerability, where the responsible party is not a traditional manufacturer at all, but a group of volunteer developers whose code is integrated into thousands of unrelated user-facing products.[65] In these cases, notifying the "manufacturers" of every affected product using the vulnerable code is effectively impossible, and a public disclosure is the best method to ensure all affected parties, manufacturers, and end-users alike, are aware of the flaw and can take mitigating action.

Moreover, good faith security researchers' responsible and coordinated disclosure of the flaws they find is rarely, if ever, the only, or even the primary, method by which bad actors might become aware of such flaws. There is already a well-established and heavily trafficked market for undisclosed security vulnerabilities through which bad actors may purchase "secret" flaws that they may then use to exploit software and devices in a manner the manufacturer is completely

[63] Cencini, Andrew, Kevin Yu, and Tony Chan, *Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure* (2005).

[64] Brain Krebs, *True Goodbye: Using TrueCrypt Is Not Secure*, Krebs on Security, May 29, 2014.

[65] The Heartbleed Bug, CVE-2014-0160 (2014).

unaware of.[66] Indeed, it is likely that many of the flaws discovered by security researchers are already available to the highest bidder on such black markets.

Thus, in many instances, any public disclosure of a vulnerability is preferable to no disclosure of the vulnerability, since it takes the vulnerability off the market and ensures that both the public and the manufacturers can account for its existence and react accordingly.[67] Indeed, many companies are so concerned about the threat posed by the underground black market for security vulnerabilities that they run "bug bounty" programs paying members of the general public 10s of thousands of dollars for each vulnerability they find and disclose.[68] Good faith security researchers merely seek to find the vulnerabilities bad actors often already know about and make the responsible parties and the general public aware so that something may be done.

Thus, the proper manner and method of responsibly disclosing a security vulnerability is a complex and situation-specific task not well suited for codification in a Section 1201 exemption. Good faith security researchers are already very familiar with the complexities and best practices involved in such disclosures, and have demonstrated their ability to undertake such disclosures in an appropriate manner well suited to both the public interest and the interests of the manufacturer. The security research community is continually seeking and revising the ideal disclosure practices, and no single consensus is appropriate for inclusion in an exemption standard at this time.

Furthermore, the DMCA is intended to protect against copyright infringement, not to regulate the best practices of good faith researchers. The Register need not, and should not, interfere with such internal regulation by imposing inflexible disclosure rules as part of the proposed exemption. Indeed, the real risk to user security is not the public disclosure of discovered flaws, but instead lack of research into such flaws caused by the chilling effect Section 1201 has on security researchers. Bad actors already know about many security flaws and are unconcerned with liability under Section 1201. It is important that the Register recommend the proposed exemption to ensure that good faith security researchers can also discover and responsibly disclose such flaws without fear of infringing Section 1201.

B. If the exemption must include disclosure standard, it should apply only if the researcher actually finds a vulnerability and discloses it.

We do not believe the inclusion of a disclosure standard in the proposed exemption is necessary or appropriate. Nevertheless, if the Register chooses to recommend one, it is critical that any such standard should only apply in cases where (i) the researcher actually finds a security vulnerability in the course of pursuing their research and (ii) the researcher wishes to disclosure

[66] HackerOne, *The Wolves of Vuln Street—The First System Dynamics Model of the 0day Market*". April 14, 2015; Bruce Schneier. *The Vulnerabilities Market and the Future of Security*, Forbes, May 30, 2012.

[67] Dan Geer, *Cybersecurity as Realpolitik*, Black Hat Conference, Las Vegas, 2014, at https://www.blackhat.com/us-14/video/cybersecurity-as-realpolitik.html.

[68] Google, *Google Vulnerability Reward Program (VRP) Rules*, https://www.google.com/about/appsecurity/reward-program/; Microsoft, *Project Spartan Bug Bounty Program Terms*, https://technet.microsoft.com/en-us/dn972323.aspx.

such a vulnerability to the manufacturers and/or the general public. Often, security researchers do not know if they will discover a vulnerability when they embark on security research, and tying eligibility for the proposed exemption to disclosure without exempting cases where researchers do not find anything worth disclosing will impose an impossible barrier to starting research. Any standard must also allow researchers the option to keep discovered exemptions to themselves to accommodate situations where they do not feel there is any safe or ethical way to disclose such a vulnerability.

C. Any disclosure standard must be sufficiently flexible, consistent with the First Amendment, and subject to public scrutiny.

Any discourse standard must be highly flexible to avoid harming the public in cases of an unreachable or uncooperative manufacturers and to prevent unduly binding researchers in cases where advanced disclosure is either undesirable or impracticable, as discussed in Section V.A. *supra*. Furthermore, any disclosure standard must withstand First Amendment scrutiny and be aligned with the safety and interest of the general public, even when that alignment may be at the expense of the reputation or business interests of the manufacturers or parties whose code is shown to contain vulnerabilities.

Contrary to the exemption standard proposed by Security Researchers, we do not believe it would be appropriate to include closed ISO standards the proposed exemption text because those standards are proprietary and not accessible to the general public.[69] It is not possible for us or the public to comment on the contents of closed standards or to endorse their inclusion in an exemption until they are made publically available or entered into the public record. Specifically incorporating non-public standards in an exemption would not meet the spirit or the letter of the Administrative Procedure Act's public notice and comment requirements or serve the stated goal of this exemption of providing sufficient clarity to academic researchers.[70] If such standards are made publicly available in time to incorporate them into the record in this proceeding, we would gladly evaluate them and stand ready to provide further comment.

* * *

For the foregoing reasons, the Register should recommend the proposed exemption.

Respectfully submitted,

/s/

Chelsea E. Brooks
Joseph N. de Raismes
Andy J. Sayler

Prof. Blake E. Reid

Counsel to Prof. Green

[69] *See* Security Researchers at 1; ISO/IEC 29147:2014 -- Information technology -- Security techniques -- Vulnerability disclosure; ISO/IEC 30111:2013 --
Information technology -- Security techniques -- Vulnerability handling processes.

[70] 5 U.S.C. § 553(b).