Before the
UNITED STATES COPYRIGHT OFFICE
Library of Congress

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies	))))))	Docket No. 2014-07 Proposed Class 25: Security Research

COMMENTS OF GENERAL MOTORS LLC

General Motors LLC
Harry M. Lightsey III
Jeffrey M. Stefan
25 Massachusetts Avenue, NW
Suite 400
Washington, DC 20001
(202) 775-5039

Hogan Lovells US LLP
Ari Q. Fitzgerald
Anna Kurian Shaw
Lauren Chamblee
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5423
Attorneys for General Motors LLC

March 27, 2015

TABLE OF CONTENTS

Before the
UNITED STATES COPYRIGHT OFFICE
Library of Congress

Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies	)	Docket No. 2014-07
	)	Proposed Class 25: Security Research

COMMENTS OF GENERAL MOTORS LLC

I. SUMMARY OF THE OPPOSITION TO THE PROPOSED EXEMPTION

General Motors LLC ("GM") respectfully submits these comments in response to the Notice of Proposed Rulemaking ("*NPRM*") released by the United States Copyright Office ("Copyright Office") in the above-captioned proceeding.[1] In the *NPRM*, the Copyright Office seeks comment on a number of proposed exemptions to the Digital Millennium Copyright Act's ("DMCA's") prohibition against circumvention of technological protection measures ("TPMs") that control access to copyrighted works.[2]

The Copyright Office should deny the proposed exemption for Class 25. The proposed exemption is overbroad, and the proponents have failed to establish a *prima facie* case that an exemption for Class 25 is or is likely to be noninfringing. The proponents have also failed to establish that the challenged TPMs are causing, or are likely to cause in the next three years, a substantial adverse impact on users. Because the proponents of the exemption have failed to meet their *prima facie* burden, the Copyright Office does not need to examine the relevant statutory factors; however, consideration of those factors also supports a decision to deny the

[1] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Notice of Proposed Rulemaking*, 79 Fed. Reg. 73856 (Dec. 12, 2014) ("*NPRM*").
[2] *NPRM*, 79 Fed. Reg. at 73856.

proposed exemption. Importantly, the proposed exemption presents a host of potential safety, security and regulatory concerns that the proponents have not fully considered. Indeed, proponents such as Dr. Green seem to ignore the fact that when it comes to cars, they are seeking an exemption for circumvention of the very TPMs designed to play an important role in the carefully considered overall safety and security framework within a vehicle and which help to ensure the safety and security of, among other things, the Electronic Control Units ("ECUs") in cars and thus, of the vehicle as a whole. [3] Furthermore, the broad exemption sought would allow dissemination of highly sensitive copyrighted information regarding the functioning and operation of ECUs in cars. [4] Even when such efforts are undertaken by well-intentioned researchers, wider distribution of such information provides access to vehicle software in a way that implicates safety and security concerns. Thus, if granted, the proposed exemption presents significant safety and security challenges.

Proposed Class 25. Various petitioners have submitted petitions and comments in support of an exemption for proposed class 25, which would allow: [5]

[3] *See* Long Comment of Dr. Matthew D. Green Regarding a Proposed Exemption at 2 ("Green Comments").

[4] *See* Green Comments at 12-14.

[5] In addition to Dr. Green, Security Researchers seek an exemption because they take the position that any access control mechanism that potentially exposes the public to risk of harm due to malfunction, security flaws or vulnerabilities is an appropriate subject of research and the proposed exemption would address the current chilling effect on noninfringing uses by eliminating ambiguity regarding whether circumvention of access controls for security research on software is illegal; the SAE International (formerly Society of Automotive Engineers) filed comments taking no position but offering to assist the Copyright Office in its inquiry; combined comments received through the Digital Right to Repair website generally expressed the view that researchers should not be at risk of running afoul of copyright law when testing the safety of computer programs, databases, and devices; and various researcher and academic short comments generally expressed the view that researchers should be able to access copyrighted software for security research and that the prohibition against circumvention has chilling effects on such research. *See* Long Comment of Security Researchers; Long Comment of Stallman et al; Short Comment of the SAE International on behalf of SAE International Vehicle Electrical System Security Committee; various Short Comments submitted by individuals; and various Short Comments submitted through the Digital Right to Repair website.

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.[6]

The Samuelson-Glushko Technology Law & Policy Clinic ("TLPC") on behalf of Dr. Matthew D. Green, PhD ("Dr. Green" or "Proponent") has set forth the most substantive comments, and GM focuses it response on these comments to the extent they concern the circumvention of TPMs in motorized land vehicles. Dr. Green and the other petitioners are collectively referred to herein as "Proponents."

Proponents request an exemption that broadly covers literary works, including computers, databases, and documentation, protected by TPMs "that control access to work, for the purpose of finding, fixing, and disclosing security vulnerabilities, flaws, or malfunctions, commenting on or criticizing such vulnerabilities, flaws, or malfunctions, or engaging in scholarship and teaching about such vulnerabilities, flaws, or malfunctions, including where the technological protection measures control access to other works, such as graphic works, audiovisual works, and sound recordings, when the research cannot be performed without accessing the other works" ("Proposed Exemption").[7]

The Proposed Exemption seeks to allow researchers to engage in security research which includes 1) researching and discovering security flaws and vulnerabilities, 2) alerting consumers and notifying companies of security flaws and vulnerabilities, 3) providing students with valuable learning opportunity to gain hands-on experience by working on a real system, 4) contributing to the academic publications and discussions of software and device security and 5)

[6] Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Notice of Proposed Rulemaking*, 79 Fed. Reg. 73856, 73870 (2014).
[7] Green Comments at 3.

applying research discoveries to fix vulnerabilities or build new, more secure software and devices.[8]

Dr. Green acknowledges that software controls our cars and "[t]he security of modern software and the devices that execute this software is thus of paramount importance for both the security of our nation and the security of our lives."[9] However, the Proposed Exemption would also cover the public distribution of security research findings, which as written, would include findings related to code in vehicle ECUs that control critical safety and security systems and systems that comply with mandatory regulations. These systems control engine functions, braking, speed, steering and airbags, among other functions. [10] Vehicle ECUs are designed to be operated as built by the automobile manufacturers, and not to be modified by circumventing TPMs. TPMs are part of a complex security and safety structure which prevent access to highly sensitive vehicle software and ECUs. Operating vehicle ECUs as built is important to protect vehicle safety and security, and for compliance with regulations. Thus, the circumvention of TPMs and widespread distribution of code relating to ECUs could have an impact automobile safety, security and regulatory landscape.

For these reasons, the Copyright Office should deny the Proposed Exemption.

II. INTRODUCTION

A. GM's Interest in this Rulemaking

GM, its affiliates and their joint ventures manufacture vehicles in 30 countries, and the company is a leader in the world's largest and fastest-growing automotive markets. GM, its

[8] Green Comments at 11.
[9] Green Comments at 3-4.
[10] *See* Green Comments at 13; http://www.ni.com/white-paper/3312/en/

affiliates and their joint ventures sell vehicles under the Chevrolet, Cadillac, Baojun, Buick, GMC, Holden, Jiefang, Opel, Vauxhall and Wuling brands. OnStar, LLC ("OnStar") is an affiliate of GM that provides in-vehicle connected safety, security and mobility telematics solutions and advanced information technology, which are available on almost all of GM's U.S. vehicles. OnStar's suite of services include automatic crash response, stolen vehicle assistance, remote door unlock, turn-by-turn navigation, vehicle diagnostics, hands-free calling and 4G LTE wireless connectivity.[11]

GM urges the Copyright Office to carefully consider the potential inadvertent risks to vehicle safety and security, if the Proposed Exemption is granted. As detailed below, TPMs play a critical role in ensuring the safety and security, as well as the regulatory compliance of the modern car. Allowing circumvention of such TPMs has consequences in these areas.

B. The Purpose of TPMs in the Modern Car

The Role of TPMs in GM Vehicles and the Risks Presented by Circumvention. Today's automobiles include, on average, 30 purpose-built ECUs with functions that range from controlling the radio to regulating vital engine and safety functions.[12] Many of these systems are critical to the vehicle and security and compliance with mandatory federal vehicle regulations. Automobile manufacturers ("OEMs") employ TPMs in vehicles to help protect them from tampering and hacking. The type of TPM used depends on the availability of the evolving technology and the type of control system involved.[13]

[11] More information on GM and its affiliates, including OnStar, can be found at http://www.gm.com.
[12] *See* http://www.nytimes.com/2010/02/05/technology/05electronics.html; http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code
[13] Examples of TPMs used by GM include seed/key access control mechanisms, firmware signing, and sensitive data encryption.

The security that protects the software operating on vehicle's ECU is ever more important in today's interconnected world. Vehicle ECUs are connected by networks that enable interaction between various systems, and, for telematics-equipped vehicles, various remote features. The software operating each ECU is carefully calibrated to ensure the safe and secure operation of the vehicle. In vehicles with connected telematics systems, ECUs are interconnected via vehicle networks that enable various remote features. For example, interconnected OnStar services include system diagnostics, and security features such as Remote Door Unlock, Remote Ignition Block and Stolen Vehicle Slowdown.[14] GM engineers use TPMs to make these systems safe and secure. Circumvention of TPMs increases access to, and as noted by Proponents, *publication* of sensitive information relating to the operation of ECUs which in turn increases the risks to safety and security and other systems that an owner trusts – the risks that the TPMs were specifically designed to mitigate. Thus, the Proposed Exemption weakens a vehicle's carefully designed safety and security framework of which TPMs are an integral part and accordingly increases the vehicle safety and security challenges.

TPMs also ensure that vehicles meet federally mandated safety and emissions standards. For example, circumvention of certain emissions-oriented TPMs, such as seed/key access control mechanisms, could be a violation of federal law. Notably, the Clean Air Act ("CAA") prohibits "tampering" with vehicles or vehicle engines once they have been certified in a certain configuration by the Environmental Protection Agency ("EPA") for introduction into U.S. commerce.[15] "Tampering" includes "rendering inoperative" integrated design elements to

[14] Remote Door Unlock enables OnStar to open a vehicle's doors without a key. Remote Ignition Block allows OnStar to send a remote signal to block the engine of a vehicle that has been reported stolen from starting. Stolen Vehicle Slowdown sends a signal that gradually slows down a stolen vehicle, enabling police to apprehend the individual who stole it. *See* OnStar Services, *available at* https://www.onstar.com/us/en/services/services.html.
[15] 42 U.S.C. § 7522(a).

modify vehicle and/or engine performance without complying with emissions regulations.[16] In addition, the Motor Vehicle Safety Act ("MVSA") prohibits the introduction into U.S. commerce of vehicles that do not comply with the Federal Motor Vehicle Safety Standards, and prohibits manufacturers, dealers, distributors, or motor vehicle repair businesses from knowingly making inoperative any part of a device or element of design installed on or in a motor vehicle in compliance with an applicable motor vehicle standard.[17] The disclosure of information relating to the ECUs controlling functions relating to fuel consumption and emissions threatens to undermine this regulatory landscape.

Even now, hackers as well as more benign car enthusiasts and hobbyists share modifications online and this online dialogue will only increase if an exemption is granted that furthers this discussion and provides access to information that can present a risk to vehicle safety and regulatory compliance.[18] All of this affects the overall security of a vehicle and could threaten safety and regulatory compliance as well as the value of and continued availability on the market for certain vehicle software.

Alternatives to Circumvention of TPMs in GM Vehicles. GM understands the value and importance of security research and identifying security vulnerabilities within the automotive industry. However, unlike in a cell phone or computer, ECUs in vehicles control the functioning of automobiles with passengers on public roads. While GM and other OEMs undertake great efforts to ensure that these ECUs are secured, the Proposed Exemption enables public discourse of the operation of these ECUs and creates a myriad of possible safety risks. GM does, however,

[16] 42 U.S.C. § 7522(a).
[17] 49 U.S.C. §§ 30112(a)(1), 30122(b).
[18] *See e.g.*, Car Hacker's Handbook available at http://opengarages.org/handbook/, http://boingboing.net/2014/07/16/car-hackers-handbook.html (Car Hacker's Handbook is an example of a set of instructions shared among hobbyists that a hobbyist might follow to make a modification or repair which could negatively impact or damage the safety systems in a vehicle.)

strongly encourage research for security and safety purposes, but within a controlled environment that does not present such risks. Therefore, GM, and other car manufacturers, partner with third party researchers to identify and address security vulnerabilities. In fact, it is quite common for automobile manufacturers to contract with third party testers and researchers for work on various parts of the vehicle. These arrangements can be open to public participation, such as in standard-setting organizations, or can be restricted when confidential information, such as the detailed operation of TPMs and ECUs, is required for appropriate research or evaluation.

In view of 1) Proponents' failure to establish a *prima facie* case for the Proposed Exemption as detailed below; 2) the potential risks to vehicle safety and security; and 3) the potential risks to the U.S. regulatory systems designed to protect vehicle safety and the environment, GM respectfully submits that the Proposed Exemption should be denied.

III. PETITIONERS HAVE FAILED TO MAKE OUT A PRIMA FACIE CASE IN SUPPORT OF THE EXEMPTION

The Proponents have failed to meet the burden of establishing a *prima facie* case in support of the Proposed Exemption. Pursuant to 17 U.S.C. 1201(a)(1)(C), Proponents of an exemption from the prohibition on circumvention bear the burden of establishing that "persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition . . . in their ability to make non-infringing uses . . . of a particular class of copyrighted works."[19] Thus, to establish a *prima facie* case for the proposed class, Proponents must demonstrate that 1) the uses affected by the prohibition on circumvention are or are likely to be noninfringing and 2) the prohibition is causing, or in the next three years is

[19] Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Notice of Inquiry*, 79 Fed. Reg. 55687, 55689 (2014) ("2014 NOI").

likely to cause, a substantial adverse impact on those uses.[20] The proponents "must prove by a preponderance of the evidence that the harm alleged is more likely than not." [21]

A. Exemption Proponents Have Failed to Establish that the Uses Affected by the Prohibition on Circumvention are Noninfringing

Neither Dr. Green, nor the other Proponents, have demonstrated that the uses for which they seek an exemption are noninfringing under 17 U.S.C. § 107. Further, Proponents must demonstrate that the affected use is or is likely noninfringing, not merely *plausibly or conceivably* noninfringing and "there is no 'rule of doubt' favoring an exemption when it is unclear that a particular use is a fair use."[22] Given this framework for evaluating whether the uses are affected and the broad category of uses covered by the Proposed Exemption, Proponents have failed to establish that use of vehicle software for security and safety research is likely to be noninfringing.

Dr. Green errantly asserts that broad proposed uses of the vehicle software, which may include copying, modifying and distributing code, in the course of security research is authorized by fair use, under 17 U.S.C. § 107. The Section 107 fair use analysis requires the consideration of four factors that on balance weigh against a finding that Proponents' proposed use is fair use: 1) the purpose and character of the use, 2) the nature of the copyrighted work, 3) the amount and substantiality of the portion used, and 4) the market for the copyrighted work.

1. Purpose and Character of Use

[20] Section 1201 Rulemaking: Fifth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies at 7 (Oct. 2012), *available at* http://copyright.gov/1201/2012/Section_1201_Rulemaking_2012_Recommendation.pdf ("2012 Recommendation").

[21] *Id.*; Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Notice of Inquiry*, 79 Fed. Reg. 55687, 55689 (2014)("2014 NOI") (citing Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies at 10 (2010), *available at* http://www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf ("2010 Recommendation")).

[22] *See* 2014 NOI at 55690 (citing 17 USC 1201(a)(1)(C)); 2010 Recommendation at 10; 2014 NOI at 55690 (citing 2012 Recommendation at 7) .

The first fair use factor considers whether the proposed use is commercial in nature, and whether it is "transformative" in that it "adds something new, with a further purpose of different character, altering the first with new expression, meaning, or message."[23] This factor further considers whether the use is commercial. However, Dr. Green does not discuss these aspects in any real depth and instead, states that "the purposes of good faith computer research are all listed as paradigmatic fair uses in Section 107's preamble: criticism, comment, news reporting, teaching, scholarship, or research."[24] Dr. Green goes on to describe how security researchers engage in scholarship, research, engage in criticism, commentary and news reporting and professors teach students through hands on investigation of software. However, he fails to address how the dissemination of highly sensitive information about how a car's ECUs or TPMs operate increases the potential risk that even individuals with benign intent might access and modify their vehicle software in such a manner that increases, rather than minimizes security and safety challenges.

2. Nature of Copyrighted Work

Proponents seek access to computer software in a vehicle's ECU and Dr. Green claims that this factor weighs in favor of fair use because the types of work used for security research are more factual and functional than creative and that copyright protection for computer programs is thin due to the many function design elements in computer programs. However, vehicle software in ECUs is a highly creative work designed by specialized engineers that have developed a delicate and precise control system within a vehicle, subject to a complex framework of security needs, regulatory requirements, and quality, performance and reliability standards. This software is a result of years of research and development and a significant

[23] 2010 Recommendation at 94-95; 2012 Recommendation at 41; 17 U.S.C§ 107(1).
[24] Green Comments at 15.

investment of resources by GM and other automotive manufacturers. The mere existence of certain functional elements does not obviate the need to protect the expressive aspects also encompassed in the work.

3. Amount and Substantiality of Portion Used

The third fair use factor considers whether "the quantity and value of the material used are reasonable in relation to the purpose of the copying".[25] Dr. Green asserts that where it is necessary to copy an entire copyrighted work, this factor does not weigh against a finding of fair use. He further indicates that published security research is transformed and the portions of copyrighted works used are necessary to complete the research, thus arguing that this factor weighs in favor of a fair use determination. However, the main question is how much of the work was copied. Even in *Sega* and *Sony*, where fair use was ultimately found, this third factor weighed in the Plaintiffs' favor where an entire work was copied.[26] Moreover, even where a small portion of a work is copied, its use will not be considered fair if that portion contains the essence or essential part of the copyrighted work.[27] Such is the case where Proponents seek to copy an entire work, which weighs against a finding of fair use.

4. Market for the Copyrighted Work

Finally, Dr. Green concedes that this factor is "undoubtedly the single most important element of fair use."[28] This last fair use factor considers whether the use threatens the potential market for, or value of, a copyrighted work.[29] Moreover, it addresses whether "unrestricted and

[25] *Campbell v. Acuff Rose Music, Inc*., 510 U.S. 569, 586-87 (1994).
[26] *See Sony*, 203 F.3d at 606; *Sega*, F.2d 1510 at 1526.
[27] *Harper & Row, Publishers, Inc. v. Nation Enters*., 471 U.S. 539 (1985)(copyright analysis considers an analysis of "the portion used in relation to the copyrighted work as a whole"
[28] Green Comments at 17 (citing Harper, 471 U.S. at 567).
[29] *See* 2012 Recommendation at 42.

widespread conduct of the sort engaged in by the defendant" would negatively impact the value of copyrighted works. [30] For the reasons set forth below, the answer is a resounding yes.

Safety is a primary factor motivating the purchasing decision of a potential vehicle owner. Vehicle safety and regulatory compliance are also critical factors for car manufacturers in the automotive industry. Therefore, the fact that vehicle firmware is sold as part of a car and not as a standalone product does not eliminate the harm to a manufacturer's copyright interests if a vehicle owner, or those acting on the owner's behalf, is permitted to circumvent TPMs to engage in security research, but then widely disseminates the code in such a manner that it 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. Allowing individuals to access, analyze, modify and then publish code for vehicle software risks increasing, not diminishing vehicle safety and security challenges. Further, such increased challenges directly and negatively impact the value of the copyrighted work.

As previously mentioned, there is no "rule of doubt" favoring an exemption when it is unclear whether a particular use is a fair use.[31] Dr. Green has failed to demonstrate that its security research as explained is clearly fair use. Moreover, its fair use analysis is largely lacking facts necessary to adequately evaluate whether its proposed uses would be fair use. In view of the foregoing, Dr. Green has failed to set forth a *prima facie* case that the broad category of security and safety research that could fall within the Proposed Exemption is noninfringing.

B. GM's TPMs and the Prohibition on Circumvention Do Not Have a Substantial Adverse Impact

Even assuming *arguendo* that Proponents could demonstrate that the affected uses are noninfringing, Proponents have still failed to demonstrate that the prohibition on circumvention

[30] *Campbell*, 510 U.S. at 590.
[31] 2012 Recommendation at 7.

has a substantial adverse impact on those noninfringing uses. For this reason also, Proponents have failed to establish a *prima facie* case in support of the Proposed Exemption.

Proponents must demonstrate that the adverse effects caused by the prohibition on circumvention are having "distinct, verifiable, and measurable impacts" occurring in the marketplace, as an exemption "should not be based on *de minimis* impacts"[32] The main focus is on whether a "substantial diminuation" of the availability of works for noninfringing uses is "actually occurring".[33] In other words, the Proponents must demonstrate by a preponderance of the evidence that the probation on circumvention has or is likely to have a *substantial* adverse effect on noninfringing uses of a particular class of works. [34]

As discussed above, vehicle owners have alternative options that permit security research and these alternatives protect the safety and do not require the unauthorized circumvention of the TPMs that protect the delicately calibrated software controlling a car's ECUs. The Registrar itself has advised that no substantial adverse impact occurs where sufficient alternatives exist to permit the noninfringing uses.[35] Given the availability of programs where manufacturers work with independent researches to test their products, GM takes the position that no *substantial* adverse impact occurs as a result of the default 1201 prohibition and Dr. Green presents no factual support to the contrary.

---

[32] 2014 NOI, 79 Fed. Reg. at 55690.
[33] 2014 NOI, 79 Fed. Reg. at 55690, citing 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) ("House Manager's Report").
[34] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 75 Fed. Reg. 43825, 43826 (2010) ("2010 Final Rule").
[35] 2012 Recommendation at 8 ("The Register and Librarian will, when appropriate, assess the alternatives that exist to accomplish the proposed noninfringing uses. Such evidence is relevant to the inquiry regarding whether the prohibition adversely affects the noninfringing use of the class of works. If sufficient alternatives exist to permit the noninfringing use, there is no substantial adverse impact.")

Dr. Green argues that the ban on circumvention chills research due to potential civil and criminal liability for those who may inadvertently violate the 1201 violation. However, Dr. Green does not provide factual evidence that the aforementioned adverse effect is *substantial*. He provides two examples where researchers were threatened with action if they attempted to present the results of their security research publically.[36] However, Dr. Green admits that in one of these cases, the threat had no effect. Dr. Green does not provide factual evidence that the aforementioned adverse effects are *substantial* and has failed to demonstrate "distinct, verifiable, and measurable impacts" occurring in the marketplace. Instead, his concern is hypothetical. He further fails to address the impact on the effectiveness of U.S. regulatory systems for maintaining vehicle safety or emissions if certain information regarding potential security vulnerabilities is publically disseminated and detailed. Cars are not CDs or personal computers. Thus, the public interest must be considered when vehicle safety issues and regulated environment protection issues arise and it is imperative the manufacturers are involved. Otherwise, allowing access to the critical infrastructure in cars may create far more chilling concerns than any *de minimis* chilling effect on security research.

Finally, Dr. Green has not demonstrated that a significant number of individuals are interested in accessing the software controlling a vehicle's ECUs for the purposes of security research, but hampered from doing so. Dr. Green has provided anecdotal evidence. However, this hardly demonstrates that adverse effects caused by the prohibition on circumvention TPMs results in "distinct, verifiable, and measurable impacts" occurring in the marketplace, and not simply de minimis impacts. Moreover, the automotive industry is aware of and focused on the potential safety implications of the wireless cars. GM understands that certain security researchers do have valuable knowledge and expertise and can assist in identifying security

[36] Green Comments at 18.

vulnerabilities. As previously mentioned, they partner with third party researchers for security testing.

In view of the foregoing, Proponents have failed to demonstrate sufficient harm to warrant granting an exemption prohibiting circumvention that Congress established.

IV. THE SECTION 1201(a)(1)(C) FACTORS WEIGH AGAINST GRANTING AN EXEMPTION

For the reasons discussed above, Proponents have failed to establish a *prima facie* case for the Proposed Exemption and, as such, it should be denied without consideration of the statutory factors, which include a) the availability for use of copyrighted works, b) the availability for use of works for nonprofit archival, preservation, and educational purposes, c) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research, d) the effect of circumvention of technological measures on the market for or value of copyrighted works, and e) such other factors as the Librarian considers appropriate.[37] Nonetheless, even consideration of the statutory factors under 17 U.S.C. §1201(a)(1)(C) support denying the Proposed Exemption. On balance, the negative ramifications likely to result if the exemption were granted outweigh any *de minimis* adverse effects resulting from the prohibition on circumvention for purposes of the Proposed Exemption.

A. The Availability for Use of Copyrighted Works

This factor considers the prohibition's impact on the availability for use of the copyrighted works. The major considerations for this inquiry are whether the availability of the work in a protected format enhances or inhibits public use of the work, whether the protected work is available in other formats, and if so, whether such formats are sufficient to accommodate

[37] 17 U.S.C. §1201(a)(1)(C)

noninfringing uses.[38] Dr. Green claims that "the broad and general exemption [he] request[s] is necessary to ensure good faith security researchers may study any form of software or device relevant to the safety of individuals or security of the nation."[39] However, Dr. Green provides only a handful of examples to demonstrate that the prohibition may limit access to software or devices including vehicle software for the purpose of security research, and fails to address the fact that alternative means of accessing software for security research, in particular vehicle software exists.

As previously mentioned, automotive companies, such as GM, engage third parties for work on various parts of the vehicle. With regard to software glitches "many companies pull in an external source code inspector to preemptively catch and remove the bugs."[40] Manufacturers also contract with researchers. These arrangements can be open to public participation, such as in standard-setting organizations, or can be restricted when confidential information, such as the detailed operation of TPMs and ECUs, is required for appropriate research or evaluation. . Accordingly, given the current availability of legitimate and safe methods of conducing security research, the current prohibition does not limit availability of the work for legitimate noninfringing uses.

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

As mentioned above in the context of fair use analysis, the proposed exemption would not advance use of the copyrighted work for nonprofit archival or preservation. To the extent Dr. Green claims the exemption would advance educational purposes by allowing student involvement in security research or education purposes, he has not provided factual evidence that

[38] *See* 2012 Recommendation at 152 (citing 2010 Recommendation at 56).
[39] Green Comments at 23.
[40] www.proservicescorp.com/auto-industry-software -glitches

the prohibition has a substantial chilling effect on availability of use of work for this purpose or that many education programs are interested in performing security research for education purposes. Therefore, this factor does not weigh in favor of granting an exemption.

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

Dr. Green claims that the current prohibition curtails speech related to criticism, comment, news reporting, teaching, scholarship and research. However, despite the prohibition, plenty of people have written articles criticizing various automotive manufacturers for certain alleged vulnerabilities, while others have published papers analyzing security systems and potential vulnerabilities in specific brands of vehicles. Moreover, issues surrounding the safety and security of vehicles are often newsworthy and reported upon. Therefore, this factor should not weigh in favor of an exemption.

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

This factor should be given serious consideration. Dr. Green is incorrect in his assertions that a general exemption for good faith security research will have a positive net effect on the market for software and devices, at least so far as automobiles are concerned.

TPMs ensure that users cannot access highly sensitive copyrighted vehicle software, including software which controls the functioning of ECUs, analyze the software and publicize how the TPMs and software work in such a way that would enable malicious actors and more benign users alike, to more easily access and modify a vehicle's safety and emissions systems. Granting the Proposed Exemption facilitates the dissemination of this information in an uncontrolled, public environment. Weakening the security of these systems may impact the ability to bring about advanced technology systems designed to increase automotive safety.

Accordingly, the value of the vehicle software will likely decrease as OEMs are continually put in a position of having to change their security structure, or to consider reducing the availability of advanced systems, each time researchers publish confidential and highly sensitive information about the security structures in place. This will detract from their ability to focus on new and innovative software, a valuable and lucrative endeavor. Furthermore, such public exposure of highly-sensitive copyrighted work would have chilling effects on OEMs' investment in development of new ECU software.

E. Such Other Factors as the Librarian Considers Appropriate

1. TPMs in Vehicles Increase Safety

Cars are not like cell phones or computer programs run on a personal computer. Instead, the availability of vehicle software for use at all is contingent upon the continued integrity of vehicle safety systems. Granting the exemption could impact vehicle safety, for example, by making it easier for both ill willed wrongdoers and unknowing hobbyists and the like to access a vehicle's software and compromise safety and regulatory compliance systems validated by the automaker. We note that although research is a favored use, the Registrar should consider the existence of alternative means for individuals to conduct security research and the negative ramifications that would likely result from hackers and others accessing this information, bypassing TPMs and modifying or otherwise interfering with ECUs. Allowing the exemption is akin to authorizing publication of and instruction manual for circumvention of safety and regulatory protocols in a vehicle and a roadmap to accessing highly sensitive and carefully calibrated vehicle software to which access is in part limited for security reasons.

OEMs are also more likely to invest in new innovative and secure vehicle software with increased functionality if third parties are prevented from accessing their highly-sensitive and

valuable copyrighted work and disclosing the details of such works publically in the name of "research", particularly when such disclosure serves to challenge the safety and regulatory mission of the software in the first place.

GM does not oppose security research into either its TPMs or ECUs and agrees with Dr. Green that security research is required to address security concerns. For that reason, GM and other OEMs, work cooperatively with both outside and internal researchers to improve their security and regulatory compliance as it pertains to both TPMs and ECUs. Further, OEMs are highly responsive when it comes to fixing software glitches and providing pertinent software updates. Dr. Green has not demonstrated that additional security research would result in any additional responsiveness or concern surrounding safety issues than is already customary in the automotive industry. Additionally, as of July 2014, "the U.S. National Highway Traffic Safety Administration was not aware of any instances of consumer vehicle control systems having been hacked."[41] Therefore, it is unclear the degree to which the alleged chilling effect on vehicle security research is having in the actual world. To the contrary, granting the broadly worded Proposed Exemption has the potential to shift the balance and create a safety and security and regulatory compliance concern that has not previously existed.

2. The Proposed Class Does Not Contain Ample Restrictions to Maintain Safety and Protect Copyright Interests.

The Copyright Office requires that the class of works for a proposed exemption should be "a narrow and focused subset of the broad categories of works . . . identified in section 102 of the Copyright Act."[42] However, Proposed Exemption is too broad and ill-defined. As currently drafted, if granted, the Proposed Exemption "would allow researchers to circumvent access

41 www.reuters.com/article/2014/07/22/cybersecurity-autos-isUSL2N0PX2FH2014722
[42] 2014 NOI at 55690.

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."[43] Dr. Green's suggested modification to the Proposed Exemption is even broader. As an initial matter, this class is broader than the other security-research related classes granted in the past, which in 2006 and 2010 covered security testing of CDs and video games that included software where the software itself acted as a TPM and created security flaws and vulnerabilities. Because of the narrowness of the class, proponents were able to demonstrate concrete examples of how the 1201 prohibition had an adverse impact on the availability of these works for security research.

For example, the Registrar recommended an exemption for "Sound recordings, and audiovisual works associated with those sound recordings, distributed in compact disc format and protected by technological protection measures that control access to lawfully purchased works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers, when circumvention is accomplished solely for the purpose of good faith testing, investigating, or correcting such security flaws or vulnerabilities" in 2006. In that situation, the Registrar stated that "the scope of the exempted class of works should be calibrated to address the harm that the proponents have demonstrated" and went on to characterize the exemption as "a relatively targeted exemption which [was] based on a really detailed technical study of [a particular security flaw], and based on that study, a concern about the same issues being important going forward." By contrast, the Proposed Exemption seeks *inter alia* to permit researchers to access hundreds of computer programs in automotive ECUs without limiting the purpose to studying the software for interoperability, encryption research, or any other previously identified use, but instead for an undefined category of "security research". Further,

[43] NPRM, 79 Fed. Reg. at 73870.

the above described security related exemption for sound recordings had no impact on safety systems, carefully crafted regulatory schemes, or the secure operation of important heavy equipment (like automobiles). For these reasons, Proponents have failed to provide sufficient evidence to support such a broad category or to support the scope of the proposed class.

V. CONCLUSION

In view of the foregoing, Proponents have failed to demonstrate a *prima facie* case that the affected uses are noninfringing or that the prohibition is having a substantial adverse impact. Furthermore, Proponents have simply failed to consider the implications such an exemption will have on vehicle safety, security, and regulatory compliance. When considering these various factors, GM respectfully submits that the Proposed Exemption should be denied.

Dated: March 27, 2015

Respectfully submitted,

By: __*/s/ Harry M. Lightsey III*_____

General Motors LLC
Harry M. Lightsey III
Jeffrey M. Stefan
25 Massachusetts Avenue, NW
Suite 400
Washington, DC 20001
(202) 775-5039

Hogan Lovells US LLP
Ari Q. Fitzgerald
Anna Kurian Shaw
Lauren Chamblee
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5423
Attorneys for General Motors LLC