U.S. Department of Justice

Criminal Division

Computer Crime and Intellectual Property Section *Washington, D.C. 20530*

June 28, 2018

Regan Smith
General Counsel and Associate Register of Copyrights
Library of Congress
Copyright Office
101 Independence Avenue, SE
Washington, DC 20559-6000

Dear Ms. Smith:

The Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice's Criminal Division submits these comments as part of the Copyright Office's Notice of Proposed Rulemaking (NPRM), its seventh triennial rulemaking proceeding under the Digital Millennium Copyright Act (DMCA).[1] More specifically, CCIPS offers these comments in response to the proposed Class 10 exemption for circumventions in connection with good-faith security research, and the petition ("petition") submitted by Professors Ed Felten and J. Alex Halderman ("petitioners") to expand the exemption for good-faith security research (the "petition"). [2] The following comments borrow the petitioners' terminology for purposes of clarity and provide CCIPS's views on several of the limitations the petitioners seeks to remove.

[1] Library of Congress, Copyright Office, Notice of Proposed Rulemaking, Exemptions to Permit Circumventions of Access Controls on Copyrighted Works, 82 Fed. Reg. 49,550, 49,555 (Oct. 26, 2017) ("NPRM").

[2] Comments of Profs. Felten and Halderman, (Dec. 19, 2017), https://www.copyright.gov/1201/2018/comments-121817/class10/class-10-initialcomments-felten-halderman.pdf The petition proposes to remove the specific security research categories listed under 37 CFR § 201.40(b)(7)(i)(A)–(C), as well as to remove five other limitations, which the NPRM describes as follows:

1. the ''lawfully acquired device or machine'' limitation;
2. the ''solely'' limitation (i.e., "solely for the purpose of good-faith security research'');
3. the ''not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986'' limitation;
4. the ''carried out in a controlled environment designed to avoid any harm to individuals or the public'' limitation; and
5. the requirement that ''information derived from the activity . . . is not used or maintained in a manner that facilitates copyright infringement.''

In their petition, the proponents categorize the limitations they propose to remove as the Device Limitation, the Controlled Environment Limitation, the Other Laws Limitation, the Access Limitation, and the Use Limitation.

Many of the changes sought in the petition appear likely to promote productive cybersecurity research, and CCIPS supports them, subject to the limitations discussed below.

The Department of Justice and the DMCA

As the federal government's primary law enforcement entity, the Department of Justice has a number of distinct interests with respect to the DMCA and computer security research. First, the Department is responsible for enforcement of the DMCA's criminal provision (17 U.S.C. § 1204), which provides significant penalties for violations of the anti-circumvention provisions in Section 1201, when committed willfully and for purposes of commercial advantage or private financial gain. Prosecutors in CCIPS and in many United States Attorneys' Offices around the country have brought criminal DMCA charges in a variety of cases, including "cracking" of access controls on commercial business software and trafficking in "mod chips" for circumventing technological protection measures on video game consoles.

Even so, CCIPS recognizes that that not all efforts to circumvent technological protection measures are illegitimate. In addition to the exemptions granted by the Copyright Office as part of the rulemaking process (for example, to permit circumventions involving literary works in electronic form for use with adaptive technologies for the visually impaired), the statute itself contains several express exemptions that permit, for example, circumventions by non-profit libraries or education institutions in connection with certain archival activities, or as part of reverse engineering for the purposes of developing interoperable products. Law enforcement agencies, including the Department of Justice, also benefit from an express exemption for legally-authorized criminal investigation activities—for example, to access a password-protected device containing electronic data relevant to a criminal investigation pursuant to a court order. To the extent that circumvention of such protections by criminal investigators may implicate the DMCA, Section 1201(e) provides an express exemption for legally-authorized criminal investigation activities, as well as intelligence and relevant government conduct.

Promotion and Regulation of Security Research

In addition to its responsibility for prosecution of criminal DMCA case, the Department is responsible for prosecution of unauthorized intrusions into computers, damage to information systems, and other related offenses under the Computer Fraud and Abuse Act (CFAA) and other statutes. In 2014, CCIPS also created a Cybersecurity Unit to focus on cybersecurity issues, which include promoting better computer security practices, improving responses to data breaches, and increasing awareness of security vulnerabilities. This work provides the Department with an in-depth understanding of the damage that can result from exploitation or manipulation of software and devices and influences our efforts to proactively prevent such crimes. It also informs CCIPS's support for legitimate security research and its appreciation of how such research benefits the public by identifying errors and vulnerabilities in software, digital devices and networks, developing solutions to fix them, and preventing them from being exploited by criminals.

Some comments opposing removal of any existing limitation on the security research exemption suggest, implicitly or explicitly, that the DMCA's security research exemption itself

poses a danger merely because it fails to prohibit a type of research to which the commenter objects. However, the purpose of the DMCA is to provide legal protection for technological protection measures, ultimately to protect the exclusive rights protected by copyright. As critically important as the integrity of voting machines or the safety of motorized land vehicles are the American public, the DMCA was not created to protect either interest, and is ill-suited to do so. To the extent such devices now contain copyrighted works protected by technological protection measures, the DMCA serves to protect those embedded works. However, the DMCA is not the sole nor even the primary legal protection preventing malicious tampering with such devices, or otherwise defining the contours of appropriate research. The fact that malicious tampering with certain devices or works could cause serious harm is reason to maintain legal prohibitions against such tampering, but not necessarily to try to mirror all such legal prohibitions within the DMCA's exemptions.

The DMCA's anti-circumvention provisions are only some of many constraints that may affect security research. Computer and network security research is subject to a range of other laws and professional norms as well. Like anyone else, researchers are subject to generally applicable criminal and tort laws that may restrict exploration of computer networks that researchers are not authorized to access. Researchers also face limitations on their use of various types of data, including financial and medical records. Researchers affiliated with professional organizations and academic institutions generally must also abide by additional guidelines. Such laws and regulations are additional controls on the exercise of security research.

As reflected in the comments below, CCIPS would support the removal of at least some of the current limitations contained in the DMCA's exemption for good faith security research. However, CCIPS regards the phrase "good faith" as meaningful in this context. Security research conducted in bad faith—for example, for the purpose of discovering security holes in software in order to exploit them for illicit financial gain rather than to improve security generally, or to extort the owners of such devices or the data within them—might be called "research," but is not in good faith. Merely labeling conduct "security research" should not be a basis for avoiding criminal or civil liability for circumvention of technological protection measures for purposes of infringement or similar bad faith conduct.

Device Limitation

The petition recommends eliminating language in the current exemption that limits its application to research conducted on three specific classes of devices:

(A) A device or machine primarily designed for use by individual consumers (including voting machines);

(B) A motorized land vehicle; or

(C) A medical device designed for whole or partial implantation in patients or a corresponding personal monitoring system, that is not and will not be used by patients or for patient care.

37 C.F.R. § 201.40(b)(7)(i)(A)–(C). The petition refers to these limitations collectively as the "Device Limitation."

CCIPS recognizes the importance of security research with regard to all three classes of devices identified in subsections (A) through (C), including the specific classes of device mentioned (voting machines, motorized land vehicles, and medical devices). However, CCIPS shares the concern raised by petitioners that the phrase in subsection A, "primarily designed for use by individual consumers," is amenable to different interpretations, and may not provide the degree of certainty necessary for prospective security researchers to be reasonably sure that their activities will be exempted. Based on the range of other comments offered on this language, it appears there is little agreement as to what the phrase includes. It is unclear, for example, whether the limitation is intended to include equipment such as elevators or large-scale lighting, HVAC, or surveillance equipment with which individual consumers may interact, but which is typically purchased and operated by building engineers or other professionals.

Further, it is unclear what rationale there may be for limiting the security research exemption to devices (apart from land vehicles or medical devices) "primarily designed for use by individuals," since such a limitation would seem to unnecessarily exclude valuable security research conducted on many classes of devices that, although arguably not "primarily designed for use by individuals," may nevertheless greatly *affect* individuals. Both consumer-operated, network-enabled home appliances (often associated with the "internet of things") and industrial-grade network routing and switching equipment can contain security vulnerabilities that can pose threats to data security, critical infrastructure, and public safety. CCIPS has investigated and prosecuted cases involving exploitation of vulnerabilities in both classes of equipment. In some cases, vulnerabilities contained in industrial grade servers or networking equipment may present even greater risks to the public than security flaws in consumer goods, highlighting the importance of legitimate security research on such devices. Accordingly, CCIPS supports making clear the research exemption would permit security research on devices regardless of whether they are primarily designed for use by individuals.

<u>Controlled Environment Limitation</u>

CCIPS understands the rationale behind the Controlled Environment Limitation, and agrees that in general, all computer security research should be conducted in a manner and under conditions that minimize the risk of harm to the public. Nevertheless, CCIPS recommends the clarification of this limitation and would not object to its removal. In light of the variety of other legal mechanisms that encourage responsible research methods and constrain harmful conduct, the DMCA's anti-circumvention provisions are not the most effective or appropriate vehicle for addressing concerns about security research methods.

CCIPS shares the concerns of petitioners that in its current form, the language of the Controlled Environment Limitation could be construed to suggest that, in order to fit within the exemption, security research must be conducted in a lab-like setting or other environment isolated from the public. Although such a tightly-controlled environment might be necessary for certain types of research that present especially serious risks of harm, isolated lab-like settings are not required in every instance of security research, and we agree with petitioners that in some

circumstances effective research may require experiments to be conducted in realistic conditions in the field. We believe reducing the risk of harm to the public is critically important, especially with regard to subject matter with obvious and significant safety implications such as motorized vehicles. But in some cases, minimizing the risk of harm may require "real world" testing outside of a lab-like controlled environment. Therefore, we believe it would beneficial to clarify that, although exempted security research need not always be conducted in a laboratory setting, it must be conducted with reasonable consideration for risks of harm, or under conditions reasonably calculated to minimize risks to the public.

Other Laws Limitation

The petition recommends removal of language in the current security research exemption that requires that a circumvention be performed only on a "lawfully acquired" device or machine and that the circumvention not violate "any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986…." The petition refers to this language collectively as the "Other Laws Limitation," but CCIPS regards the "lawfully acquired" language and the "any applicable law…" language somewhat differently.

Although the term "lawfully acquired" is not itself ambiguous, and CCIPS does not read the term in this context to require that researcher obtain formal title in a copy of software, CCIPS recognizes the petitioners' concern that this limitation could be read to exclude research on devices where ownership of the device is subject to restrictive licensing terms, or is disputed, or even where the device is merely owned by a third-party but never "acquired" by the researcher. Where good-faith security research is not itself infringing (e.g., because it does reproduce or otherwise violate exclusive rights in elements protected by copyright, or because the research falls within a statutory exception or is a permissible fair use), the question of whether such research is permissible under the DMCA should not turn on restrictive contractual terms purporting to limit use of the hardware on which the copyrighted software is running. However, given the sharply divergent views expressed by commenters on the relationships and distinctions among ownership, licensing, and possession of a particular copy of software (see., e.g., Joint Creators II Class 10 Long Comment at 4 n.1, 9 n.6; Consumers Union, Class 10 Long Comment at 2), CCIPS views the "lawfully acquired" language as less restrictive than, and preferable to, alternative limitations that would predicate permission to conduct research on ownership or formal acquisition of title in a particular copy of software or other work.

With regard to the "any applicable law" limitation, CCIPS agrees with the Register's observation in its 1201 Policy Study that this limitation may have little effect on the scope of permissible research because "other laws still apply even if the activity is permitted under section 1201." (1201 Policy Study (June 2017) at 80.) As noted above, CCIPS also does not view the anti-circumvention provisions as the most appropriate or efficient means of imposing limits on security research beyond the scope of the copyright-related goals underlying the DMCA. Accordingly, CCIPS recognizes that the reference to "any applicable law" does not change what is or is not permitted under other laws and, therefore, would not object to the removal of this phrase from the exemption, were it standing alone.

However, security research involving circumvention of technological measures protecting copyrighted works can frequently also involve circumventing technical barriers to attempt to gain access to computers or network resources, which can implicate the CFAA. Given the interplay and occasionally overlapping application of the DMCA and the CFAA, CCIPS cannot support removal of the reference to the CFAA in the Class 10 exemption. To do so might mislead researchers into believing that operating within the DMCA exemption would also provide an exemption from CFAA liability, which it does not. To avoid confusion that could place security researchers in legal jeopardy, we support retaining the express reference to the CFAA within the exemption.

Conclusion

CCIPS appreciates the opportunity to provide our views as part of the Copyright Office's seventh triennial rulemaking proceeding under the DMCA. The Class 10 exemptions are an effective component of efforts to improve the security of devices and technology. It is important to strike the right balance between encouraging security research conducted in good faith and safeguarding protections for copyrighted materials. CCIPS believes the views expressed herein accomplish that goal.

Sincerely,

/s/

John T. Lynch. Jr.
Chief