Before the

U.S. COPYRIGHT OFFICE, LIBRARY OF CONGRESS

In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. Section 1201

Docket No. 2014-07

Reply Comments

1. Commenters

Professor Candice Hoke, Cleveland State University*
Professor Douglas W. Jones, University of Iowa*
Professor Deirdre Mulligan, University of California, Berkeley*
Professor Vern Paxson, University of California, Berkeley*
Professor Pamela Samuelson, University of California, Berkeley*
Bruce Schneier
Erik Stallman, Center for Democracy & Technology (CDT)

* Affiliation for identification purposes only

Contact person: Erik Stallman, CDT, (202) 407-8817, estallman@cdt.org

2. Proposed Class Addressed

These reply comments address Proposed Class 25: Software – Security Research.

3. Overview

In past Section 1201 proceedings, the Copyright Office has stated that its primary focus is on whether access control measures have diminished or will diminish the ability to engage in lawful uses of copyrighted works that the public traditionally would have been able to make prior to enactment of the Digital Millennium Copyright Act (DMCA).[1] The majority of arguments that opponents raise in their comments have nothing to do with this question. Instead, they focus on vehicle safety, battery life, and supply chain integrity. These issues are both outside the

[1] Recommendation of the Register of Copyrights in RM 2005-11; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies at 8 (Nov. 17, 2006), *available at* http://www.copyright.gov/1201/docs/1201_recommendation.pdf .

scope of the Office's expertise and subject to regulatory regimes overseen by other agencies. Focusing squarely on the question that has guided past proceedings, Class 25 petitioners and proponents have adequately demonstrated that the adverse effect of anti-circumvention liability on good faith security research outweighs alleged harms to the owners of copyrighted works. The importance of security research and the disclosure of research results increases with the proliferation of "smart" devices and our reliance on them. Although good faith security research is a lawful, noninfringing use of copyrighted works, the existing statutory exemption under Section 1201(j) is insufficient to guide or protect researchers. Accordingly, the Librarian of Congress should grant the Class 25 exemption.

4. Asserted Noninfringing Uses

a. The Harms Asserted by Opponents Have Little or No Relation to Copyright Interests

As the Office stated in the current Notice of Proposed Rulemaking, "the primary responsibility of the Register and the Librarian in this rulemaking is to assess whether the implementation of access controls impairs the ability of individuals to make noninfringing use of copyrighted works within the meaning of 1201(a)(1)."[2] This focus flows directly from the language and intent of Section 1201. The enumerated statutory factors under 1201(a)(1)(C) focus on the availability of, market for, and value of copyrighted works.[3] The House Manager's Report explaining the Section 1201 inquiry and process clarified that "the rulemaking proceedings should consider the positive as well as the adverse effects of [technological protection measures] *on the availability of copyrighted materials*."[4]

The majority of concerns raised by opponents of the Class 25 exemption have nothing to do with the stated goals of this proceeding. General Motors and the Alliance of Automobile Manufacturers ("Auto Alliance") suggest that permitting unauthorized security research of software embedded in vehicles presents "significant safety and security challenges."[5] Similarly, the Advanced Medical Technology Association ("AdvaMed") contends that a security research exemption

[2] Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Notice of Inquiry*, 79 Fed. Reg. 55687, 55688 (Sept. 17, 2014).

[3] 17 U.S.C. §1201(a)(1)(C). The statute does permit the Librarian of Congress to consider "other factors" deemed appropriate. However, the focus at all times remains on copyright interests.

[4] Staff of House Comm. On the Judiciary, 105th Cong. *Section by Section Analysis of H.R. 2281 as passed by the United States House of Representatives on August 4, 1998*, at 6 (Comm. Print 1998).

[5] Comment of General Motors at 2 ("GM Comments").

that would permit security researchers to circumvent technological protection measures ("TPMs") controlling access to software in medical devices would drain battery life and potentially harm the safety and privacy of users of those devices.[6] AdvaMed also raises concerns with health care costs, supply chain integrity, and the "litigious nature of society."[7] As discussed below, research into potential vulnerabilities of critical devices and networks enhances the overall safety of those devices. As a general matter, however, CDT and security researchers agree with LifeScience Alley that "the Copyright Office is not the forum in which to address these possible issues."[8]

Similarly, concerns about "regulatory landscape[s]"[9] unrelated to copyright interests fall outside the proper scope of this proceeding. Opponents cite the Clean Air Act, the Motor Vehicle Safety Act, and standards administered by the Food and Drug Administration among the reasons why a security research exemption is unwarranted.[10] While independent security research can play a critical role in ensuring that certain devices comply with applicable laws and regulations,[11] enforcing compliance with those laws and regulations ultimately rests with the expert agencies, not the Librarian of Congress.

A few opponents of the security research exemption recast safety and regulatory concerns as copyright interests. For example, General Motors contends that increased vehicle safety and security challenges "directly and negatively impact the value of the copyrighted work."[12] However, that impact depends on the possibility that a researcher might circumvent TPMs and then publish vehicle firmware code that "may be used by bad actors for intentional malicious reasons or by benign hobbyists for purposes which could create inadvertent risks to safety, security and regulatory compliance."[13] Those risks might harm the value of the vehicle, but not the market for, or value or availability of the firmware that comes with it. Opponents have failed to articulate a harm to their *copyright* interests that

[6] Comment of Advanced Medical Technology Association at 2-3 ("AdvaMed Comments").
[7] AdvaMed Comments at 5.
[8] Comment of LifeScience Alley at 3.
[9] GM Comment at 7.
[10] *Id*. at 6-7; AdvaMed Comments at 3.
[11] *See* Class 22 Comment of Electronic Frontier Foundation at 17 & n.113 ("EFF Comments")(citing a letter from United States Senator Ed Markey criticizing automobile manufacturers for "dismissing vulnerability found by DARPA-funded researchers").
[12] GM Comments at 12.
[13] *Id*.

outweighs the substantial adverse effects anti-circumvention liability places on security research and researchers.[14]

b. Security Research Is Noninfringing Fair Use Regardless of Whether That Research Focuses on Technological Protection Measures or the Protected Work

The Copyright Office has previously applied the statutory factors under Section 107 to security research and concluded that such research is fair use.[15] Opponents of a security research exemption here contend that the Office's reasoning is limited only to "security vulnerabilities *caused by access controls*."[16] This limitation is unwarranted.

Purpose and character of use. Whether a security researcher is investigating a vulnerability in a protected work or the TPM protecting that work, the purpose is research, a use expressly recognized in the preamble to Section 107.[17] "Like all of the activities listed in the preamble of Section 107, it involves a broader socially productive activity."[18] In addition, use of copyrighted works in security research accomplishes a wholly different purpose than that served by the original work and is therefore a transformative use.[19] Because security researchers' use of copyrighted works is transformative, this factor weighs strongly in favor of fair use.

Nature of the copyrighted work. General Motors describes vehicle software as a "highly creative work" designed by "specialized engineers."[20] The Office reached a similar conclusion with respect to the video games at issue in the 2010 security

[14] *See Lexmark Int'l, Inc. v. Static Control Components, Inc.,* 387 F.3d 522, 545 (6th Cir. 2004) (holding that the lower court erred in focusing on the market for toner cartridges rather than the market for the "Toner Loading Program" accessed by circumvention of a TPM).

[15] 2010 Recommendation at 186 (concluding that "[t]he socially productive purpose of investigating security and informing the public do not involve use of the creative aspects of the work and are unlikely to have an adverse effect on the market for or value of the copyrighted work itself" and that "[o]verall, the factors tend to strongly support a finding of fair use in this context.").

[16] Auto Alliance at 3 (emphasis in original).

[17] 17 U.S.C. § 107.

[18] 2010 Recommendation at 184.

[19] *See Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1164-67 (9th Cir. 2011) ("A work is transformative when the new work does not merely supersede the objects of the original creation but rather adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message.") (internal quotation marks omitted).

[20] GM Comments at 10.

research exemption. Nonetheless, the Office stated that the "security research at issue here focuses on the functionality, rendering the creative aspects of the video games irrelevant."[21] In both cases, the research involves "functional works entitled to lesser consideration."[22] Because researchers are concerned with the functional, rather than the creative, aspects of a work, this factor weighs in favor of fair use.

Amount and substantiality of the portion used. The Office's 2010 Recommendation recognized that in the course of security research, the entire work may be reproduced but concluded that "[g]iven likely nonexistent use of the copyrighted work in any results the researchers provide to the public, this factor tends to weigh in favor of fair use."[23] Here, the distinction between research on TPMs and on the underlying works may heighten the likelihood that some functional elements of the work appear in research results. However, the reproduction of the expressive elements of a protected work in security research results is likely to be small, limited to the part of the software that makes the system vulnerable to cyberattack. Accordingly, this factor should be given little weight, especially when copying the entire work is necessary for research purposes.[24]

Effect on the market for the copyrighted work. The Office's 2010 Recommendation concluded that "good faith research would be unlikely to adversely affect the potential market for or value of a work in a manner cognizable under the Copyright Act."[25] That conclusion flowed from two considerations. First, the researcher had to lawfully obtain a copy of the work, therefore having no direct effect on the market for that work. Here, where Auto Alliance argues that even if one purchases an automobile, she does not own the firmware that comes with it,[26] it is unclear what market for the copyrighted work is affected by her – or a researcher – studying that work to uncover vulnerabilities.[27] Second, the 2010 Recommendation observed that unfavorable or critical research findings "would not

[21] 2010 Recommendation at 185.

[22] *Id*. (citing *Sega Enters. Ltd. V. Accolade, Inc.*, 977 F.2d 1510, 1524 (9th Cir. 1992)).

[23] *Id*.

[24] *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596, 606 (9th Cir. 2000) (giving "very little weight" to this factor when use required an intermediate copy of the entire work but the final product did not contain infringing material).

[25] 2010 Recommendation at 186.

[26] Auto Alliance Comments at 4.

[27] Even if the owners of protected works provided a means for a user or researcher to request permission to access that work, the failure to request such permission would not be fatal to a finding of fair use. *See Campbell v. Acuff-Rose Music*, 510 U.S. 569, 585 n.18 (1994) ("if a use is otherwise fair, then no permission need be sought or granted").

be relevant harm to Section 106 rights."[28] Further, research that fails to uncover vulnerabilities enhances the value of the work.[29]

With the possible exception of the third factor, all statutory factors weigh in favor of finding that security research is fair use regardless of whether that research is conducted on a TPM or the protected work.

5. Adverse Effects

a. Petitioners and Supporting Commenters Have Demonstrated That Section 1201's Prohibition of Circumvention of TPMs Has a Substantial Adverse Effect on Security Research

Security researchers have put forward substantial evidence showing that the DMCA's anti-circumvention prohibition subjects them to legal risk and discourages both academic institutions and government entities from funding critical security research.[30] Opponents counter that anecdotal evidence and individual cases are insufficient to satisfy petitioners' evidentiary burden.[31] While a petitioner must show a distinct and verifiable impact of a prohibition on lawful activity, she need not show that she either is or imminently will be subject to liability. As the Office explained in its 2010 Recommendation, Section 1201 "requires only that the proponents prove that the prohibition causes more than an insubstantial adverse effect on noninfringing uses."[32] Proponents of a research exemption have done so here.

[28] 2010 Recommendation at 186.

[29] *Id.*

[30] *See, e.g.,* Comment of Dr. Matthew D. Green at 18 & n.57 ("Green Comments") (discussing a vendor's letters to researchers, their employers, and conference organizers to discourage further research or disclosures related to digital watermarking technologies); Comment of Jay Radcliffe at 1 (discussing advice of counsel to forego further research into certain medical devices); Comments of Mark Stanislav at 1 (discussing inability to perform research into web cameras and Internet-connected children's toys); Comments of Dr. Salvatore J. Stolfo at 1 (discussing the need to "alter and . . . methodologically weaken the proposals that I have submitted to government funding agencies").

[31] GM Comments at 14; Comment of BSA| The Software Alliance at 2 ("BSA Comments").

[32] Recommendation of the Register of Copyrights in RM 2008–8, Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (June 11, 2010) ("2010 Recommendation"), *available at* http://www.copyright.gov/1201/2010/initialed-registers- recommendation-june-11-2010.pdf.

Auto Alliance reads the 2010 exemption to mean that researchers must identify a vulnerability before a security research exemption is appropriate.[33] This requirement would result in an almost entirely useless exemption as a researcher would first have to violate the DMCA's anti-circumvention provision in order to obtain sufficient evidence to secure an exemption from it. Furthermore, given that "technology in these fields evolves quickly[,]" the three-year cycle of the exemption process could mean that a vulnerability-specific exemption would be irrelevant by the time it was granted.[34] To the extent that the 2010 exemption requires more than "suspicion" or "speculation" of a security vulnerability,[35] proponents meet that standard here. As Professor Green explained, "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 cyberattacks and an increase of over 60% in cyber-breaches relative to previous years."[36] In view of the growing pervasiveness of cybersecurity threats, a general exemption is necessary to mitigate Section 1201's adverse effects on good faith security research. According to the 35 noted researchers and academics who have submitted the statement attached to these comments, "[a]s the urgency of the cybersecurity threat has grown, the inhibiting effect of these laws [including Section 1201] has also grown."[37] Researchers, academic institutions, funders, and publishers currently face barriers performing, supporting, and disclosing security research in critical areas.[38]

Opponents separately argue that Section 1201 has no substantial adverse effect on security research because the owners of protected works partner with third-party researchers to investigate and resolve security vulnerabilities.[39] For example, LifeScience Alley discusses the work that the Department of Homeland Security and its Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) perform in concert with industry stakeholders.[40] Although these efforts are to be commended, they are in themselves insufficient because the owners of protected works may choose to hide potential vulnerabilities uncovered by research they

[33] Comment of The Alliance of Automobile Manufacturers at 8 ("Auto Alliance Comments").

[34] *See* Comment of Prof. Steven M. Bellovin, et al. at 3 ("Security Researchers Comments").

[35] 2010 Recommendation at 187-88.

[36] Green Comments at 4 & n.3 (citing Symantec Corporation, Internet Security Threat Report 19 (2014), a*vailable at* https://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19 _21291018.en-us.pdf).

[37] "Statement on Legal Impediments to Cybersecurity Research," May 1, 2015, at 3 (attached to these comments as Appendix A).

[38] *Id*. at 4.

[39] GM Comments at 13.

[40] LifeScience Alley Comments at 3.

control or they may fail to address those vulnerabilities with expediency. Last year, ICS-CERT issued an advisory with respect to certain vulnerabilities because a vendor had "decided not to resolve these vulnerabilities because of compatibility reasons with existing engineering tools."[41] That inaction "places critical infrastructure asset owners using this product at risk."[42] Moreover, these arrangements provide no protection for independent or "accidental" researchers who discover a vulnerability but have no means to disclose it without potentially subjecting themselves to liability under Section 1201.

b. Section 1201(j) Provides Insufficient Guidance or Protection for Security Researchers

The petitioners and proponents for the Class 25 exemption are motivated in large part by the insufficiency of Section 1201(j) to foster and protect good faith security research. Far from "reasonable constraints" on that research,[43] 1201(j)'s limiting factors leave researchers and the institutions that fund their efforts no meaningful safe harbor for performing essential security research.

Especially with the growing number of networked devices, the requirement that the researcher seek out and receive "the authorization of the owner or operator of such computer, computer system, or computer network" may be impossible to comply with. In many instances, those owners will resist investigation and disclosures of vulnerabilities that may cast the owner in a negative light.[44] Often, determining whose authorization must be secured may be impossible. Assuming that a vehicle owner is not the owner of the software that comes with it, who may authorize the research into embedded software or networked components? Is the owner of the vehicle the "operator" of the software? Is the software owner's permission sufficient to perform research that may disclose a vulnerability of a network to which the vehicle connects? Congress likely did not contemplate these difficulties when enacting the statutory exemption. Imposing such a requirement unreasonably restricts non-infringing uses of copyrighted works.

Similarly, the reference in 1201(j)(2) to "applicable law other than this section," expressly including the Computer Fraud and Abuse Act (CFAA),[45] imports ambiguities in those statutes into the question of liability under the Copyright Act.

[41] ICS-CERT Advisory (ICSA-14-084-01), *available at* https://ics-cert.us-cert.gov/advisories/ICSA-14-084-01.
[42] *Id*.
[43] *Id.* at 2.
[44] Green Comments at 18 (discussing Texas Instruments' attempts to block disclosure of vulnerabilities with its Data Storage Tag by contacting the researchers' universities).
[45] 18 U.S.C. § 1030.

Depending on the relevant device or system, security research may raise unanswered questions under the Wiretap Act,[46] the Stored Communications Act,[47] or the Pen Registers and Trap and Trace Devices statute.[48] Dealing with just the CFAA, a researcher's liability for violating terms of use may depend on the particular jurisdiction in which she performs her research. Section 1201(j) compounds the risk and uncertainty a researcher faces when dealing with unsettled areas of the law.

Section 1201(j)(3)(A)'s limitation of permissible security testing to uses "solely to promote the security of the owner or operator of such computer, computer system or computer network" or shared directly with the developer also unduly constrains the freedom to perform and disclose research. In arguing for Section 1201(j)'s scope of permissible testing, BSA cites the DMCA Conference Report's analogy to testing a door lock:

> a prospective buyer may test the lock at the store with the store's consent, or may purchase the lock and test it at home in any manner he or she sees fit . . . *What that person may not do, however, is test the lock once it has been installed on someone else's door, without the consent of the person whose property is protected by the lock*.[49]

The problem with this analogy is that with the proliferation of software-enabled or networked devices, the person whose property, safety, or privacy is protected by the lock may not be able to authorize testing it. Security researchers and all of us who depend on their work need a clearer answer than Section 1201(j) provides.

6. Statutory Factors

BSA correctly observes that the most important factor under Section 1201 is "the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, and research."[50] That is precisely why the Class 25 exemption should be granted. Even while allowing that some research may be beneficial, opponents are expressly seeking to limit public disclosure and discussion of that research. For example, AdvaMed expresses concern that "publicity related to accessing a patient's medical devices creates fear in the public and in the patient because they worry that

[46] 18 U.S.C. § 2510 et seq.
[47] 18 U.S.C. § 2701 et seq.
[48] 18 U.S.C. § 3121 et seq.
[49] BSA Comments at 4-5 (quoting H. R. Rep. No. 105–796, at 67 (1998) (Conf. Rep.)) (BSA's emphasis).
[50] *Id*. at 5 (quoting 17 U.S.C. §1201(a)(1)(C)((iii)).

their device will be accessed or controlled."[51] But if the device is insecure, patients should be fearful, and the copyright law should not be used to limit criticism, comment or news reporting about those insecurities.

In many instances, the lack of disclosure itself becomes a security vulnerability. As security expert Bruce Schneier has observed, "[s]mart security engineers open their systems to public scrutiny, because that's how they improve."[52] The National Institute of Standards and Technology agrees that security of information technology systems "should not depend on the secrecy of the implementation or its components."[53] We agree with BSA's contention that the Copyright Office neither is nor should be "the arbiter of what a responsible software company's policies and practices should be."[54] But neither should the Office nor rightsholders dictate when research should be conducted or disclosed. Without a robust security research exemption, any person performing research in the open is at risk of uncertain and possibly catastrophic liability under Section 1201.

7. Documentary Evidence

"Statement on Legal Impediments to Cybersecurity Research," attached to these comments as Appendix A.

8. Conclusion

For the reasons above, the Librarian of Congress should grant the Class 25 exemption for security research.

[51] AdvaMed Comments at 6. *See also* GM Comments at 7 (expressing concern that "online dialogue will only increase").

[52] Bruce Schneier, "The Insecurity of Secret IT Systems," Schneier on Security, Feb. 14, 2014, *available at* https://www.schneier.com/blog/archives/2014/02/the_insecurity_2.html.

[53] National Institute of Standards and Technology, *Guide to General Server Security*, Special Publication 800-123, at 2-4, *available at* http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf. *See also* EFF Comments at 9.

[54] BSA Comments at 4.

APPENDIX A

Statement on Legal Impediments to Cybersecurity Research
May 1, 2015

Cybersecurity is an urgent national priority. Vulnerabilities in a wide range of digital devices, systems, and products, including critical infrastructures, can and have been exploited to undermine national security, economic prosperity, and personal privacy. The rapid emergence of the Internet of Things heightens the risk, as consumer products widely used in daily life, ranging from automobiles to medical devices to thermostats and home appliances, become connected to the Internet and thus vulnerable to remote manipulation, exploitation, and attack. The growing complexity and interdependencies among devices and networks compounds the risks, making it increasingly important to assess, and address, vulnerabilities in technically and socially complex real world settings.

In this environment, cybersecurity research is vital. Security by obscurity – the notion that vulnerabilities can be kept hidden from adversaries – has failed in the past and is particularly poorly suited to today's interconnected environment.

Corporate, governmental, academic, and independent cybersecurity researchers all contribute to identifying and remediating cybersecurity vulnerabilities. However, there are serious legal impediments today to cybersecurity research. The Digital Millennium Copyright Act, the Computer Fraud and Abuse Act, and the web of statutes amended by the Electronic Communications Privacy Act all impose uncertain and potentially catastrophic liability on good-faith security research and the disclosure of security vulnerabilities. We, the undersigned, warn of the negative impact of these impediments, and we urge policymakers to address and mitigate them.

Even in the face of these barriers, cybersecurity research has advanced the security, trustworthiness, and resilience of systems ranging from cyberphysical, to voting systems, to medical devices. It has benefited human health and safety, protected democratic self-governance, and shored up systems essential to the economic and physical wellbeing of the nation. Much further positive work could be done if the legal barriers to research were lowered.

Three examples highlight the value of research conducted under the cloud of legal uncertainty:

Research on automobiles: Modern automobiles are becoming increasingly computerized — with many components controlled partially or entirely by computers and networked both internally and externally. While this architecture provides many benefits, the risks have not been carefully considered or addressed by the automotive industry. University researchers and others have begun to examine these risks, yielding important findings. They have showed that existing automobiles are extremely fragile to attack and empirically demonstrating that a range of vectors (including dealership shop tools, media players, Bluetooth and cellular telematics connections) all can be used to compromise even safety critical components (e.g., remotely disabling the brakes).[1] This was research that was not being pursued by the automotive industry, involved extensive reverse engineering of automotive systems and has had major positive concrete impacts for the public. Among the visible side effects of this work include the establishment of a new cybersecurity standards effort undertaken by the Society of Automotive Engineers, a cyber security testing and evaluation capability being created by the Department of Transportation's National Highway and Traffic Safety Administration (NHTSA), a $60M research program created by DARPA (HACMS) to develop new technologies to increase vehicle security, a pending Senate bill soon to be introduced regulating automotive cybersecurity and significant automotive industry investment in cybersecurity. (For example, Eric Gassenfeit, OnStar's chief information security has been publicly quoted as saying that his team has had its resources and staff grow "by an order of magnitude" in the period after the publication of this research.[2]) All of these benefits accrued only because the researchers took risks that they should not have to take.

Research on voting machines identified significant vulnerabilities in the technical systems upon which the most fundamental act of our democracy relies. Election officials lack the expertise to analyze these systems, federal and state standards failed to deliver sound security, and yet, researcher access was limited by contracts that prohibited most forms of testing, as well as reverse engineering. But for cybersecurity researchers willing to take risks, the investment of the National Science Foundation, and the diligence of a handful of Secretaries of State, the public would have remained unaware of the vulnerabilities in these systems, and election officials would have been unable to seek fixes to mitigate risks of election fraud and failure.[3] The majority of voting system vendors were hostile to independent security analysis of their systems, and went to great lengths to prevent election officials and

[1] S. Checkoway et al., "Comprehensive Experimental Analyses of Automotive Attack Surfaces," USENIX Security, August 2011, available at http://www.autosec.org/publications.html.

[2] Keith Barry, "Can Your Car be Hacked?" Car and Driver (July 2011) http://www.caranddriver.com/features/can-your-car-be-hacked-feature.

[3] See Virginia Information Technologies Agency, "Security Assessment of WinVote Voting Equipment for Department of Elections," April 14, 2015, http://elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf.

researchers from independently examining them. The work of security researchers led to the decertification of insecure voting systems, the adoption of new policies, procedures, and technologies, new methods of oversight and certification of machines, and improved training for election workers. Internet voting, which is now being promoted, deserves similar security research, but that research may be impeded by the laws mentioned above.

Medical device security researchers have uncovered fundamental flaws in devices such as pharmaceutical drug compounders, automated external defibrillators, ventilators, drug infusion pumps, and implantable medical devices. Very few medical device companies have security engineering teams. Independent security researchers have taken the risk to publish security flaws in the public interest. In general, medical device engineers sincerely care about helping patients live longer and healthier lives. The devices save countless lives. However, the majority of medical device manufacturers lack the level of cybersecurity engineering maturity found in the information technology and finance sectors. Thus, medical device manufacturers often respond with hostility during a first encounter with a security researcher. The existing laws give companies unnecessary means of recourse that do not protect patients from the most prevalent cybersecurity threats; the laws only serve to chill research on medical device security.

In other sectors as well, multiple security advancements in the marketplace are the product of, or informed by, cybersecurity research. The benefit of independent cybersecurity research is also underscored by the fact that numerous companies have started their own or joined collaborative “bug bounty” programs aimed at fueling adversarial research on their systems. These programs literally pay researchers to hack into systems and identify vulnerabilities, because companies view external testing by security experts as essential to maintaining a strong security posture.

However, legal barriers remain and are even increasing. The legal impediments to cybersecurity research arise from various sources, including the Computer Fraud and Abuse Act, section 1201 of the Digital Millennium Copyright Act, and the wiretap laws. The impediments also arise from contracts and terms-of-service (the breach of which may expose one to criminal liability) that broadly prohibit modifications of devices or collections of data. As the urgency of the cybersecurity threat has grown, the inhibiting effect of these laws has also grown. Meanwhile, contractual prohibitions on reverse engineering have proliferated. New categories—such as “sensitive security information”—have entered the legal lexicon,[4] statutes have been broadly interpreted, and technical protections have

[4] Originally created to limit what TSA, airline and airport personnel could say about air travel security measures, the category “sensitive security information” has expanded in scope over time to cover virtually the entire transportation sector and, moreover, there is

been added to an array of consumer products to limit tinkering and modification. While there are arguments that the laws at issue would not be used to actually prosecute legitimate cybersecurity research, the laws are ambiguous and can be broadly interpreted, generating uncertainty that has a wide chilling effect.

The chilling effect of these barriers takes many forms: Academic and other research institutions can be risk-averse, advising faculty and students to steer clear of research with unclear liability; faculty advise students to work in areas less fraught with potential legal and public-relations challenges; and peer review may look unfavorably upon researchers whose work treads too closely to legal lines[5]. Funders may be reluctant to support certain kinds of research. Academic publication venues are forced to wrestle with questions regarding the legality of research, despite its public value. Papers have been both delayed and outright pulled due to court intervention, threats of suit by research subjects, and program committee concerns with potential liability exposure for the committee, the institution, or the venue.[6] Independent researchers face an outsized threat of criminal prosecution and civil litigation. Researchers at corporations face a chill as well, because the questionable legality of certain security research may raise an appearance of impropriety if another company's technology is the subject of analysis.

In light of these concerns, we recommend that:

- The Copyright Office should endorse the security research exemptions that have been proposed in the current triennial review.

- The US Department of Justice, in order to narrow the possibility of prosecution for cybersecurity research aimed at improving the security of devices or of our nation's Internet systems, should issue guidance clarifying the government's interest in promoting cybersecurity research and describing practices that will not be subject to prosecution.

an ever growing set of trigger conditions spread across many different laws that make one subject to restrictions applicable to it.

[5] Edward Felten, "The Chilling Effects of the DMCA," Slate (March 29, 2013) http://www.slate.com/articles/technology/future_tense/2013/03/dmca_chilling_effects_how_copyright_law_hurts_security_research.html. See generally EFF, "Unintended Consequences: Twelve Years under the DMCA" (March 2010) https://www.eff.org/wp/unintended-consequences-under-dmca.

[6] See, for example, MBTA v. Anderson, where three students at MIT were sued by the Massachusetts Bay Transit Authority and forced to cancel a scheduled conference presentation. Court filings available at https://www.eff.org/cases/mbta-v-anderson.

- University general counsels and other university officials should defend cybersecurity research, including by assisting university researchers to thread their way through the maze of laws.

- Vendors and other entities in a position to correct cybersecurity vulnerabilities should adopt procedures, such as those recommended in ISO standards, to receive and respond to reports of vulnerabilities.

- Congress should amend laws that impede cybersecurity research to make it clear that those laws do not prohibit research intended to improve the security of devices or of our nation's Internet systems and infrastructure.

Ben Adida, VP Engineering, Clever Inc.
Jacob Appelbaum, The Tor Project
Ruzena Bajcsy, NEC professor, Electrical Engineering and Computer Sciences, University of California, Berkeley
Kevin Bankston, Policy Director, New America's Open Technology Institute
Steven M. Bellovin, Professor, Computer Science, Columbia University
Eric Burger, Research Professor, Computer Science, Georgetown University
L. Jean Camp, Professor of Informatics, Indiana University
Nicolas Christin, Assistant Research Professor, Electrical and Computer Engineering, Carnegie Mellon University
Donald E. Eastlake 3rd, network engineer
Timothy H. Edgar, Visiting Fellow, Watson Institute, Brown University
David Evans, Professor, Computer Science, University of Virginia
Bryan Ford, Associate Professor, Computer Science, Yale University
Kevin Fu, Associate Professor, Electrical Engineering and Computer Science, University of Michigan
Jennifer Stisa Granick, Director of Civil Liberties, Stanford Center for Internet and Society
Joseph Lorenzo Hall, Chief Technologist, Center for Democracy & Technology
Nadia Heninger, Magerman Term Assistant Professor, Computer and Information Science, University of Pennsylvania
Richard Kemmerer, Professor, Computer Science, University of California, Santa Barbara
Susan Landau, Professor of Cybersecurity Policy, Worcester Polytechnic Institute
Sascha Meinrath, Director, X-Lab
Sigurd Meldal, Director, Silicon Valley Big Data and Cybersecurity Center, San Jose State University
Katie Moussouris, HackerOne
Deirdre K. Mulligan, Associate Professor, School of Information, University of California, Berkeley
Vern Paxson, Professor, Electrical Engineering and Computer Sciences, University of

California, Berkeley
Ron Rivest, Vannevar Bush Professor, Massachusetts Institute of Technology
Avi Rubin, Professor, Computer Science, Technical Director, Information Security Institute, Johns Hopkins University
Pamela Samuelson, Richard M. Sherman Distinguished Professor of Law, University of California, Berkeley
Stefan Savage, Professor, Computer Science, University of California, San Diego
John E. Savage, An Wang Professor of Computer Science, Brown University
Bruce Schneier, cryptography and security researcher
Micah Sherr, Assistant Professor, Computer Science, Georgetown University
Barbara Simons, IBM Research (retired)
Janos Sztipanovits, E. Bronson Ingram Distinguished Professor of Engineering, Vanderbilt University
David Wagner, Professor of Computer Science, University of California, Berkeley
Nicholas Weaver, staff researcher, International Computer Science Institute, University of California, Berkeley
Stephen Wicker, Professor of Electrical and Computer Engineering, Cornell University

Affiliations for identification purposes only.