# 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. 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

After reviewing the comments in prior rounds, we offer the following amended and restated version of our proposed exemption:

" 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 Reasonable Vulnerability Management Practices; or (2) the finder of the malfunction, security flaw or vulnerability reports the malfunction, security flaw or vulnerability to the copyright holder by providing Vulnerability Replication Information in advance of or concurrently with public dissemination of the security research.

For purposes of this exemption,

Reasonable Vulnerability Management Practices shall be defined as the following requirements, which mirror those appearing in ISO 29147 and 30111:

1. Creation and prominent publication of a publicly viewable corporate vulnerability disclosure policy on the corporate website.
2. Creation and prominent display of a prominent internet "front door" – clear instructions for submitting external vulnerability reports to the company on the corporate website.

3. Creation of an internal corporate vulnerability management handling process which designates responsible individual(s) for (1) intake, handling, monitoring of public sources for vulnerability information and (2) external finder communications, who possess(es) adequate corporate authority to bind the company in its promises to finders.
4. Acknowledgement of all external reports of malfunctions, security flaws or vulnerabilities within seven calendar days of a finder's submission.

Vulnerability Replication Information shall be defined as the following items, which mirror those in Annex A of ISO 29147:

1. a basic summary that includes (a) a technical description, (b) the finder's contact information, (c) a description of any public disclosure plans known as of the day of alerting the copyright holder to the vulnerability, (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."

--

Opponents' objections to the language of the proposed exemption were as follows:

1. Opponents allege that the closed, proprietary nature of the ISO was an obstacle to researchers' ability to assess a company's compliance.

Opponents pointed to the closed nature of the ISO standards as an obstacle to their use by both the Copyright Office and researchers seeking to use the exemption. To wit, we have addressed this objection through identifying and explaining the requirements of reasonable vulnerability management practices for purposes of this exemption request. These articulated requirements mirror those of the two ISO standards that were referenced by the Security Researchers as a touchstone for the original iteration of this exemption request.[1]

[1] That said, Opponents erred when they asserted that researchers would be unable to ascertain whether an entity is ISO compliant for purposes of this exemption. As stated above, the most basic requirement of the ISO standards in question is that a company must offer a conspicuously marked "front door" point of reporting security vulnerabilities through its corporate website. If a researcher accesses a corporate website and no such obvious reporting mechanism exists, the researcher has actual knowledge that the company is not ISO compliant. For example, using the members of the BSA as listed on http://www.bsa.org/about-bsa/bsa-members as a sample, a review of members' corporate websites demonstrates that a majority of members are not ISO compliant. While Microsoft, Oracle, Adobe and Siemens offer "front doors" on their websites, the websites of the remaining BSA members appear to lack this information. Therefore, a researcher would assume that those four members with "front doors" are likely ISO compliant, with the remainder unlikely to be ISO compliant. That said, this exercise is now functionally moot, as our amended and restated exemption request clarifies this basic component of Reasonable Vulnerability Management expressly.

2. Opponents assert that the exemption allegedly empowers the Copyright Office, an office they erroneously allege to lack expertise on matters of digital copyrightable works, to set corporate information security policy.

Opponents assert that the Copyright Office should not be the arbiter of software policies. However, the DMCA has already placed the Copyright Office squarely in this role; this is not a new role driven by our exemption request. That said, the Security Researchers sought to avoid imposing undue burden on the Copyright Office by suggesting the mirroring of a standard crafted by an internationally-recognized standards body, whose standards are already widely in use across both government and industry. The substance of the two touchstone ISO standards mirrored in part by the language of our exemption were constructed through a collaborative 8 year process among numerous multinational industry participants, government bodies and other interested parties, including some member entities of Opponent BSA.[2]

3. Opponents allege the definition of a "security researcher" covered by the exemption is unclear.

While Opponents assert that the definition of a "security researcher" is unclear, this asserted definitional issue is entirely irrelevant with respect to our exemption request. Although we use the term "researcher" in our comments, the exemption is carefully worded to be exclusively conduct-based. Anyone whose conduct conforms to the specifications of the exemption can appropriately assert it. Anyone whose conduct does not conform to the specifications of the exemption -- regardless of job title -- does not qualify as a person covered by the exemption. A conduct-based framing acknowledges an important reality of information security in practice: many finders of sophisticated vulnerabilities are sole proprietors, entrepreneurs, technologists with non-security expertise or students of various fields of computer science. A conduct-based

[2] ISO participants in the U.S. proposals included, among others, the following companies, departments, and agencies: Alcatel-Lucent International, Amazon Web Services Inc, Atsec Information Security Corporation, Booz Allen & Hamilton Inc CERT Coordination Center Cigital Inc., Cisco Systems Inc., Department of Commerce – NIST, EMC Corporation, Futurewei Technologies Inc., Gemalto, General Electric, HackerOne, Hewlett-Packard Company, Hitachi Data Systems, Intel Corporation, International Association of Privacy Professionals (IAPP), International Council on System Engineering (INCOSE), Kantara Initiative, Lexmark International Microsoft Corporation, NetApp Inc, Oracle, Plum Hall Inc, Raytheon Company, Ricoh Corporation, Salesforce.com, SecureRF Corporation, The Open Group, Unified Compliance Framework, United States Dept of Defense, United States Dept of Defense – NSA, United States Dept of Homeland Security, Utilities Telecom Council, VHA CHIO, WidePoint Corporation,Yaana Technologies, Zygma LLC. A number of Opponent BSA entities are named in this list. Indeed, it was BSA member, Microsoft, which dedicated significant time of an employee, Katie Massouris, to lead the crafting of one of the referenced standards and collaborate on the other. As such, undoubtedly these BSA companies believed that spending corporate resources on participation in ISO standard-setting was a fruitful enterprise. It seems, therefore, inconsistent, that BSA is advocating to undercut modeling a Class 25 exemption on the international standard its members worked hard to create. The two current lead drafters of the ISO standards in question, Katie Massouris (HackerOne) and Art Manion (CERT) have expressed their willingness to advocate for making the touchstone ISO standards publicly available.

exemption allows for the exemption's use by the full spectrum of possible flaw finders, provided they comply with its requirements.

4. Opponents allege the proposal lacks adequate safeguards.

Some Opponents argue that the proposal lacks safeguards and permits researchers to never disclose discovered problems to the author of the code.[3] This interpretation constitutes a misreading of the plain language of our exemption request: the exemption provides that if a researcher chooses to publicly disclose uncovered flaws or vulnerabilities in code, the researcher must previously or concurrently disclose to the copyright holder, provided that the copyright holder is compliant with the basic requirements of Reasonable Vulnerability Management. Other Opponents object to the absence of a concrete lockup period in the timing of disclosure, and they instead propose a radical new approach that takes the current requirements of Section 1201 and evolve them into an even more draconian regime.[4] This approach does not improve the current security research climate, and it inappropriately replaces the Congressional intent embodied in Section 1201 with Opponents' business interests. In this way, these Opponents appear to contradict their own arguments that Congress was amply clear in its drafting of Section 1201.[5] This argument also ignores Congress's clear intent to empower consumers to defend their data privacy and security in Section 1201(i), analyzing the functioning of code to verify privacy/security behaviors without needing the permission of the copyright holder.

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

The comments of several Opponents reflect confusion regarding the basics of security research and the technological impact of the proposed exemption. These inaccuracies asserted in Opponents' comments include the following:

1. Opponents assert that the exemption allegedly sanctions the "corruption" of devices by researchers.[6]

Opponents mischaracterize the nature of security research: security researchers do not corrupt devices. They identify preexisting coding errors that were not caught and corrected by the copyright holder when these errors can result in detrimental consequences. If no code flaws or vulnerabilities are present in a product as created by the copyright holder, the product's code cannot potentially cause malfunction or harm. In other words, security researchers do not rewrite existing code.

2. Opponents assert that the exemption allegedly sanctions Frankenstein-like experimentation by security researchers on humans wearing medical devices.

[3] Comments of The Advanced Medical Technology Association; Comments of BSA
[4] Comments of BSA
[5] Comments of SIIA
[6] Comments of The Advanced Medical Technology Association

Citing no references and providing no actual examples, Opponents paint an offensively inaccurate image of security researchers testing devices on living patients, and, for instance, running out the batteries of existing patients' pacemakers.[7] To the Security Researchers' knowledge, there has never been a case where a security researcher has tested a device while the device was being worn by a third party living patient. In addition to using outdated statistics regarding the capacity of devices and battery life,[8] Opponents again significantly mischaracterize the basics of security research. Security research on devices such as medical devices happens in controlled environments to maintain rigor in the investigation. Testing a device while worn by a live patient would potentially constitute a criminal act and would never be approved by a university IRB Board. Tellingly, Opponents provided no facts to support their entirely fictional fear mongering.

## Item 5. Asserted Noninfringing Use(s)

Item 5 of the First Round Comments of the Security Researchers is incorporated by reference.

## Item 6. Asserted Adverse Effects

Adverse effects asserted by Opponents include the following:

1. Opponents assert that "the Proposed Exemption enables public discourse."

Opponent GM has asserted that an adverse effect of the proposed exemption would be "enabling public discourse" regarding software and product safety.[9] The Security Researchers enthusiastically stipulate that the granting of this exemption would indeed significantly enrich and further public discourse on information security in our society. It would also lead to the creation of numerous new copyrightable works as a consequence. We do not, however, characterize public discourse stimulation and the consequential outpouring of copyrightable creativity as an "adverse effect." Instead, we view a vigorous public discourse in writing around software safety as highly desirable: this exemption seeks to further creation of new copyrightable works, stimulate high quality code innovation, and encourage citizen involvement in concern for our national information security.[10]

While Opponents may find security researchers' First Amendment-protected speech[11] about the safety of the code in their products to be inconvenient for business, this speech triggers information security improvements in our society and stimulates creation of new copyrightable

[7] Comments of The Advanced Medical Technology Association
[8] Comments of The Intellectual Property Owners Association.
Compare http://www.mayoclinic.org/tests-procedures/pacemaker/basics/results/prc-20014279
[9] Comments of GM
[10] As one of the Security Researchers testified before Congress recently, the state of information security deficiencies in our society is reaching national crisis levels.
[11] For a discussion of the First Amendment limits of security vulnerability disclosures, see Andrea M. Matwyshyn, Hacking Speech: Informational Speech and the First Amendment, 107 Nw. U. L. Rev. 795 (2013).

works. Each time a copyright holder issues a patch for its software as a result of a researcher alerting it to a flaw, the copyright holder creates a new copyrightable work. Each researcher's article disclosing a newly-discovered vulnerability or flaw in a category of products or a particular product results in a copyrightable work. Each blog post, news article, comparative analysis, white paper or video recorded by journalists and even by the public comparing products on software safety based on new research constitutes the creation of a new copyrightable work. Each new product that enters the marketplace seeking to compete on the basis of software security is a copyrightable work. This exemption and the public discourse it would enable to which Opponents object will unquestionably stimulate a cornucopia of new copyrightable works.

2. Opponents assert that the exemption will allegedly result in creating fear and panic that devices are not safe.

This business concern regarding Opponents' marketing challenges and brand image devaluation as a result of unpatched errors in their code is not a copyright concern. Unpatched software vulnerabilities and flawed code can, in fact, result in serious threats to human life in some cases. Fear of information security failures in consumer products leading to harms is not irrational. For example, one senior citizen has, according to a jury, already died due to software malfunction in a car.[12]

3. Opponents assert that the exemption will allegedly facilitate infringement.

Opponents' allegations that infringement and an unquantified loss of intellectual property will somehow result from the requested exemption are inconsistent with the plain language of the requested exemption. Security researchers test code; they do not copy and republish code in full. Opponents have cited no case and can provide no factual support for the assertion that security research has ever led to an instance of intellectual property theft or loss. Further, the researcher in any such hypothetical theft scenario would not qualify for the proposed DMCA exemption – theft of intellectual property does not constitute good faith security testing.

Opponents state that the correct inquiry for the Copyright Office to ask is whether users would be more secure if access controls were simply removed?[13] We assert the answer is an unequivocal yes. If access controls were removed from the works at issue, no DMCA barrier would exist to security researchers' investigating the extent of flaws in code. The currently chilled security research climate would improve dramatically. Researchers would be more comfortable with notifying companies of dangerous errors and publishing the results of their research, thereby stimulating the creation of secondary copyrightable works, such as comparative consumer safety reports and articles.

[12] http://www.eetimes.com/document.asp?doc_id=1319903

[13] Comments of The Alliance of Automobile Manufacturers ("A simple test illustrates the difference: would users of the systems in question (personal computers, in 2006 and 2010; cars, today) be more secure if the access controls in question were simply removed and discarded? The Register's answer in the earlier proceedings was clearly yes; but no proponent has asserted that the answer is yes with regard to this proceeding.")

4. Opponents assert that the exemption allegedly sanctions the release of patches by security researchers.

Opponents allege that the exemption request sanctions security researchers' release of patches that correct code errors in products.[14] Again, Opponents appear to lack rudimentary knowledge of the work of security researchers. Security researchers do not release patches; they report vulnerabilities to companies, in order to assist the company in releasing a fix. Opponents provide no citations or factual support for the patently false assertion that security researchers release patches.

5. Opponents assert that the exemption allegedly negatively impacts innovation because it would increase liability, costs of recalls and reporting, and the expense of stronger access controls

These allegedly innovation-driven concerns – possible liability, cost of recalls, cost of reporting, and expense of stronger access controls – are not copyright concerns. These are business concerns of the type that the Copyright Office is traditionally loathe to consider. Opponents correctly point out that "in past rulemaking cycles, the Copyright Office has been unreceptive to objections to proposed exemptions that it perceives to be motivated by harms to "business interests" rather than "copyright interests.""[15] But, let us assume purely for the sake of argument that new, stronger access controls would be created by copyright owners. Those new access controls constitute additional copyrightable works. Thus, Opponents implicitly concede that the exemption positively impacts innovation through stimulating creation of numerous additional copyrightable works that simultaneously make the public and our country safer and informed.

6. Opponents assert that the exemption would encourage allegedly pointless duplicative testing, and adequate security testing is allegedly already happening inside entities.

Duplicative code testing is, first and foremost, again a business issue and not a copyright question. However, the Security Researchers will take this opportunity to point out that if Opponents believe duplicative testing offers no benefits to them because rigorous internal security testing is already detecting and correcting all code errors in their products, their opposition to this exemption request seems illogical. If Opponents believe, as they assert, that their products are fully vetted with respect to information security, the Copyright Office's grant of this exemption should prove entirely unobjectionable to them. Presumably, researchers will find the Opponents' products to be flawless, and Opponents will, therefore, never need to interact with researchers or contend with the exemption.

Opponents boldly state that no data exists to show that security improvements happen based on outside research.[16] That factually inaccurate assertion is, most charitably construed, indicative of Opponents' lack of working knowledge of the basics of information security. Sophisticated technology companies, such as the members of the Internet Association, who are supporters of

[14] Comments of The Intellectual Property Owners Association
[15] Comments of The Alliance of Automobile Manufacturers
[16] Comment of The Advanced Medical Technology Association

this exemption request,[17] have long known that duplicative testing done by external parties is the only way to build safer code into products. In fact, entities confident in the quality of their products believe in the importance of redundant testing to such a great extent that they now run their own "bug bounty" programs, using financial incentives to entice outside security researchers to "break" their products in order to provide feedback for the purpose of product improvement.[18] A fledgling industry even exists around facilitating these research relationships between outside researchers and such companies.[19] For example, Google has paid out over $4 million in bug bounties to third party security researchers,[20] Facebook has spent over $1 million,[21] and Microsoft has awarded over $500,000 in bug bounties to security researchers.[22] These payouts are driven by corporate interest in developing and delivering secure products and an understanding that independent security researchers are a resource that assists in improving their products' information security. In fact, some companies have recognized the looming legal threats of the DMCA and other statutes that chill security researchers by issuing public statements of cooperation, publicly promising not to use the DMCA and other causes of action against researchers who report vulnerabilities to them.[23] Sophisticated companies who are ready to stand behind the quality of the code in their products embrace external security research.

7. Opponents assert that the exemption will allegedly adversely impact various non-copyright statutory regimes including the Computer Fraud and Abuse Act, privacy laws, the FDA, the EPA, DHS, NTSA and others, as well as allegedly interfere in doctor-patient relationships.

Opponents attempt to divert the Copyright Office's attention from the DMCA and copyright concerns. Providing no copyright-related caselaw, agency statements or any factual evidence of any kind to support their assertions, Opponents allege a litany of fabricated regulatory concerns unrelated to copyright, yet somehow allegedly implicated by this DMCA exemption request. The requested exemption solely involves a copyright question -- whether security researchers are protected from suit under the DMCA under certain circumstances when an act of security research may have allegedly circumvented a TPM.

This exemption request in no way adversely impacts any of the numerous other legal frameworks referenced by the Opponents. If the exemption request is granted, copyright holders retain all non-DMCA recourse options against security researchers and all regulatory obligations under every other legal regime. In other words, recourse under the Copyright Act and the CFAA, as well as manufacturers' obligations to other government agencies such as the FDA would be

[17] http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_InternetAssociation_Class25.pdf
[18] See, e.g., https://www.google.com/about/appsecurity/chrome-rewards/index.html
[19] HackerOne https://hackerone.com/ and Bugcrowd https://bugcrowd.com/ are examples of such intermediaries.
[20] http://venturebeat.com/2015/01/30/after-paying-over-4m-in-bounties-since-2010-google-expands-program-to-include-its-android-and-ios-apps/
[21] https://www.facebook.com/notes/facebook-security/recent-reports-on-our-whitehat-program/10151538365500766
[22] https://technet.microsoft.com/en-us/security/dn469163.aspx
[23] https://www.facebook.com/whitehat/ ; https://technet.microsoft.com/en-us/security/cc261624.aspx

wholly untouched if the Copyright Office were to grant the Security Researchers' exemption request.

8. Opponents assert that medical devices and cars should be carved out of the exemption.

Opponents have provided no credible rationale explaining why medical devices should be treated differently from all other Internet of Things devices. The argument that the FDA already governs information security in medical devices is both incorrect and not a copyright issue. The FDA does not require medical device manufacturers to test the information security of their products for FDA approval.[24] The FDA has only issued "nonbinding recommendations" relating to information security.[25] Similarly, disclosure by medical device manufacturers on Form MDS2 is entirely optional, and some medical device manufacturers appear to refuse to provide the information to consumers, even in response to direct inquiries about product safety.[26]

Opponents allege that FDA adverse event reporting structures adequately address the copyright concern that the DMCA chills security research.[27] Again, this argument is not based in copyright. Further, FDA adverse event reporting is a closed system, primarily driven by doctor and pharmacist reports – not patient or security researcher reports. Meanwhile, doctors and pharmacists are unlikely to be skilled information security experts qualified to identify cases of patient death and injury due to code malfunction or error.[28] Rather than interfering in doctor-patient relationships, security research simply makes additional safety information available for both doctors and patients as they select among various devices in the market. Security research encourages competition on the basis of good information security in medical devices and the

---

[24] While information security guidance exists, it is optional. Any security testing processes the FDA may require in the future will likely be required for the initial approval process permitting the company to sell the product.

[25] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf; Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication http://www.fda.gov/safety/medwatch/safetyinformation/safetyalertsforhumanmedicalproducts/ucm357090.htm

[26] For example, one consumer's attempts to obtain MDS2 forms resulted in the following exchange:

> Matt [from Boston Scientific] called me back. "We don't have any of those M...[mumbled letters] things. But I can give you some talking points on security for our devices." "Boston Scientific devices include security features that are intended to prevent hacking, specifically, encryption, and a unique key for each programming session." "Can't be done by anything hacking." … "Unlike a computer, a pacemaker doesn't connect to the internet to download code. So it's almost impossible to hack…0 reports ever of security breaches for Boston Scientific…It just doesn't happen." ..No idea what kind of encryption protocols they use, when I asked.

Email from Christina J. DeVries, April 30, 2015.

[27] Comment of LifeScience Alley

[28] RAND Health Research Report: Promoting Patient Safety Through Effective Health Information Technology Risk Management, May 2014, at page 60 (noting limitations on how health IT events are reviewed and reported), avail. at http://www.healthit.gov/sites/default/files/rr654_final_report_5-27-14.pdf (last visited May 1, 2015). Also, adverse event reports are usually not made public by the FDA. Hence, the system does not usually warn other doctors and patients in real time to avoid using the flawed medical devices or provide a public accountability mechanism that ensures that life-threatening security flaws are corrected in medical devices.

creation of additional copyrightable works of both code and product critique by manufacturers, journalists, doctors and patients.

Opponents allege that car companies adequately test the security of the code in their cars, and that cars are "not computers."[29] In fact, cars *are* now computers on wheels – cars frequently run upwards of 100 million lines of code.[30] The positioning of Opponent car manufacturers sits starkly in contrast to the approach to information security of the most technologically sophisticated car manufacturer in the U.S., Tesla Motors. Tesla Motors has not objected to this exemption request. Indeed, the company has a positive relationship with the security research community, requesting vulnerability reports through its website,[31] maintaining a security researcher hall of fame,[32] and a bug bounty program.[33] Unlike Tesla, Opponent GM's website indicates no "front door" for reporting vulnerabilities and a search of the website yields no evidence of a bug bounty program. Opponent The Alliance of Automobile Manufacturers asserts that car company employees attend DEFCON and similar conferences,[34] but a review of recent DEFCON speakers on the DEFCON website does not initially appear to indicate any talks given by employees of car companies other than Tesla.[35] In contrast, Tesla not only brings its cars to the DEFCON conference, asking researchers in attendance to analyze the code on site,[36] but the engineers of Tesla are internationally recognized for their expertise in information security.[37] If the most technologically-sophisticated car company in the U.S. has not objected to our exemption request and welcomes security research with open arms and cash rewards, Opponents are hard-pressed to demonstrate their objections are driven by anything other than concern that their business will need to divert resources from "a valuable and lucrative endeavor"[38] into responding to potentially life-saving security research and patching vulnerable, unsafe code. Again, software malfunctions have already killed passengers in cars, according to at least one jury.[39]

## Item 7. Statutory Factors

None of the Opponents' comments have challenged the Security Researchers' assertion that Section 1201(i) likely encompasses the conduct in the requested exemption. As such, we ask

[29] Comments of GM
[30] http://www.technologyreview.com/view/508231/many-cars-have-a-hundred-million-lines-of-code/
[31] https://www.teslamotors.com/about/legal#security-vulnerability-reporting-policy
[32] https://www.teslamotors.com/about/legal#tesla-security-researcher-hall-of-fame
[33] http://www.forbes.com/sites/thomasbrewster/2014/07/09/10000-is-on-offer-for-anyone-who-can-hack-a-tesla-car/ ; http://www.opptrends.com/2014/08/tesla-motors-inc-tsla-plans-to-hire-hackers-at-defcon/
[34] Comments of The Alliance of Automobile Manufacturers
[35] www.defcon.org
[36] http://www.forbes.com/sites/thomasbrewster/2015/04/28/tesla-opening-car-to-hackers/
[37] For example, Tesla's "Security Princess" Kristin Paget has given multiple talks at leading information security conferences in the recent past and is well-known in the information security community. http://cleantechnica.com/2014/02/18/tesla-motors-snags-kristin-paget-apple/ No GM information security employee holds a similarly high profile among information security professionals to our knowledge.
[38] Comments of GM
[39] http://www.eetimes.com/document.asp?doc_id=1319903

the Copyright Office to construe this lack of Opponents' objections as a stipulation that the Security Researchers' Section 1201(i) argument is meritorious.

It is the position of the Security Researchers that as both researchers and consumers of digital products, they fall cleanly within the Congressional intent articulated for the inclusion of Section 1201(i) in the DMCA.[40] Indeed, as Opponents have stated,[41] Congress crafted the existing provisions of the DMCA carefully and deference to its drafting is appropriate. This drafting included Section 1201(i).

Granting this exemption will stimulate criticism, comment, news reporting, teaching, scholarship, or research on information security – one of the most important social and national security issues of our time. The market for and value of copyrighted works that researchers have found to be well-coded will significantly increase if this exemption is granted.

## Item 8. Documentary Evidence

Opponents have asserted that the current DMCA framework which requires permission for researchers to test the security of products and services functions well and that the burden rests with the Security Researchers to prove a negative – that research was not performed because of fear of legal consequences.[42] If the DMCA works as well as opponents claim, it seems surprising that they have failed to provide evidence of a single documented case where an independent security researcher approached a company asking for permission to test the software safety and received consent. Further, Congress did not include a consent-based regime in Section 1201(i), the section most directly connected with this exemption request.

In contrast, when security researchers have asked for permission to test systems, those requests have been denied, sometimes questioning their research motivations or accusing them of trying to extract free products.[43] Most of these researchers are afraid to come forward due to the risk of legal ramifications. This point regarding reasonable fear of repercussions was succinctly and firmly explained by the numerous supportive comments filed on behalf of the Security Researchers' exemption request by business entities, nonprofits, and the world's leading information security academics, including those of the Internet Association and USACM. All of these comments assert that security research critical to our economic and national security is being lost or damaged due to the restrictions of the DMCA at present.

[40] For a discussion of DMCA Section 1201(i), see Andrea M. Matwyshyn, Technoconsen(t)sus, 85 Wash U. L. Rev. 3 (2007).
[41] Comments of SIIA
[42] Comments of BSA
[43] See, e.g. email from Knud Erik Højgaard, April 10, 2015.