Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201

Item 1. Commenter Information

Prof. Steven M. Bellovin (Columbia University), Prof. Matt Blaze (University of Pennsylvania), Prof. Edward W. Felten (Princeton University), Prof. J. Alex Halderman (University of Michigan), and Prof. Nadia Heninger (University of Pennsylvania) (the "Security Researchers").

Item 2. Proposed Class Addressed

Proposed Class 25: Software – Security Research

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.

Item 3. Overview

Literary works, including computer programs and databases, protected by access control mechanisms that potentially expose the public to risk of harm due to malfunction, security flaws or vulnerabilities when

(a) circumvention is accomplished for the purpose of good faith testing for, investigating, or correcting such malfunction, security flaws or vulnerabilities in a technological protection measure or the underlying work it protects; OR

(b) circumvention was part of the testing or investigation into a malfunction, security flaw or vulnerability that resulted in the public dissemination of security research when (1) a copyright holder fails to comply with the standards set forth in ISO 29147 and 30111; or (2) the finder of the malfunction, security flaw or vulnerability reports the malfunction, security flaw or vulnerability to the copyright holder by providing the information set forth in Form A* in advance of or concurrently with public dissemination of the security research.

* Form A is a format derived from ISO 29147 Annex A:

FORM A

A researcher disclosing a vulnerability to a copyright holder shall provide the following information in writing:

1. a basic summary that includes (a) a technical description, (b) the finder's contact information, (c) a description of any public disclosure plans, (c) projected impact or a threat and risk assessment, to the extent possible (d) a description of the software configuration at the time of the discovery, if not default; (e) any relevant information about connected devices; AND

2. a product-specific component consisting of (a) if the software or hardware, the product name or model, the operating system, and the version or revision number of the product or (b) if an online service, the time and date of discovery, the relevant URL, browser information including type and version, and the input required to reproduce the vulnerability.

Item 4. Technological Protection Measure(s) and Method(s) of Circumvention

For purposes of this exemption, any access control mechanism that potentially exposes the public to risk of harm due to malfunction, security flaws or vulnerabilities is an appropriate subject of research. These access control mechanisms will vary in type from technology to technology. The particular design and architecture of the product dictate the type of copy protection measure selected by the copyright holder. There are two types of copyrightable material implicated by this exemption: first, software that runs on general purpose computer and, second, firmware and hardware in embedded devices and products. A wide range of mechanisms exists – the hardware, platform and architecture of the device determine the choice. Code obfuscation, failure to provide interfaces, sophisticated hardware with anti-reverse engineering features, and the use of encrypted code and data are some of the access control methods commonly used by copyright holders to limit copying of their code and are, therefore, implicated by this exemption. However, new methods of copy protection are developed regularly and a typical product or device may incorporate any combination of these or other methods.

<u>Example of TPMs in past research that could have raised DMCA concerns but did not solely because of Secretary of State intervention</u>

For example, one of the Security Researchers was asked by the Ohio Secretary of State to lead a team to examine the integrity of various vendors' voting machines certified for use in Ohio. Because voting machine vendors generally maintain tight controls over the software and technical details of their systems, this investigation happened solely because of the Secretary of State's intervention and request. In the course of this investigation, the researcher team discovered numerous serious exploitable vulnerabilities in almost every component of every vendor's system that was examined, including vulnerabilities that could be used to undetectably alter the outcome of an election. As a result of this study, technical and procedural changes were made in Ohio and other states to make it more difficult to exploit the flaws that we discovered. In the course of the analysis, the researcher team needed to defeat hardware and software mechanisms that were intended to prevent copying or alteration of data. The research team developed techniques for misusing various hardware and software interfaces to extract and alter software, firmware and other data stored on the machines that were not intended to be copied or altered. These machines used multiple different types of TPMs, and they all needed to be defeated in order to fully conduct the research as desired by the Secretary of State of Ohio.

Example of TPM that inhibited actual research that remained unperformed until disclosure by a third party and a DMCA exemption.

In 2006, two of us sought to research the safety of technological protection measures being included on consumer audio and other media CDs. We sought the advice of counsel who cautioned us about risks associated with DMCA Section 1201. We decided to request an exemption for the research from the Copyright Office. This exemption was ultimately granted. We filed for a DMCA exemption request in which we described the TPMs at issue as follows: "The current breed of active technological protection measures rely almost invariably on the AutoRun feature of the Windows operating system for initial installation. AutoRun allows software code contained on removable media like CDs to run automatically when inserted into a computer. Using AutoRun a CD can automatically install software on a computer without the knowledge or consent of its owner. In the context of CD protection measures, the software installed using AutoRun often includes a device driver that limits the functionality of the consumer's CD-ROM drive, preventing consumers from playing or copying their CD and creating the security risks described above. The current active technological protection measures exploit this aspect of AutoRun, because most consumers would prefer the freedom to make personal backup copies, listen to tracks in order of their preference, or transfer CDs to iPods or other portable media players and are therefore reluctant to install software that would limit these lawful activities. Absent the installation of the this software, the CD format by nature allows consumers to freely access and use CD audio files."[1]

However, the TPMs described above are not necessarily representative of all current approaches, as technology in these fields evolves quickly. Meanwhile, a third party researcher disclosed a portion of the analysis, and we decided to assume the DMCA legal risk, complete the research and disclose our findings. We were vindicated in this choice when the Copyright Office ultimately granted our exemption request, however, in the interim, we had delayed the performance of the research due to DMCA concerns and then later uncomfortably risked the possibility that a litigant or prosecutor may decide we violated Section 1201 in performing our research. The ambiguities of the statute gave us no comfort. The research had been time sensitive, and millions of machines were compromised by the rootkit at issue, in both the public and private sector.[2] The delay in our research arguably had actual information security for consumers and national security consequences.

Example of TPM that inhibited actual research that remain unperformed on the advice of counsel

However, in most research circumstances, a governmental actor is not asking for the assessment or willing to intervene on behalf of researchers. Consequently, in most other cases, when the research begins to involve TPMs, researchers seek the advice of counsel. Attorneys regularly counsel in this circumstance that the DMCA is an unclear statute and that undertaking any such

[1] See p. 3-4 Comments of Comment of Edward W. Felten Professor of Computer Science and Public Affairs; J. Alex Halderman Department of Computer Science, Princeton University, dated December 1, 2005

[2] http://www.nytimes.com/2005/11/19/business/media/19online.html?_r=0 For an academic discussion of legal implications of security-invasive digital rights management technologies for consumers, see, e.g., Andrea M. Matwyshyn, Technoconsen(t)sus, 85 Wash U. L. Rev. 3 (2007).

research exposes the researcher to legal risk. As such, attorneys usually counsel against continuing the research. For example, one of us was investigating the integrity of a secure wireless communication system used by various government agencies. In the course of this investigation, s/he was counseled by an attorney that constructing tools to extract the firmware from a particular vendor's product in ways not supported by the existing interfaces for the purpose of vulnerability analysis could constitute a violation of the DMCA. This precluded analysis of implementation vulnerabilities and limited the scope of analysis to those vulnerabilities that could be found in the published specifications for the system.

Because the exemption request is driven by the nature of the research and the disclosure conduct of the researcher, the environment in which the research is conducted will vary. Security research teams exist in many major corporations,[3] in academia and in government agencies, among other places.

Item 5. Asserted Noninfringing Use(s)

The types of noninfringing uses that are adversely affected by the absence of this exemption under Section 1201 of the DMCA include the following:

- Research: The work will be used by security researchers in order to (a) unlock public access to knowledge about security research through conference presentations and publications in academic journals and proceedings; (b) improve safety of products and services relying on computer code; (c) improve national security of critical infrastructure relying on computer code; and (d) enable companies to perform and access security research as part of their legitimate business operations in order to create better products. Internet of things startups in particular face challenges in obtaining and affording security testing of their products.

- Teaching: Training the next generation of information security professionals to work in government and in the private sector as security engineers who defend sensitive information assets is impossible without their teachers being able to demonstrate the mechanics of various types of attacks, including those on devices with TPMs.

- The policy goals that underpin Section 1201 (g)(f) and (j), when combined with the language of granted exemptions. Granting this requested exemption cleanly updates and clarifies the scope of statutorily allowed research in Sections 1201(g)(f) and (j) in light of the ambiguities created by new types of information security threats facing companies, consumers, and our country's national security. Further, as articulated in the 2006 Audio Recording Security Research Exemption, no infringement occurs when circumvention is accomplished for the purpose of good faith testing, investigating, or correcting

[3] See e.g., Short Comments of Internet Association supporting this exemption request

malfunctions, security flaws or vulnerabilities, as well as the circumvention that was part of an investigation that resulted in the public dissemination of security research regarding malfunctions, security flaws or vulnerabilities.

- Protecting consumers under Section 1201(i). Section 1201(i) was presciently crafted by Congress and is well-suited to specifically encompass this exemption request in light of the new security and privacy dangers for consumers arising out of the Internet of Things. 1201(i) on its face demonstrates that Congress specifically contemplated and sought to protect the public from malfunctioning, flawed or vulnerable code that harms consumers: Section 1201(i) states that a consumer's investigation of code functionality on a privately-owned system in order to determine whether a privacy harm is happening does not constitute an impermissible circumvention. In this spirit of 1201(i), this exemption request similarly seeks to empower consumers with better information about how computer code is behaving on their systems and the systems upon which their safety relies. However, unlike 1201(i), this exemption request recognizes the practical reality that most consumers lack the technological skills needed to engage in the type of technical inquiry 1201(i) expressly authorizes. This exemption request, therefore, empowers security researchers to unlock the truth of code behaviors, acting as agents on behalf of the consumers suffering the harms contemplated by 1201(i) and other malfunctions, security flaws or vulnerabilities that expose the public to risk of harm.

The security risks sought to be avoided include various forms of harms that arise from malfunctioning, flawed or vulnerable code and lead to a company's or a consumer's loss of control over a system, machine or device. This loss of control may mean that a third party attacker can manipulate outcomes or that a malfunction will cause the machine to automatically generate a dangerous outcome.

Technologically, this loss of control may result from any one of a number of categories of security problems and attacks including, but not limited to, the following examples:

- Attacks that exploit race condition
- Passive interception of communication
- Active interception of communication such as a man in the middle attack
- Exploitation of deliberate but unpublished backdoor access mechanisms
- Rootkits
- Code injection through mechanisms such as buffer/heap/stack overflows
- Exploitation of poor input validation such as defects that permit SQL injection
- XXS
- DoS
- Access control problems
- Unvalidated inputs and misconfiguration errors
- Weaknesses in authentication, authorization or cryptographic practices[4]

[4] For discussions of various vulnerabilities and coding errors, see, e.g., Ross Anderson, Security Engineering (2001).

As a result of this loss of control, the human-experienced security risks include but are not limited to the following:

- Physical harm to humans through malfunctioning, e.g., medical devices, including possible death. In some cases, children are disproportionately impacted by their reliance on devices.[5]
- Damage to property, the economy and national security interests, e.g., loss of control over networked home and office automation devices.
- Loss of control over sensitive information that resides on the machines or devices at issue.
- Loss of control over privacy from unwanted intrusions by compromised cameras and microphones

Item 6. Asserted Adverse Effects

There are no potential alternatives that permit the asserted noninfringing uses without the need for circumvention. The safety of the code of a particular machine or device can only be accomplished through rigorous analysis by experts.

The inability to conduct security research where a TPM exists has or is likely to have adverse effects on the following noninfringing uses:

1. Research:

    a. Research for journal publication and conference presentations. The research of each of us has been negative impacted by the ambiguities of DMCA Section 1201. We have altered both the subject matter and the methodology of our intended research in cases where we were advised by counsel of DMCA Section 1201 risks. These alterations made our research lower in quality and thoroughness than it would have been otherwise. This research directly leads to the development of more robust security strategies to innovate the next generation of more secure products.

    b. Government funded research. Because some of us are funded by grants from the Federal Government, including the National Science Foundation and the Department of Defense, this means that when DMCA Section 1201 restrictions cause subject matter and methodology alterations in our research, this change then negatively impact our government-funded research,[6] as well as our private sector funded research.

    c. National security research. A portion of the research that we perform has obvious national defense implications, seeking to improve the information integrity of the economy and the security of government systems. For example, some of us research and create software testing tools to facilitate manual and automated software security

[5] See e.g., Short Form Comments of Jay Radcliffe, Senior Security Consultant, Rapid7
[6] See also Short Form Comments of Professor Salvatore Stolfo, Columbia University

testing by legitimate businesses and government entities to defend their systems against criminals and attacking nation state actors.[7]

d. International security research. Because the internet and networked devices are inherently global in their reach, the loss of security research caused by Section 1201 has negative ripple effects not only domestically but also on the United States' trusted global allies and researchers internationally. When we quash security research in the United States we harm not only our own national security but also the security of other countries.[8]

e. Consumer safety research. This exemption would facilitate researcher, consumer and third party diagnoses and mitigation of defects in consumer products such as Internet of Things devices, cars, and medical devices. Similarly, researchers could be asked by media or safety assessment organizations to empower consumers who want to make informed purchasing decisions with better information.

2. Assisting consumers in permitted consumer investigations of privacy invasion under Section 1201(i).

3. Educational use in teaching, especially for training minors in the basics of information security

Granting the exemption would have no negative repercussions with respect to the safety or security of the works that are the subject of the research. The flaws uncovered by the security research that the exemption will facilitate are pre-existing, not caused by the research. The research does not make it easier for wrongdoers to access sensitive applications or databases – criminals undoubtedly already know about these defects in the code and are potentially already actively exploiting them to harm consumers.

[7] Id.
[8] See e.g. Short Form Comment of Dr. Ian Brown, et. al.

Item 7. Statutory Factors

Evaluate the proposed exemption in light of each of the statutory factors set forth in 17 U.S.C. 1201(a)(1)(C):

(i) the availability for use of copyrighted works;

The lack of a security research exemption damages the availability of works relating to security research. Because of fear of legal consequences under the DMCA, security researchers are creating fewer publications relating to information security research. This proposed exemption would ensure a safer environment for security research that would stimulate production of more works. More copyrighted works would be created, and the work would be of even higher caliber.

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

The absence of this exemption means that information security education efforts are actively hampered on all levels of the educational system. The information security skills needed to defend our country against sophisticated attackers from other countries take years of intensive, rigorous training that can only be accomplished through analysis and examination of flawed code, under the supervision of an expert.

(iii) 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;

A serious, negative impact on computer security scholarship exists because of fear of legal consequences under DMCA Section 1201.[9] As explained above, teaching the next generation of technology professionals capable of defending our national security, economy and corporate digital assets is also hindered. If granted, this exemption would allow for secondary analysis and critique by the press to arise regarding security of consumer products. This type of criticism and synthetic analysis by journalists for consumer consumption would stimulate safer consumer choices in their purchasing decisions. Similarly, this exemption would allow for greater collaboration between news reporters and security researchers to investigate safety of code that runs critical systems and popular consumer products.

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

Without robust security research the market fails to incorporate accurate information regarding quality of security in products. Companies that invest in information security would be rewarded if this exemption is granted. This market information deficit on security quality undervalues companies that invest in security and overvalues those that do not.

(v) any other factor that may be appropriate for the Librarian to consider in evaluating the proposed exemption.

[9] See e.g., Short Form Comment of Prof. Salvatore Stolfo, Columbia University; Short Form Comment of Prof. Brown et. al., Oxford University

Granting this exemption would enable security research into products particularly designed for children. For example, child diabetics are particularly dependent on insulin pumps that may contain code flaws.[10]

Item 8. Documentary Evidence

Because of the legal ambiguities that exist around Section 1201 with respect to security research, we, the Security Researchers have not performed the following specific acts of research, which have been foregone or delayed due to the lack of the current proposed exemption. In each case, the security research at issue is critical to the safety and privacy of consumers, as well as the security of our economy and our country. Delay in performing this research has been caused directly by our fear of legal consequences under the Section 1201 of the DMCA.

- Potential backdoors in popular consumer programs and other privacy invading features. Such backdoors – unpublished remote access features included by design but not controllable by the user - would enable a remote attacker to engage in undisclosed and undetected privacy invasions of consumers. A backdoor could allow a malicious attacker to remotely turn on webcams and microphones on computers and other devices to monitor consumers' conversations and activities inside their homes. Similarly, a backdoor could allow for an attacker to control the speakers of a device to project harassing messages. Child predators could use backdoors to control a system and, for example, communicate with children through devices in their rooms at times when parents were not present. Additionally, this type of vulnerability would compromise the privacy of all of a consumers' financial, health and other personal data stored on the machine or device.

- Various vulnerabilities in cars: Cars contain millions of lines of computer code and are increasingly controlled by software. Vehicles now also contain a wide range of wireless and other communication mechanisms that expose this software to inputs from potentially a wide range of potentially remote and malicious sources. The consequences of security vulnerabilities in these systems can be dramatic and deadly, including loss of control over acceleration, braking, steering and other critical safety functions.

- Various vulnerabilities in Internet of Things products: As the Internet of Things increasingly permeates the lives of consumers and connected devices become omnipresent, devices expose consumers to new types of risks, including death due to device malfunction. For example, internet connected smoke alarms and carbon monoxide detectors present health risk.[11]

- Various vulnerabilities in connected surveillance cameras. Connected surveillance cameras allow third party attackers on servers, privately operated through the internet. In

[10] See, e.g., Short Form Comment of Jay Radcliffe, Senior Security Consultant, Rapid7
[11] See, e.g., Short Form Comment of Mark Stanislav, Senior Security Consultant and Researcher, Rapid7

this way, an attacker could blind cameras to commit crime both inside homes and inside government and commercial buildings.

- Various vulnerabilities in public safety communications. Analysis of software and firmware in two way secure public safety communications will find methods – attackers could disable, monitor or interfere with sensitive public safety and national security communications systems, such as those used by state and local law enforcement agencies, federal law enforcement, counterintelligence and executive protective security agencies

- Evaluation of security of hardware and software cryptographic modules used in financial services. Cryptographic modules are used to protect a wide range of commercial financial transactions, including ATS, card payment systems, and mobile payment platforms. Flaws, malfunctions or vulnerabilities could result in financial losses for both consumers and business entities. In a large attack, defects in cryptographic modules could severely harm or even destabilize a portion of the U.S. economy or corrupt stock market transactions.

- Evaluation of hardware and software cryptographic modules used to protect access controlled data and integrity in government and commercial computing and information systems. Any agency, government contractor or other company that transfers or protects sensitive data connected to network systems is at risk of information harm due to possible defects in these cryptographic modules.

- Analysis of electronic and computerized systems used in physical security applications such as mechanical locks, "smart" locks, safes and vaults and alarm systems. Physical security devices prevent attackers from intruding in physical space.

- Analysis of electronic voting systems. Electronic voting machines and the systems used to configure them and count votes are subject to manipulation and a wide of possible attacks. Flaws in these systems have obvious implications for the democratic process and discovery of weaknesses permits vulnerabilities to be repaired or procedural safeguards implemented to prevent their exploitation.[12]

- Analysis of code in medical devices. Flaws in code in medical devices may result in death or serious injury.

ISO 29147 and ISO 30111, the standards referenced in the proposed exemption, provide a floor of corporate conduct that embodies security practices already implemented at responsible corporate entities. Hinging an exemption on these standards assists in creating a logical balance between information security and intellectual property protection for responsible corporate entities.

[12] See e.g. Short Form Comment of Verified Voting