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

Long-Form Comment:
Proposed Class 25: Security Research
of
Dr. Matthew D. Green

1. *Commenter Information*

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

Matthew D. 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 user privacy. The student attorneys at the Samuelson-Glushko Technology & Policy Law Clinic (TLPC) at Colorado Law advocate for the public interest in important public policy and legal matters with technological dimensions.

Table of Contents

2. *Proposed Class Addressed:* Class 25: Software—Security Research

The Office's *Notice of Proposed Rulemaking* (*NPRM*) proposes this language for Class 25:

> This proposed class would allow researchers to circumvent access controls in relation to computer programs, databases, and devices for purposes of good-faith testing, identifying, disclosing, and fixing of malfunctions, security flaws, or vulnerabilities.[1]

After reviewing Proposed Class 22: Vehicle Software—Security and Safety Research, Proposed Class 27: Software—Networked Medical Devices, and the related Class 25 submission by Steven M. Bellovin, Matt Blaze, Edward W. Felten, J. Alex Halderman, and Nadia Heninger, we offer the following clarification to our proposed class.

The proposed exemption, as worded in the *NPRM*, limits the subject matter of the research to literary works alone, and therefore fails to address some of the key ambiguities that chill good faith security research. Importantly, good faith security research may target technological protection measures ("TPMs") protecting copyrighted works ancillary to the target of the research itself and thereby may not be covered under an exemption limited strictly to literary works. So that our exemption may encompass the need to circumvent a broad range of TPMs in the furtherance of good faith security research, we propose this modified language:

> Literary works, including computer programs, databases, and documentation, protected by technological protection measures that control access to the work, for the purpose of finding, fixing, and disclosing security vulnerabilities, flaws, or malfunctions, commenting on or criticizing such vulnerabilities, flaws, or malfunctions, or engaging in scholarship and teaching about such vulnerabilities, flaws, or malfunctions, including where the technological protection measures control access to other works, such as graphic works, audiovisual works, and sound recordings, when the research cannot be performed without accessing the other works.

This revised language serves to further Congressional intent by promoting good faith security research in the spirit of Section 1201's existing security-related exemptions while addressing the problematic ambiguities and shortcomings of those exemptions.

3. *Brief Overview of Proposed Exemption*

Software is pervasive in modern technologies. It is the basis of the personal computers we use every day, it underlies the World Wide Web on which we depend, and it controls our vehicles, home appliances, and life-saving medical devices. The security of modern software and the devices that execute this software is thus of paramount importance for both the security of our

---

[1] *Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies*, Notice of Proposed Rulemaking, 79 Fed. Reg. 73,856 (Dec. 12, 2014) (to be codified at 37 C.F.R. pt. 201) ("*NPRM*").

nation and the security of our lives.[2] Yet 2014 was the worst year ever with respect to the safety and security of our software and computing devices, with an increase of over 90% in cyber-attacks and an increase of over 60% in cyber-breaches relative to the previous year.[3]

To rectify these failings, it is critical that security researchers are able to work without fear of substantial legal liability to find and fix vulnerabilities in the software and devices on which we rely. In order to do this vital work, security researchers must occasionally bypass various measures designed to control access to software and devices.

We seek an exemption that permits TPM circumvention for the purpose of good faith security research related to computer programs, databases, documentation, and related works. While Section 1201 contains built-in exemptions for reverse engineering, encryption research, and security research, these exemptions do not adequately delineate what security researchers can and cannot do.[4] At a time when such research is more vital than ever before, these ambiguities raise the burden, the cost, and the perceived risk of performing security research.[5] They chill research and put the safety of individuals and the security of our nation at risk.

This exemption builds on previous exemptions that recognized the importance of allowing TPM circumvention for security research. The Copyright Office granted a similar exemption for good faith security research into sound recordings on compact discs during the 2006 proceeding and video games accessible on personal computers during the 2010 proceeding.[6]

Our requested exemption builds on those previous exemptions, as well as the exemptions codified in the Digital Millennium Copyright Act (DMCA), and seeks to unify them under one exemption to remove the ambiguity and other shortcomings that chill security research.[7] We seek an exemption to make clear that circumvention of TPMs on software and software-controlled

---

[2] Julie Hirschfeld Davis, *Obama Calls for New Laws to Bolder Cybersecurity*, New York Times, Jan. 13, 2015, *available at* http://www.nytimes.com/2015/01/14/us/obama-to-announce-new-cyberattack-protections.html?_r=0.

[3] Symantec Corporation, *Internet Security Threat Report*, 19 (2014), *available at* https://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19_21291018.en-us.pdf.

[4] *See* discussion *infra*, Part 6(B).

[5] E.g. By requiring researchers to spend and pay for "many hours with lawyers examining the implications of the DMCA." David Wagner, Email, *FC: Princeton student is latest to say he could be sued under DMCA* (Nov 25, 2002), *available at* http://lists.jammed.com/politech/2002/11/0090.html.

[6] *Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies*, 71 Fed. Reg. 68,472 (Nov. 27, 2006) (codified at 37 C.F.R. pt. 201) ("*2006 Final Rule*"); *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*").

[7] 17 U.S.C. § 1201(f), (g), (j); *Petition of a Coalition of Medical Device Researchers for Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, *NPRM* at 73,871-72; *Exemption to Permit Circumvention of TPMs on Software that is Embedded in Vehicles*, *NPRM* at 73,868-69.

systems is permitted for the full range of good faith security research. Such an exemption will ease the burden of performing this class of research, ensuring that researchers are free to continue their work safeguarding and securing the range of software systems upon which we rely every day.

4. *Technological Protection Measures and Methods of Circumvention*

A variety of TPMs are used to control access to our proposed class of works. To bypass these measures, researchers need the ability to exercise a variety of circumvention techniques. While not every measure will necessarily qualify as a TPM under the meaning of Section 1201(a)(3)(B) depending on the specifics of its implementation, we outline several classes of common protection measures, including measures controlling installation, execution, or use, measures controlling reading or inspection, and measures controlling modification, as well as general methods used to circumvent those measures.

A. Measures for Controlling Installation, Execution, or Use

One class of measures is designed to control whether or not a user can install, execute, or otherwise use software or a device and the manner in which they may do so. In order to undertake good faith security research, it is essential to be able to install, execute and run a variety of legitimately obtained software or devices for a range of fair use purposes. Researchers must be allowed to circumvent protection measures aimed at controlling these capabilities, which include keys, shared secrets, usernames, passwords, external authentication or tethering systems, dongles, installation media, hardware fingerprinting, and license prompts or click-through dialogs.

i. Keys, Shared Secrets, Usernames, and Passwords

The most common measures in this class include keys, shared secrets, and username-password pairs. These measures all operate by requiring a user to provide some form of unique text, such as a software key, prior to installing, executing, or using software or a device.[8]

Internally, software verifies these values against a set of valid values in order to determine whether or not a user should be granted the ability to execute the software or use the device. In some instances, the user provided values may be compared against locally stored values, either directly or after some form of algorithmic transformation, to confirm validity. In other cases the values may simply be checked for specific internal patterns or relationships as a self-certifying indication of validity.

Researchers may need to bypass such measures if they lack access to the original key or secret needed to unlock the software, or if they wish to test how the software will behave in the absence of such a key or secret. Bypassing such mechanisms is generally done either by manipulating the software to avoid undertaking such checks in the first place, or by forcing the software to believe a legitimate value has already been provided.

---

[8] Gleb Naumovich & Nasir Memon, *Preventing Piracy, Reverse Engineering, and Tampering*, IEEE Computer 36 (2003), *available at* http://www.rcisp.net/sites/default/files/3.pdf.

ii. External Authentication Systems and Tethering

Some systems rely on external authentication, monitoring, or tethering infrastructure to control a user's ability to install, execute, or use software or a device.[9] Such systems require end-user software and devices to "phone home" to a centrally controlled service in order to verify whether a specific instance of the software or device has been approved for use. These systems are often similar to those discussed above in that they require the user to provide some form of unique information to the system in order to use it. Unlike the measures above, these systems then validate the user's input via communication with an external service instead of locally.

Researchers may need to bypass such measures in cases where the required external service is no longer operating, or when the operator of the external service is not willing to cooperate with good faith research. Bypassing such checks might also be necessary if researchers are working in restricted environments like classified or sensitive research labs where external Internet access is not available.[10] External authentication or monitoring checks can generally be bypassed by methods such as running a local service that mimics the behavior of the official external service, tricking the software into believing it has received the authorization it is expecting. Alternatively, such measures might be bypassed by manipulating the software or device to simply skip performing such checks in the first place.

iii. Dongles, Installation Media, and Hardware Fingerprinting

Another set of measures designed to control a user's ability to install, execute, or use software or a device requires the presence of a physical item when the software or device is in use.[11] The required physical items range from "dongles"—*i.e.*, special hardware devices provided by the software publisher—to copies of the installation media—*e.g.*, CDs or DVDs.[12] The software checks for the presence of the associated item when it runs, and will refuse to run if the item is not present. Similarly, some software systems employ fingerprinting measures to ensure that software will only run on a specific piece or set of hardware. These systems "fingerprint" the hardware on which the software is first installed and will disable the software anytime they detect a change in the underlying hardware.

In cases where the required verification item is no longer functioning or available it may be necessary to bypass physical device checks or fingerprints. It may also be necessary to bypass such mechanisms in order to study how the software behaves in the absence of these measures. Fingerprinting may need to be bypassed in order to support legitimate modifications to the

---

[9] Karen Merceds Goertzel, *Protecting Software Intellectual Property Against Counterfeiting and Piracy*, CrossTalk: The Journal of Defense Software Engineering 24 (2011).

[10] Department of Defense Manual, *DoD Information Security Program: Marking of Classified Information*, 5200.01-V2, (Feb. 24, 2012) (Updated Mar. 19, 2013), *available at* http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf; *NPRM* at 73870.

[11] Naumovich, *supra*, at 66.

[12] *See Exemption to Prohibited Circumvention of Copyright Protection Systems for Access Control Technologies*, Final Rule, 68 Fed Reg. 62,011, 62,013 (Oct. 31, 2003) (describing the long-standing "dongle" exemption, granted in the 2003, 2006, and 2010 proceedings).

original hardware, including the repair or replacement of defective parts, or the upgrade of outdated or obsolete parts. Bypassing such checks is often accomplished by modifying the software to skip such checks or by emulating or otherwise simulating the presence of the required physical item. In the case of hardware fingerprinting, bypass may also be accomplished by modifying the originally recorded fingerprint to match that of the updated hardware.

iv. License and Dialog Click-Through Prompts

Some parties have asserted that even a simple click-through license or user-agreement prompt that must be approved before a given piece of software or a specific device will run qualifies as a protection measure under Section 1201.[13] Such mechanisms operate by recording whether or not the user has responded to a specific prompt by clicking a button to indicate their approval. When no such response has been recorded, such systems refuse to operate. We do not believe that such simple measures rise to the definition of a TPM under Section 1201(a)(3)(B), but this has not stopped companies from making legal threats against their circumvention.[14]

It is often necessary for researchers to bypass such prompts in order to perform research into the underlying software, either because the original license is no longer available for review and approval, or because mandatory acceptance of such a license would undermine the good faith security research being performed. Such bypasses are generally performed by modifying the software to avoid presenting the license prompt in the first place, or by manipulating the software to falsely believe that a prompt has already been approved.

B. Measures for Controlling Reading or Inspection

A second class of measures is designed to control whether or not a user can read, inspect, or study software or a device. Being able to read, inspect, and study software is a critical component of finding and fixing security vulnerabilities. Thus, good faith security researchers must be allowed to circumvent mechanisms designed to prevent users from accessing such programs or devices.

i. Obfuscation

One such measure for preventing users from studying software is known as obfuscation.[15] Obfuscation is a process that aims to modify software in ways that make it difficult for humans to read and interpret while still persevering a computer's ability execute the program. Obfuscation is common at both the source code level as well as at the machine code level.

Good faith security researchers must be able to de-obfuscate and de-compile code in order to study it for the purpose of finding and fixing security vulnerabilities. Because obfuscated programs must still be executable by a standard computer, obfuscation has limited effectiveness and can often be circumvented using tools designed to reverse the obfuscation and/or

---

[13] Naumovich, *supra*, at 65-66.

[14] Robin "Roblimo" Miller, *Microsoft Asks Slashdot To Remove Readers' Posts*, Slashdot (May 11, 2000), *available at* http://slashdot.org/story/00/05/11/0153247/microsoft-asks-slashdot-to-remove-readers-posts.

[15] Naumovich, *supra*, at 67-68.

compilation process. Such tools convert the code back into a form that is more easily interpreted and studied by a human.

ii. Execute-Only Memory and Trusted Platform Modules

Another mechanism for subverting an end-user's ability to read or study software that they have acquired is the use of hardware-backed security measures such as execute-only memory or trusted platform modules.[16] Such systems place hardware-level restrictions on the user's ability to access and read software stored in a computer's memory. Execute-only memory operates by storing a computer program in a special segment of memory that the processor can access, but that the end-user cannot. Thus, programs stored in such memory may be executed, but not examined. Similarly, trusted platform modules store data in a manner where it can be written or updated but not read by the user. Such systems are often designed to perform cryptographic operations on behalf of the user.

Such mechanisms must be bypassed in order for good faith security researchers to study the underlying software. These mechanisms may be bypassed by exploiting flaws in the design or implementation of the hardware—*e.g.*, by monitoring side channels. Such flaws may expose otherwise protected memory regions, allowing researchers to access and analyze the software they contain. Alternatively, it may be possible to remove the backing hardware security measure altogether, providing access to the memory, and thus software, it was designed to protect.

iii. Encryption

In addition to obfuscation and hardware-backed measures, the user's ability to read and study software can also be subverted through the use of encryption. Encryption uses mathematical operations to transform software into a form that only individuals possessing a specific encryption "key" are able to read. Such encryption is generally of the traditional runtime variety, which protects code up until the moment it is executed. Alternatively, next-generation homomorphic encryption systems might be used to protect code before, during, and after execution.[17] Such encryption subverts good faith security research by making it difficult to read and study the code.

Allowing researchers to subvert encryption is a necessary step to ensure they can analyze and study software for the purpose of finding and fixing security vulnerabilities. Bypassing encryption can be done via several means. Traditional runtime encryption must be decrypted to be executed, and can often be captured in its non-encrypted form during that process. Homomorphic encryption might be susceptible to various side-channel subversions. All forms of encryption may be susceptible to flaws in the underlying design or vulnerabilities in the specific

---

[16] ARM, 2.22: Building applications for execute-only memory, Compiler Software Development Guide, Version 5.05 DUI0471K (2014); ISO/IEC 11889, Information technology - Trusted Platform Module (2009).

[17] Scut & Grugq, *Armouring the ELF: Binary encryption on the UNIX platform*, Phrack 11.58.5 (Dec. 28, 2001); Michael Brenner, et al., *Secret program execution in the cloud applying homomorphic encryption*, Proceedings of the 5th IEEE International Conference on Digital Ecosystems and Technologies Conference (DEST) (2011).

implementations. Such flaws or vulnerabilities may be exploited to decrypt encrypted software. Furthermore, it may be possible to recover the encryption keys associated with a piece of encrypted code, and these keys could then be used to decrypt and read the code.

C. Measures for Controlling Modification

A third class of protection measures aims to control whether or not users can modify the underlying software or device to change the manner in which it operates. Whether it be in support of the previously discussed circumventions, or as the primary goal of their research, security researchers are often required to modify software or devices. The ability to modify obtained software is a key component of effective security research. Therefore, our proposed exemption must be granted to allow good faith security researchers to make such modifications.

i. Hashes, Checksums, and Digital Signatures

One class of "tamper-proofing" measures includes static mechanisms such as one-way hash functions, checksums, or digital signatures.[18] These mechanisms operate by computing a reproducible and verifiable value associated with a copy of the software or device they protect. Any modification to the software or device will cause a change in this value. This value is re-computed and verified each time the software or device is used, disabling the software or device when verification fails due to a modification.

Hash functions, checksums, signatures, and other static methods can often be bypassed by simply manipulating the value the software is checking to match the "correct" value after modifying the software. In cases where this is not possible, it may also be possible to bypass these measures by manipulating the software to avoid verifying them in the first place. Alternatively, these mechanism might be bypassed by exploiting a vulnerability in the underlying hash function, checksum, or signature algorithm to generate a collision: a set of modifications to the code that generate the same hash, checksum, or signature value as the original unmodified code.

ii. Runtime Guards and Assertion Checks

In addition to static methods, there are a number of runtime mechanisms that attempt to prevent the modification of software or a device. Guards and assertion checks are examples of measures that perform runtime tamper-proofing.[19] Guards operate by employing a network of checks that work together to ensure the running program does not deviate from a set of expected behaviors. Assertion checks verify specific program behaviors or outcomes at certain points in time. Both mechanisms will generally abort the execution of the program if a deviation from the standard behaviors is detected.

Runtime checks like guards or assertion checks can be bypassed by removing them from the software all together or by feeding them false information in order to trick them into believing the software is operating as originally designed.

---

[18] Naumovich, *supra*, at 66.

[19] *Id.* at 66.

D. Measures for Tracking

A final class of protections simply aim to track software or a device, track the manner in which a user uses or modified software or a device, and/or report this data to external parties. While these techniques do not directly control or protect access to software or a device, they do serve to report the user's activities to an external party. There are a number of situations where security researchers would need to circumvent such mechanisms for the purpose of maintaining the confidentiality of their research or as part of an investigation into the security of the tracking mechanism itself. The ability to subvert tracking or reporting measures on legitimately obtained software for the purpose of performing good faith security research should be protected in our exemption.

i. Watermarks

Some software systems employ watermarking techniques to make it easier to track and trace the software and its usage.[20] Watermarks operate by marking software or a device with a unique code that allows it to be traced back to its point of origin. Watermarks are designed to be read off any copy of the software or device to identify the source of that particular copy.

Bypassing watermarks can be accomplished via various means. It is often possible to simply remove the watermark from the associated software or device altogether. In other cases, it may be possible to modify the watermark to make it unreadable. It may also be possible to spoof a watermark to make it appear a piece of software has a watermarked origin different from its true origin.

ii. External Monitoring

Some systems may employ measures to periodically contact an external server for the purpose of reporting on their location, usage, or other metric. Such measures generally operate by "phoning home" to their manufactures or other third parties and reporting on a range of data they have collected about the manner in which the software or device has been used.

External monitoring can often be circumvented by blocking outgoing communications from a piece of software to the outside world using a firewall, air gap, or similar network control mechanism. It may also be possible to modify the software or device to avoid attempting contact with external services in the first place.

E. Ancillary Measures

While our proposed exemption primarily involves circumventing TPMs that protect software or devices, it may occasionally be necessary to circumvent TPMs protecting other forms of works in the process of researching the security vulnerabilities of software or devices. The purpose of such ancillary circumventions is not to gain access to the additional protected works, but is instead an unavoidable consequence of, or requirement to, finding and fixing security vulnerabilities. Examples of such ancillary measures may include rootkit-level protection on CDs or related sound recording media, or cryptographic protections on eBooks, software manuals, DVDs, or other media accessed via software-controlled devices. The Copyright Office has

[20] *Id.* at 68-69.

granted such exemptions for bypassing TPMs on such works in the past for the purpose of good faith security research.[21]

It is important that security researchers be able to find and fix security vulnerabilities in any software or device, even when they must circumvent both TPMs designed to protect the software or device itself (the primary class of works) as well as TPMs designed to protect additional works accessed via software or a device (the ancillary class of works). We believe all forms of software-based TPM circumvention should be allowed for the purpose of good faith security research under the exemption we seek, regardless of the form of underlying work they were deigned to protect.

5. *Noninfringing Use:* Security Research

Security researchers need the ability to circumvent access controls in order to conduct good faith security research. Good security research includes a variety of non-infringing activities that either do not constitute copyright infringement or are paradigmatic fair uses.

A. The Holistic Process of Engaging in Security Research

Each of our intended uses is consistent with paradigmatic fair uses of copyrighted works. In particular, the uses encompassed in security research include:

i) Researching and discovering security flaws and vulnerabilities;
ii) Alerting consumers and notifying companies of security flaws and vulnerabilities;
iii) Providing students with valuable learning opportunities in which they have the opportunity to gain hands-on experience by working on a real system;
iv) Contributing to the academic publications and discussions of software and device security; and
v) Applying research discoveries to fix vulnerabilities or build new, more secure software and devices.

Each of these uses is a part of the overarching, holistic process of engaging in "security research." The holistic nature of these uses is exemplified in Prof. Green's proposed research plan attached under "Documentary Evidence" in Section 8.

i. Researching and discovering security flaws

First, security researchers must research and discover security flaws. The research and discovery process involves performing a systematic investigation into the extent to which a software or device is able to operate as intended, is secure from attack by malicious actors, and is capable of protecting the privacy and security of its users.

Gartner researchers estimate 26 billion devices will be connected to the Internet by 2020; ABI Research estimates 30 billion, and Cisco anticipates 50 billion devices.[22] Unfortunately, the software and devices connected to the Internet are increasingly vulnerable to security flaws.[23]

---

[21] *2006 Final Rule*, 71 Fed. Reg. at 68,477.

[22] Gartner *Gartner Says the Internet of Things Will Transform the Data Center* (Mar 18 2014), http://www.gartner.com/newsroom/id/2684915; Karen Tillman, *How Many Internet Connections are in the World? Right. Now.*, Cisco Blog (July 29, 2015) http://blogs.cisco.com/news/cisco-
(continued…)

One example involves personal video recorders, game consoles, and other home appliances that are networked to one another and the Internet.[24] Flaws in the software powering these devices may result in serious security problems such as permitting a malicious user to eavesdrop on a home surveillance system and view what that system has recorded.

ii. Alerting customers and notifying companies of security flaws and vulnerabilities

Once a good faith researcher discovers a security flaw in a piece of software or a device, the researcher will generally bring the issue to the attention of the manufacturer to allow them to repair the flaw. Once the manufacturer has had an opportunity to address the issue, the researchers will generally disclose the problem to the public, allowing users to take the necessary actions to remain secure in light of the discovered vulnerability. Security researchers who document and responsibly disclose security flaws and vulnerabilities in a software or device engage in criticism, commentary, and news reporting by alerting consumers and notifying companies of actual or potential security problems.

As an example of the importance of such disclosure, Professor Alex Halderman noted in his 2010 Comment in Support of Proposed Exemptions 8A and 8B that "evidence of significant vulnerabilities would be a valuable addition to the growing research literature."[25] Under our proposed exemption, security researchers would comply with industry and community standard disclosure practices in notifying companies of security flaws, and vulnerabilities. Such practices might include the coordinated disclosure mechanisms discussed in ISO 29147 and ISO 30111, as well as industry-standard mechanisms such as Google's 90-day disclosure policy.[26]

iii. Providing students with valuable learning opportunities to gain hands-on experience by working on a real system

In addition to discovery and disclosure, the proposed exemption would make it possible for students studying security research to actively engage with these access controls, instead of merely engaging with access control theory. In his proposed security research plan, Professor Halderman explained the importance of providing students with valuable learning opportunities to gain

---

connections-counter/; ABI, *More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020* (May 9, 2013), https://www.abiresearch.com/press/more-than-30-billion-devices-will-wirelessly-conne.

[23] Katie Notopoulos, *Somebody's watching: how a simple exploit lets strangers tap into private security cameras* (Feb. 3, 2012) http://www.theverge.com/2012/2/3/2767453/trendnet-ip-camera-exploit-4chan.

[24] Naumovich, *supra* at 65.

[25] Alex Halderman, *Research Plan: Side-Effects of the SecuRom DRM System*, *available at* http://www.copyright.gov/1201/2008/responses/glushko-samuelson-30.pdf.

[26] ISO/IEC 29147:2014: Information technology — Security Techniques — Vulnerability Disclosure; ISO/IEC 30111:2013: Information Technology — Security Techniques — Vulnerability Handling Processes; Peter Bright, *When Google squares off with Microsoft on bug disclosure, only users lose*, Ars Technica, Jan. 12, 2015.

hands-on experience by working on a real system, noting that "security research studies how computers are attacked in order to devise new ways to defend them. As I tell the students in my security class, the only way we can hope to build systems that won't fail under attack is by understanding how our adversaries think and learning how they operate."[27]

Many prominent computer science departments hold security research classes, including Carnegie Mellon University, Cornell University, University of California, Berkeley, University of Colorado, University of Texas, Purdue University, and the University of Southern California.[28] The well-established benefits of hands on learning apply to security researchers just as they do with a variety of other professions, and would be available to security researchers if our exemption were granted.[29]

iv. Contributing to the academic publications and discussions of software and device security

The exemption would also enrich the analysis of security vulnerabilities and flaws through exchanges of, and presentations on, ideas and research projects regarding program and software security. Contributing to the academic publications and discussions of software and device security would mean allowing security researchers to publish their findings and contribute to the widespread ecosystem of journals, conferences, and discussions in this space.

Security research is a vibrant and growing field with many venues sponsored by leading professional and technical organizations. Top publication venues in the realm of computer security, privacy, and cryptography research include the Journal of ACM Transactions on Information and System Security, the ACM Conference on Computer and Communication Security, the ACM Symposium on Access Control Models and Technologies, the USENIX Security Symposium, the USENIX Network and Distributed Security Symposium, the USENIX Workshop on Offense Technologies, the Privacy Enhancing Technologies Symposium, the Journal of Cryptology, and the Journal of Computer Security.[30] In order to have a broad

---

[27] Halderman, *supra*, at 1-2; *see also* discussion *infra*, Part 8.

[28] *Security and Privacy Research in the Computer Science Department at Carnegie Mellon,* Carnegie Mellon, http://www.csd.cs.cmu.edu/research/areas/security/; *Cornell University Department of Computer Science*, Cornell University, http://www.cs.cornell.edu/research/security; *About UC Berkeley Security*, University of California Berkley http://security.cs.berkeley.edu/; *Ethical Hacking*, University of Colorado, http://www.cs.colorado.edu/~jrblack/class/csci7000/f14/; Ponemon Institute, *2014 Best Schools for Cybersecurity*, *available at* http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf.

[29] J. Scott Armstrong, *Natural Learning in Higher Education*, *available at* http://repository.upenn.edu/cgi/viewcontent.cgi?article=1151&context=marketing_papers.

[30] *Top Conferences in Security and Privacy,* Microsoft Academic Search, http://academic.research.microsoft.com/RankList?entitytype=3&topDomainID=2&subDomainID=2; *Top Journals in Security and Privacy*, Microsoft Academic Search, http://academic.research.microsoft.com/RankList?entitytype=4&topDomainID=2&subDomainID=2.

exchange of ideas and a richer analysis of potential threats and methods to mitigate them, good faith security researchers need to be able to participate in not only the top journals and conferences referenced, but all journals, conferences, and other venues that serve as platforms for discussion salient to their work.

v. Applying research discoveries to build a new, more secure software and devices

Finally, the exemption would allow security researchers to take what they have discovered in terms of flaws or vulnerabilities in software or devices and use that research to construct new software and devices that are better guarded from malicious use.

The work of security researchers has fixed numerous real world problems. For example, David Wagner and Ian Goldberg found flaws in an initial model Netscape software that encrypts financial transactions over the Internet. After the discovery, Netscape publicly thanked Wagner and Goldberg for bringing the flaw to their attention and preventing the malicious exploitation of the flaw.[31] More recently, security researchers have found critical software flaws such as Heartbleed, Shellshock, and Ghost in a variety of widely deployed modern software.[32] These discoveries have allowed developers to fix the underlying flaws, improving the security of a vast swath of Internet users. Such discoveries also contribute to the state of the art in software development, decreasing the likelihood of such vulnerabilities occuring again in the future.

B. Computer security research is either not copyright infringement or is fair use.

The vast majority of computer security research does not constitute an infringing act because it simply involves accessing functional, non-copyrighted elements of the works. Functional elements of copyrighted works are separate from the copyrighted elements of that work.[33] Although software and devices contain both creative and functional elements, legitimate computer security researchers focus on the functional elements. The functional elements, such as a computer program's object code, which contains ideas and executes tasks, are excluded from copyright protection.[34] Computer programs are protected to a lower degree than traditional literary works because they "contain unprotected aspects that cannot be examined without copying."[35]

---

[31] Sara Robinson, *Awaiting DMCA Clarification, Researchers Proceed Cautiously*, SIAM News, Volume 35, Number 1, *available at* http://www.siam.org/pdf/news/387.pdf.

[32] MITRE, *CVE-2014-0160*, National Vulnerability Database, (2014); MITRE, *CVE-2014-6271*, National Vulnerability Database, (2014); MITRE, *CVE-2015-0235*, National Vulnerability Database, (2015).

[33] *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992), as amended (Jan. 6, 1993).

[34] *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 602 (9th Cir. 2000) (citing 17 U.S.C. § 102(b)).

[35] *Id.*

Moreover, in most security research, nothing is reproduced, distributed, or adapted. Most relevant security research focuses not on the reproduction, distribution, or adaptation of copyrighted works, but on the investigation said works. In the course of good faith security research, there may be some incidental reproduction, distribution, or adaptation, but that reproduction will almost certainly be ancillary to the research. As such, the majority of good faith security research is non-infringing.

Even where security research involves more than *de minimis* reproduction, distribution or adaptation, it is universally likely to be a non-infringing fair use. Fair use includes four factors: (1) the purpose and character of the use, including whether such use is for commercial or nonprofit, educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.[36]

Except where noted, the fair use factors apply in the same or substantially similar ways for each of the good faith security research uses outlined above.[37] While it is difficult to offer a specific infringement analysis for each individual use, all of the uses are consistently under the banner of fair use and therefore support the grant of an exemption since they will not result in copyright infringement.[38] Importantly, the proposed exemption does not seek to insulate activities that go beyond good faith security research.

i. The purpose and character of security research weigh in favor of the first factor of fair use.

The purpose and character of the intended uses of our exemption weigh in favor of a fair use determination. The purpose and character of a use is determined by whether the use is transformative rather than merely derivative, whether the use is for educational purposes, and if the use is for commercial use.[39] Whether or not a work is transformative depends on "whether the new work merely supersede[s] 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;" it asks, in other words, whether and to what extent the new work is transformative.[40]

The purposes of good faith computer security research are all listed as paradigmatic fair uses in Section 107's preamble: criticism, comment, news reporting, teaching, scholarship, or research. When good faith computer security researchers investigate and discover security flaws and vulnerabilities in software or devices, they engage in scholarship or research. When researchers document and responsibly disclose security flaws and vulnerabilities they engage in criticism, commentary, or news reporting. When professors permit students to perform hands on

---

[36] 17 U.S.C. § 107.

[37] *See* discussion *supra*, Part 5(A).

[38] *See* 17 U.S.C. § 1201(c)

[39] *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 570 (1994).

[40] *Id.*

investigations of software or a device's security flaws and vulnerabilities the professors are engaging in teaching and education. Thus, the first factor weighs in favor of fair use.

ii. The nature of the works impacted by security research weighs in favor of the second factor of fair use.

The degree of creativity involved in the original work, as well as whether or not the original work has been published, both play a role in the second factor of a fair use determination.[41] The more factual and less creative a work, the more likely it is to be subject to fair use.[42] Publishing also increases the likelihood that a work is subject to fair use.[43]

With computer security research, the nature of the copyrighted works at issue weighs in favor of fair use because the types of works are more factual and functional than they are creative. The scope of copyright protection for computer programs is quite thin since programs embody many functional design elements that copyright law does not protect.[44] While there are undoubtedly creative aspects to computer programs, there are strict rules and conventions that limit the creativity involved. Also, many of these programs are aimed at addressing a specific factual problem rather than expressing creativity. Access to any other copyrighted works during the pursuit of good faith security research is only incidental to that research. Thus, the second factor weighs in favor of fair use.

iii. The amount and substantiality of copyrighted works used in security research generally weigh in favor of the third factor of fair use.

The third factor asks whether the secondary use employs more of the copyrighted work than is necessary, and whether the copying was excessive in relation to any valid purposes asserted under the first factor.[45] For some purposes, it may be necessary to copy the entire copyrighted work, in which case the third factor does not weigh against a finding of fair use.[46] So long as the copying is required for a valid use and results in some form of "transformation," courts lean in favor of fair use.[47]

Good faith researchers' investigations of security flaws and vulnerabilities often utilize few or none of a piece of software's copyrighted elements. When security research does require the copying of protected elements, that copying is merely incidental to the goal of the research, and is necessary to adequately investigate security concerns. When security research is published, it does not contain substantial portions of the original copyrighted work, and has completely

---

[41] *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1524 (9th Cir. 1992), as amended (Jan. 6, 1993).

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Campbell*, 510 U.S. at 586–87.

[46] *Authors Guild, Inc. v. HathiTrust*, 755 F.3d 87, 98 (2d Cir. 2014)

[47] *See Cariou v. Prince*, 714 F.3d 694, 710 (2d Cir.) cert. denied, 134 S. Ct. 618(2013); *Authors Guild Inc.,* 755 F.3d at 710; *Authors Guild, Inc. v. Google Inc.*, 954 F. Supp. 2d 282, 292 (S.D.N.Y. 2013).

transformed the copyrighted work for a significantly different use than the original. Because the works used are necessary to complete the research, and any published aspects are transformed by said research, the third factor weighs in favor of a determination of fair use.

iv. Our intended uses will have little to no effect on the relevant market, weighing in favor of the fourth factor of fair use.

The Supreme Court has described the fourth factor as "undoubtedly the single most important element of fair use."[48] The fourth factor looks at "the effect of the use upon the potential market for or value of the copyrighted work," and, in particular, whether the secondary use "usurps the market of the original work." [49] The market for the original work here is the market for the software that is the focus of the research, since there is no protectable market for criticism or commentary.[50]

Good faith security research will not usurp the market for any original works subject to said research. Security research is not a replacement for any software, but only serves to criticize or comment on the security features of that software. Although a computer program or software company might suffer economic or reputational harm because its product's security flaws or vulnerabilities were disclosed, that harm is irrelevant since it does not usurp the original market.[51] Much of that harm will likely be avoided through coordinated disclosure with the company and the net result will be positive since this will lead to a market for works with more robust security. Thus, the fourth factor weighs in favor of a fair use determination.

6. *Adverse Effects:* Chilling Effects on Legitimate Security Research

The DMCA imposes significant chilling effects on good faith security research due to the ambiguities, gaps, and burdens in Section 1201's built-in exemptions. Moreover, the nature of security research means that no reasonable alternative to circumvention exists in most cases. Granting our proposed exemption is essential to show that security-related circumventions are either exempt from or are not covered by Section 1201(a)(1). This will alleviate uncertainty around the scope of covered access controls.

A. Without the proposed exemption, the risk of serious liability will substantially chill research.

Since its enactment, Section 1201 has had substantial chilling effects on research due to the potential liability researchers must assume. Because Section 1201 can open researchers up to significant civil and criminal liability and because its built-in exemptions are unclear, many researchers are afraid to begin new security research projects involving TPMs. This chilling effect

---

[48] *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 567, 105 S. Ct. 2218, 2234 (1985).

[49] 17 U.S.C. § 107(4); *NXIVM Corp. v. Ross Institute,* 364 F.3d 471, 482 (2d. Cir. 2004).

[50] *Campbell*, 510 U.S. at 592.

[51] *Id.*

has weakened security for the very copyright owners Section 1201 is in place to protect, as well as other users of software and devices.[52]

Students, teachers, and researchers who circumvent TPMs in the pursuit of good faith security research risk going to prison under the provisions in Sections 1203 and 1204 of the DMCA. Under Section 1203, researchers face potential liability for civil damages up to $2,500 per act of circumvention, and under Section 1204, researchers face criminal penalties of up to $500,000, up to 5 years in prison, or both.[53] Anyone found guilty of a subsequent violation, faces a fine of up to $1 million, 10 years in prison, or both.[54]

The risk of incurring thousands or even millions of dollars in liability and being sent to prison is a strong deterrent for those who would otherwise be conducting good faith security research. The risk to security researchers' careers, finances, and freedom often results in researchers avoiding investigating security problems altogether where TPMs are involved.

One example of the chilling effects researchers face under Section 1201 arose in the public challenge issued by the Secure Digital Music Initiative (SDMI). SDMI challenged experts to defeat watermarking technologies intended to protect digital music.[55] Researchers from Princeton, Rice, and Xerox succeeded in removing the watermarks and prepared to unveil their results at an academic conference. SDMI threatened those researchers, sending letters to conference organizers and the researchers' employers.[56] The researchers were forced to withdraw their paper from the conference, and after enduring a subsequent legal battle, some of the researchers involved decided to forgo further research efforts in this field.[57] Researchers were challenged to find vulnerabilities in watermarking technologies so these technologies could be improved in the future, but Section 1201 was used as a sword to prevent the researcher's efforts from helping contribute to more secure technology.

A second example of Section 1201's chilling effects arose when researchers disclosed vulnerabilities in the Texas Instruments' Data Storage Tag (DST), which uses sensors to track information. When they did so, Texas Instruments contacted officials at the researchers' universities in an attempt to block disclosure.[58] These attempts were ultimately unsuccessful, in part because the researchers had a fully mature research result and a paper prepared for submission. But many researchers in the early stages of a project are currently inhibited by Section 1201 for fear that a lawsuit will not only stop research and innovation, but could destroy a researcher's practice or a student's future career. The opportunity for security researchers to

---

[52] Robinson, *supra*.

[53] 17 U.S.C. § 1203(c)(3)(A); 17 U.S.C. § 1204(a)(1).

[54] 17 U.S.C. § 1204(a)(2).

[55] Pamela Samuelson, *Anticircumvention Rules: Threat to Science*, 293 Science 2028, 2028 (Sept. 14, 2001).

[56] *Id.*

[57] Letter from Matthew Oppenheim, SDMI General Counsel, to Prof. Edward Felten (Apr. 9, 2001) *available at* http://cryptome.org/sdmi-attack.htm.

[58] Samuelson, *supra*, at 2028.

collaborate on this topic, creating a broader discussion for sharing research findings, will help the discipline gain insight into possible dangers lying within software and the mitigation thereof.

The chilling effect has not been limited to U.S. researchers alone. Foreign researchers have even been deterred from working in and traveling to the U.S. for fear of prosecution under the anti-circumvention provision of the DMCA. For example, the Russian government went so far as to issue a travel advisory stating they "would like to draw the attention of all Russian specialists cooperating with U.S. firms in the computer software and programming business to the fact that [Section 1201] may be used against them on U.S. territory."[59]

B. Section 1201's built-in exemptions provide insufficient clarity and breadth to cover the uses in the proposed exemption.

Without the proposed exemption, the lack of clarity and breadth in Section 1201's built-in exemptions will continue to chill research. Although Congress included exemptions in Section 1201 that were intended to apply to some of the research that would be covered under this exemption—Section 1201(f) for reverse engineering, Section 1201(g) for encryption research, and Section 1201(j) for security testing—these exemptions suffer from a variety of problems.[60] Their overly narrow scopes, restrictions on research, restrictions on dissemination of information, authorization requirements, reliance on multi-factor tests, and other infirmities mean that the built-in exemptions fail to provide the certainty necessary for researchers to pursue projects involving TPMs.

This dynamic necessitates that the Librarian grant the proposed exemption to avoid chilling research that Congress intended to enable. These chilling effects have been previously acknowledged by the Copyright Office, and should be addressed in this rulemaking to avoid further injury to security research.[61]

i. The Reverse Engineering Exemption (Section 1201(f))

Under Section 1201(f), a person who has legally obtained a computer program that is protected under copyright may reverse engineer and circumvent the access control protection on that program.[62] Section 1201(f) is limited to circumvention "for the sole purpose of identifying

---

[59] Jennifer Lee, *Travel Advisory for Russian Programmers*, NY Times, Sept. 10, 2001, *available at* http://www.nytimes.com/2001/09/10/technology/10WARN.html.

[60] *See* U.S. Copyright Office, *The Digital Millennium Copyright Act of 1998 U.S. Copyright Office Summary* (December 1998) *available at* http://www.copyright.gov/legislation/dmca.pdf.

[61] In the 2010 Rulemaking Exemption, the Register acknowledged that "NTIA believed that the proponents have "persuasively argued that without a research exemption, research into all current and future vulnerabilities will be and is chilled now," and concurred with the Librarian's conclusion in 2006 that the research may not be covered completely by the existing statutory exemptions." *2010 Final Rule*, 75 Fed. Reg. at 43,833.

[62] 17 U.S.C. § 1201(f).

and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program."[63]

The problem with this exemption is that not all vital security research has the "sole purpose" of improving interoperability. Under Section 1201(f)(4), interoperability is defined as "the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged."[64]

While some research may have the purpose of improving inoperability, research often has other purposes in addition to (or exclusive of) interoperability. Some crucial security research may be broadly construed to improve the interoperability of computer programs by exposing security flaws, incentivizing companies to repair those flaws, and thereby improving the suitability of the programs for interoperation with the other programs. However, the broader aims of good faith security research include publication, teaching students in security research to understand the access controls they are working with, and improving the security of all software and devices.

ii. The Encryption Research Exemption (Section 1201(g))

The encryption research exemption in Section 1201(g) contains numerous ambiguities and requirements that do not provide sufficient clarity as to the legality of good faith security research. For example:

- Section 1201(g) limits "encryption research" to activities that are "necessary" to identify flaws and vulnerabilities of "encryption technologies."[65] Some security research may simply not involve encryption technologies.[66]
- To be eligible for Section 1201(g), activities must be conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products.[67] Not every security research project is conducted with those aims exclusively in mind. For example, some projects are conducted to provide students with valuable experience working on real systems. Under the current exemption, it is unclear whether doing so would be considered advancing the state of knowledge in encryption technology.
- Section 1201(g) requires researchers to undertake efforts to obtain authorization from copyright holders.[68] This requirement poses a problem for security researchers where copyright holders deny requests for authorization and use their knowledge of the researchers' activities to thwart the potentially reputation diminishing research through spurious legal action.

---

[63] *Id.*

[64] 17 U.S.C. § 1204(f)(4).

[65] 17 U.S.C. § 1201(g)(2); 17 U.S.C. § 1201(g)(1)(A).

[66] *See* discussion *supra*, Part 4.

[67] 17 U.S.C. § 1201(g)(1)(A).

[68] 17 U.S.C. § 1201(g)(2)(C).

- The application of Section 1201(g) requires the evaluation of a multifactor test, which makes determining *ex ante* whether a particular course of research will be eligible for the exemption impossible.[69]
- The second factor of the multifactor test is problematic because it potentially restricts Section 1201(g)'s applicability to people who are "engaged in a legitimate course of study" or "appropriately trained or experienced"—without defining those terms.[70] Although many working in security research are professionals, there is much valuable work being done in this space by amateurs.[71]
- The third factor of the test is problematic because it potentially requires that researchers disclose their findings and documentation by some particular "time" without specifying what that time is. Again, researchers cannot determine *ex ante* when they must disclose research to qualify for Section 1201(g), and even doing so on a timeline consistent with coordinated disclosure guidelines widely accepted in the community may ultimately be seen by a court as too late.

iii. The Security Testing Exemption (Section 1201(j))

Finally, Section 1201(j)'s exemption for security testing contains similar infirmities:

- Section 1201(j) only applies to acts of "security testing."[72] "Security testing," in turn, applies only to accessing "a computer, computer system, or computer network."[73] The Copyright Office has issued guidance construing "a computer, computer system, or computer network" narrowly under Section 1201(j).[74] This makes it "unclear whether Section 1201 (j) applies in cases where the person engaging in security testing is not seeking to gain access to "a computer, computer system, or computer network."[75]
- Section 1201(j) requires security researchers to seek the authorization of the owner or operator of the computer, computer system, or computer network that is the focus of the research.[76] Determining who the owner or operator of a computer system can be a complex factual determination, and in many cases is impossible.

---

[69] *See* 17 U.S.C. § 1201(g)(3).
[70] 17 U.S.C. § 1201(g)(3)(B).
[71] *See* Dan Goodin, *Texas Instruments Aims Lawyers at Calculator Hackers*, The Register, Sept. 23, 2009, *available at* http://www.theregister.co.uk/2009/09/23/texas_instruments_calculator_hacking/; Robert McMillan, *Apple is Sued after Pressuring Open-Source iTunes Project*, PC World Apr. 29, 2009, *available at* http://www.pcworld.com/article/163909/apple_is_sued_after_pressuring_opensource_itunes_project.html.
[72] 17 U.S.C. § 1201(j)(2).
[73] 17 U.S.C. § 1201(j)(1).
[74] *2010 Final Rule*, 75 Fed. Reg. at 43,832-33.
[75] *Id.*
[76] 17 U.S.C. § 1201(j)(1).

- As with the encryption research exemption, the requirement of authorization creates the potential for a copyright holder to deny the researcher's authorization, then thwart the research through legal action.[77]
- Section 1201(j) also imposes a multi-factor test that prevents *ex ante* determination of whether particular research will be deemed permissible under Section 1201.[78]
- The first factor of the test is especially problematic because it hinges on whether the activity is solely for the benefit of a computer's owner or operator.[79] Many research projects may lead, for example, to the release of information on how the owner or operator of a computer, computer system, or computer network failed to properly secure a computer system, or other outcomes that may benefit the public, but not the owner.

C. No widely applicable non-circumventing alternatives exist.

In most cases of security research, there are no reasonable alternatives to circumvention. This is because all instances of the software or device under investigation are protected by TPMs, thus no investigation can take place without bypassing a TPM. In addition, software developers and copyright holders lack adequate incentives to conduct the necessary security research themselves. In many cases, developers and copyright holders attempt to leverage Section 1201 against researchers to *conceal* security vulnerabilities rather than fixing them.

7. *Statutory Factors:* Additional Considerations under Section 1201

Under Section 1201(a)(1)(C), the Librarian of Congress considers five factors in whether to grant an exemption:

(A) The availability for use of copyrighted works;
(B) The availability for use of works for nonprofit archival, preservation, and educational purposes;
(C) The impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
(D) The effect of circumvention of technological measures on the market for or value of copyrighted works; and
(E) Such other factors as the Librarian considers appropriate.[80]

Each of these factors weigh in favor of granting the proposed exemption.

A. The Availability for Use of Copyrighted Works

A general exemption for good faith security research will increase the number of copyrighted works available for study by superseding the existing patchwork of prior, narrowly-defined good faith security research exemptions. Prior good faith security exemptions have been limited to

[77] *See* discussion *supra*, Part 6(B)(ii).
[78] 17 U.S.C. § 1201(j)(3).
[79] *See* 17 U.S.C. § 1201(j)(3)(A).
[80] 17 U.S.C. § 1201(a)(1)(C).

narrowly defined classes of works, placing many works researchers wish to study outside of the scope of the exemption. The broad and general exemption we request is necessary to ensure good faith security researchers may study any form of software or device relevant to the safety of individuals or security of the nation. Security researchers will make use of access to this broader class of works to further advance the safety and security of software and devices. The works themselves will become more useful and more valuable through this increased safety and security.[81]

B. The Availability for Use of Works for Nonprofit Archival, Preservation, and Educational Purposes

The risk of liability under Section 1201 when performing security research in educational contexts forces researchers to limit student involvement and can push risk-averse universities from such research. Because the individuals conducting security researchers are often graduate students with few resources, professors limit their involvement to limit their liability. Liability under Section 1201 can result in large monetary damages and criminal prosecution, possibly destroying a student's chances at future employment or even leading to incarceration. Ambiguities in the existing exemptions make it difficult to be sure that any given research project falls under an exemption, which can lead to problems in obtaining research approval and funding. Granting a general exemption for good faith security research would remove ambiguities and improve educational access to the copyrighted works necessary for such research. A general exemption would also increase educational access, and improve the educational opportunities available for budding security researchers.

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

Academic and amateur security researchers, commonly known as "white hat" researchers, are negatively affected by a prohibition on circumvention of technological measures in a variety of contexts. Good faith security research includes criticism, commentary, news reporting, teaching, scholarship, and research. All aspects of security research, from scholarship, to teaching, to testing, to commenting, criticizing, and reporting, are disincentivized by the current gaps and ambiguities in Section 1201's exemptions. The resulting chilling effects inhibit key security research, hindering the security of critical information infrastructure. The importance of improving the security of these systems has never been more apparent as evidenced by the recent high-profile breach at Sony, and the seemingly endless list of credit card systems that have been compromised.[82] The White House, Congress, the National Telecommunications and

---

[81] *See* discussion *supra*, Part 6(B).

[82] Grant Gross, *US Lawmaker Asks Sony for Details on Data Breach*, ComputerWorld, Dec. 23, 2014, *available at*, http://www.computerworld.com/article/2863054/us-lawmaker-asks-sony-for-details-on-data-breach.html; Kate Vinton, *Credit Cards Compromised In Month-Long Kmart Data Breach*, Forbes, Nov. 10, 2014, *available at*,
(continued…)

Information Administration (NTIA), and other government entities support improving security as a national priority, and the Copyright Office can do its part by granting this exemption.[83]

The existing exemptions for reverse engineering, cryptography research, and security testing in the DMCA highlight the importance of implementing a general security research exemption. The existing exemptions show that the DMCA was not meant to inhibit security research.[84] Unfortunately, the ambiguities and gaps in those exemptions have a chilling effect on good faith security research. Security research has a direct impact on national security. The fact that vast majority of the United States' critical infrastructure is owned and/or operated by the private sector highlights the importance of fostering security research to identify issues that might otherwise be swept under the rug.[85] The interconnected nature of the Internet means that vulnerabilities in individual systems can have widespread public safety effect.

The more security research that is carried out, the less vulnerable American infrastructure is to attack. A general exemption would further the intent of the current exemptions and serve the national interest through promoting secure information systems.

D. The Effect of Circumvention of Technological Measures on the Market for or Value of Copyrighted Works

A general exemption for good faith security research with positive net effect on the market for software and devices. While the research furthered by this exemption might hamper the market for some software and devices by exposing weaknesses in their security, this effect will not be due to copyright infringement. Any damage to the market for copyrighted works will result only from the exposure of inherent shortcomings in the works themselves.

Moreover, coordinated disclosure guidelines help to reduce the risk of market impacts by allowing companies time to address vulnerabilities before they are made public. This dynamic

---

http://www.forbes.com/sites/katevinton/2014/10/10/credit-cards-were-compromised-in-kmart-data-breach/.

[83] *See* Andrea Shalal and Alina Selyukh, *Obama seeks $14 billion to boost U.S. cybersecurity defenses,* Reuters, *available at* http://www.reuters.com/article/2015/02/02/us-usa-budget-cybersecurity-idUSKBN0L61WQ20150202; Exec. Order 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11737 (Feb. 19, 2013) *available at* https://federalregister.gov/a/2013-03915; Press Release, The White House Office of the Press Secretary, Launch of the Cybersecurity Framework (Feb. 12, 2014), http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework; *NTIA, Recommendations to the President on Incentives for Critical Infrastructure Owners and Operators to Join a Voluntary Cybersecurity Program* (Aug. 6, 2013) *available at* http://www.ntia.doc.gov/report/2013/discussion-and-recommendations-president-incentives-critical-infrastructure-owners-and-o.

[84] U.S. Copyright Office, *The Digital Millennium Copyright Act of 1998 U.S. Copyright Office Summary* 3 (December 1998) *available at* http://www.copyright.gov/legislation/dmca.pdf.

[85] *President Barack Obama, Remarks by the President on Securing Our Nation's Cyber Infrastructure* (May 29, 2009) *available at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

will create a stronger incentive for secure works and opportunity to repair deficient technologies. Thus, the net effect of a general exemption will be to increase the quality and value of the works themselves and the safety and security of the consumers who depend on them.

E. Factors the Librarian may Consider Appropriate

Good faith security research testing is a matter of national security. Rather than having negative repercussions on safety and security of critical infrastructure by allowing the malicious exploitation of flaws and vulnerabilities, a general exemption for good faith security research will help identify and repair such flaws and vulnerabilities before they can be exploited. Thus, promoting greater security research yields a public good. Furthermore, promoting security research is vitally important for the government and the economy. We have the resources to lead the world in the creation and maintenance of secure software and devices, and a broad, general good faith security research exemption will promote this.

In addition to being critically important to U.S. security, the conduct and publication of security research is protected by the First Amendment. As a result, granting the proposed exemption is critical, at a bare minimum, to avoid an unconstitutional application of Section 1201. The triennial exemption process is Section 1201's mechanism for recognizing fair use, which the Supreme Court has labeled a "built-in First Amendment accommodation." Thus, failing to grant the proposed exemption would subject Section 1201 to constitutional scrutiny. [86]

* * *

For the foregoing reasons, the Librarian should grant the proposed exemption.

Respectfully submitted,

/s/

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

Prof. Blake E. Reid, Director

Counsel to Prof. Green

[86] *Golan v. Holder*, 132 S. Ct. 873, 876 (2012).

8. *Documentary Evidence*

The following documentary evidence is a research plan composed by Prof. Green.

I am a Research Professor in the Information Security Institute at Johns Hopkins. My primary academic research focuses on the field of computer security and applied cryptography. Before I joined the faculty at Johns Hopkins, I was also founder and CTO of a security consulting firm with clients including Walt Disney Publishing, MovieLabs, Barnes & Noble, and MasterCard.

Introduction

Over the past decade, I have conducted extensive research aimed at improving the security and robustness of information systems. Throughout the course of my research, my colleagues and I have investigated systems where the consequences of a security failure include the theft of sensitive personal information, financial loss, and—in at least one case—the potential for loss of human life.

In order for good faith security researchers to secure modern information systems from attack, a researcher must first *understand* the weaknesses that make the systems vulnerable. The main challenge in my work is that both products and attack techniques evolve constantly. To gain understanding, academic and industry security researchers like me must examine deployed software and devices to determine which vulnerabilities are present, and to gain insight into how these vulnerabilities may be exploited by motivated attackers.

Unfortunately, the process of examining real systems carries potential legal risks, many of which result from Section 1201. In support of my request for exemption from the anti-circumvention measures of the DMCA, this document outlines the course of an example research project from conception to execution and publication.

Stage 1: Identification

The first stage of any research project is to identify a specific category of software or device that may not achieve its security goals as designed. For example, in one project we sought to analyze the security of wireless "contactless" payment systems. To do this, we first examined a number of deployed payment systems to gain an understanding of what technologies were in place to secure these systems against fraudulent use – and to determine whether those systems properly achieved this task.

The challenge in this first phase is to understand a given system well enough to determine whether it may potentially be vulnerable. In a very limited set of cases we can accomplish this using only published documents provided by the manufacturer. In many other cases, however, manufacturers choose not to publish the necessary information. Thus, even *identifying* potentially vulnerable systems requires some degree of detailed analysis of a system, up to and including reverse-engineering and defeating technological protection measures (TPM) that may protect aspects of the system.

This potentially puts us in conflict with Section 1201. The legal risk at this stage can be particularly chilling, given that many academic research projects require the assistance of graduate students. As an academic researcher, I may feel comfortable taking on a limited amount of legal risk. However, there are ethical challenges in exposing students to the same risk. Even when the risk of a potential lawsuit is low, this risk must be weighed against the potential costs and the student's limited resources.

At this stage of our research, we may be considering a variety of information systems with different characteristics—and moreover, have not yet begun to carefully analyze the system for real vulnerabilities. Thus, it may be challenging to request permission from a manufacturer.

Stage 2: Initial Analysis

Once we have determined that a given system may contain security vulnerabilities, we now analyze the security system to understand what security measures it offers, and to determine whether these measures are vulnerable to attack.

The techniques we use to conduct this analysis depend on the specific project. In some rare projects we are able to conduct a "black box" analysis of a system—reverse-engineering the design of the system simply by measuring its outputs.

However, in most cases, we must analyze the software used in the system and even sending data to the system may require us to defeat a technological protection measure. For example, in one research project we attempted to send data to a system, but found that a simple password check prevented us from even performing this interaction. In order to go forward with our research, we were forced to defeat this measure. While our goal in doing this was clearly not to violate any copyrights, the current language of Section 1201 put us at risk, regardless of our intentions.

Often, before we can begin any process of serious analysis, we retain counsel to advise us on the DMCA and other legal risks. While we've been fortunate to receive pro bono assistance from experts at the Electronic Frontier Foundation (EFF), this assistance is not something we or other researchers can take for granted.

Stage 3: Execution

Our research is not complete once we have discovered vulnerability in a system. We then look at ways in which we can address the security flaw. On more than one occasion we have identified a flaw in a system—one that has the *potential* to be exploited—only to be told by the manufacturer that the flaw was not serious enough to be addressed. In many cases, this occurs when a manufacturer is not convinced that a given flaw can actually be *exploited* into a valid attack on the system. In some cases, this understanding may be correct—but in many other cases, it is not. Manufacturers' failure to remedy vulnerabilities due to a perceived 'lack of exploitability' has resulted in many widely publicized security failures.[87]

---

[87] For example the recent "Ghost" attack on Linux Domain Name Service implementations involved a patch to a bug that was released in 2013, but not widely deployed in production (continued…)

Thus, in many cases, an important component of our research is to actually implement a simulated attack and conduct every step of the exploitation in order to determine whether the system truly is vulnerable. We never perform this process on a production-ready system without the explicit approval of the manufacturer; often it suffices to execute our attack on a "test bed" setup.

The challenge here is that executing an attack substantially increases the probability that we will—perhaps unwittingly—circumvent a TPM. For example, in a recent project involving the FIPS-approved (Federal Information Processing Standard) cryptographic libraries, actually running an attack required us to modify a checksum in the software that might have been considered a TPM protecting the binary code.

Stage 4: Disclose and Publication

As security researchers, we adhere to a strict policy of "coordinated disclosure" for all vulnerabilities we discover. Coordinated disclosure involves notifying a vendor of security vulnerability and—in many cases—demonstrating how it can be exploited. Disclosure, and an opportunity to repair the flaw, always comes before any publication of our work.

Paradoxically, one of the worst consequences of Section 1201 is its chilling effect on the process of coordinated disclosure. While we have many positive stories resulting from disclosing vulnerabilities to vendors, we have also experienced responses that amount to harassment. In one instance, a vendor contacted the Provost at Johns Hopkins and asked that our research be suppressed. This is not consistent with our obligations as public researchers, but, when such threats are backed by the potential for legal action under Section 1201, they can be compelling and can force us to avoid doing further research.

Ironically, this risk only exists when researchers responsibly disclose vulnerabilities. This, combined with financial incentives, has led many qualified individuals to avoid disclosing vulnerabilities, resulting in both "black market" and "grey market" economies for system exploits. The former involves criminal uses of vulnerabilities. The latter market involves sales of exploits to government agencies, both domestic and international, for use in surveillance and potential cyber-attacks.

Once all disclosure obligations have been satisfied, we typically publish our work in a reputable computer science conference or journal so that public users and software developers may benefit from the work. Again, we may face threats under Section 1201 from doing so.

A remark

The sections above describe the course of a *successful* investigation. Unfortunately, research success is never guaranteed, and many investigations produce negative results. Unfortunately, these cases can be the most challenging from a legal perspective, since we incur exactly the same potential legal risks, but have no publication to show for our work.

---

systems due to the fact that it was not viewed as an exploitable security flaw. In 2015, exploit code was published that made it possible to take control of a Linux system via this flaw.