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 22: Vehicle Software – Security and Safety 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 22: Vehicle Software-Security and Safety Research

COMMENTS OF GENERAL MOTORS COMPANY 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 22. The proposed exemption is overbroad, and the proponents have failed to establish a *prima facie* case that an exemption for Class 22 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 proposed exemption. Importantly, the proposed exemption presents a host of potential safety, security and regulatory concerns that the proponents have not fully considered. Indeed, although proponents such as Electronic Frontier Foundation concede that Electronic Control Units ("ECUs") in vehicles raise safety and security concerns, they seem to ignore the fact that the exemption they seek would permit circumvention of the very TPMs designed to play an

[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.

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, those very same ECUs. [3] Furthermore, the exemption being sought is broad and would allow copying code, modifying code and distributing code. [4] Even when such efforts are undertaken by well-intentioned researchers, wider distribution of such information provides third parties, both those with ill will and those with more benign interests, access to vehicles in a way that implicates safety and security concerns. Thus, if granted, the proposed exemption will likely result in significant safety and security challenges.

Proposed Class 22. Various petitioners have submitted petitions and comments in support of an exemption for proposed class 22 which would allow: [5]

> CIRCUMVENTION OF TPMS PROTECTING COMPUTER PROGRAMS THAT CONTROL THE FUNCTIONING OF A MOTORIZED LAND VEHICLE FOR THE PURPOSE OF RESEARCHING THE SECURITY OR SAFETY OF SUCH VEHICLES. UNDER THE EXEMPTION AS PROPOSED, CIRCUMVENTION WOULD BE ALLOWED WHEN UNDERTAKEN BY OR ON BEHALF OF THE LAWFUL OWNER OF THE VEHICLE.[6]

Electronic Frontier Foundation ("EFF") has set forth the most substantive comments and GM focuses its response on these comments. EFF and the other petitioners are collectively referred to herein as "Proponents."

---

[3] *See* Long Comment of Electronic Frontier Foundation Regarding a Proposed Exemption at 2 ("EFF Comments").
[4] EFF Comments at 7.
[5] In addition to EEF, Dr. Matthew D. Green, Ph.D. seeks a broader exemption, such as the broad good faith security exemption as proposed in Class 25, the SAE International (formerly Society of Automotive Engineers) filed comments taking no position but offering to assist the Copyright Office in its inquiry, the SAE International (formerly Society of Automotive Engineers) on behalf of the SAE International Vehicle Electrical System Security Committee (VESS) filed comments taking no position but offering to assist the Copyright Office in its inquiry, and combined comments received through the Digital Right to Repair website generally expressed the view that that researchers should not be at risk of running afoul of copyright law when testing the safety of vehicles.) *See* Short Comment of Dr. Matthew D. Green, Ph.D.; Short Comment of SAE International on behalf of the SAE International Dedicated Short Range Communication Standards Committee Regarding a Proposed Exemption; Short Comment of SAE International on behalf of the SAE International Vehicle Electrical System Security Committee Regarding a Proposed Exemption; various Short Comments submitted through the Digital Right to Repair website.
[6] NPRM at 73869.

EFF's petition and comments in support of proposed class 22 broadly seek to allow vehicle owners or others, on their behalf, to circumvent TPMs to access all computer programs that control the functioning of a vehicle, "[including programs that modify the code or data stored in such a vehicle and including compilations of data used in controlling or analyzing the functioning of such a vehicle,] for the purpose of researching the security or safety of such vehicles" ("Proposed Exemption").[7] EFF characterizes this exemption as merely allowing independent researchers to review software running in a vehicle and "identify flaws in critical code on which hundreds of millions of Americans depend in their travels."[8] However, the exemption would also cover the public distribution of code relating to 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 others. [9] The 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 the 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 impact the 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 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,

[7] *See* Petition of Electronic Frontier Foundation at 1 ("EFF Petition"); EFF Comments at 1.
[8] EFF Comments at 2.
[9] http://www.ni.com/white-paper/3312/en/

remote door unlock, turn-by-turn navigation, vehicle diagnostics, hands-free calling and 4G LTE wireless connectivity.[10]

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.[11] Many of these systems are critical to the vehicle safety 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.[12]

The security that protects the software operating on a 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 diagnostic and security features such as Remote Door Unlock, Remote Ignition Block and Stolen Vehicle Slowdown.[13] GM engineers use TPMs to make these systems safe and secure.

---

[10] More information on GM and its affiliates, including OnStar, can be found at http://www.gm.com.

[11] *See* http://www.nytimes.com/2010/02/05/technology/05electronics.html; http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

[12] Examples of TPMs used by GM include seed/key access control mechanisms, firmware signing, and sensitive data encryption.

[13] 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.

With TPMs as part of systems protecting vehicle safety, security and regulatory compliance, it would be inappropriate to permit their circumvention. 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 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.[14] "Tampering" includes "rendering inoperative" integrated design elements to modify vehicle and/or engine performance without complying with emissions regulations.[15] 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.[16] 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.[17] All of this affects the overall security of a vehicle and could

[14] 42 U.S.C. § 7522(a).
[15] 42 U.S.C. § 7522(a).
[16] 49 U.S.C. §§ 30112(a)(1), 30122(b).
[17] *See e.g.*, Car Hacker's Handbook available at http://opengarages.org/handbook/, http://boingboing.net/2014/07/16/car-hackers-handbook.html; EFF Comments at 23.

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 automotive manufacturers ("OEMs") undertake great efforts to ensure that these ECUs are secured, the Proposed Exemption enables public dissemination of highly sensitive information about the operation of these ECUs and creates a myriad of possible safety risks. GM does, however, 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."[18] 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 likely to cause, a substantial adverse impact on those uses.[19] The proponents "must prove by a preponderance of the evidence that the harm alleged is more likely than not." [20]

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

Neither EFF, nor the other proponents, have demonstrated that the uses for which they seek an exemption are noninfringing under either under 17 U.S.C. § 117 or 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."[21] Given this framework for evaluating whether the uses are affected and the broad category of uses covered by the Proposed Exemption, EFF has failed to establish that use of vehicle software for security and safety research is likely to be noninfringing.

1. The Affected Uses Are Not Noninfringing Under 17 U.S.C. § 117

17 U.S.C. § 117 permits "owners" of computer programs to make a copy of such computer program, if the copy is 1) created as an essential step in the utilization of the computer program in conjunction with a machine and used in no other manner, or 2) for archival purposes only and all archival copies are destroyed in the event that continued possession of the computer

[18] 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").
[19] 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").
[20] *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")).
[21] *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).

program should cease to be rightful. Here, Proponents have failed to demonstrate that vehicle owners are the owners of the computer programs in the vehicle or that the broad category of affected uses fall within the narrow categories of use specified in Section 117.

a) Proponents Have Failed to Demonstrate That Vehicle Owners "Own" the Computer Programs in Vehicles

Proponents incorrectly conflate ownership of a vehicle with ownership of the underlying computer software in a vehicle.[22] The Registrar has admitted that the state of the law regarding software ownership under Section 117 is unclear (or "murky" as conceded by EFF).[23] In fact, in the context of analyzing wireless handset software ownership under § 117, the Registrar went so far as to conclude that "the lack of certainty in the law makes it impossible for proponents to have established their case. . . ." [24] and that "[e]ven if proponents had submitted agreements to support a claim that wireless handset software is owned rather than licensed, the uncertain state of the law would still preclude the Registrar from developing conclusions sufficient to permit determination of the software ownership issue."[25] Although we currently consider ownership of vehicle software instead of wireless handset software, the law's ambiguity similarly renders it impossible for Proponents to establish that vehicle owners own the software in their vehicles (or even own a copy of the software rather than have a license), particularly where the law has not changed. Indeed, EFF relies on the *same* two cases considered in the 2012 Recommendation, *Krause v. Titleserv, Inc. and Vernor v. Autodesk Inc.*, when the Registrar concluded that the law was too uncertain to determine whether software was owned.[26] We briefly revisit these cases below.

In *Krause,* the court determined that formal title alone was not the sole consideration to establish ownership in a copy of a computer program, but instead considered several factors to determine whether "sufficient incidents of ownership" existed to establish ownership, including: 1) whether substantial consideration was paid for the copy, 2) whether the copy was created for the sole benefit of the purchasers, 3) whether the copy was customized to serve the purchaser's

[22] *See* EFF Comments, 12-16.
[23] *See* 2012 Recommendation at 92; EFF Comments at 12.
[24] 2012 Recommendation at 92.
[25] *Id.*at 92-93.
[26] *Krause v. Titleserv, Inc.* 402 F.3d 119, 124 (2nd Cir. 2005);*Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1110-1111 (9th Cir. 2010).

use, 4) whether the copy was stored on property owned by the purchaser, 5) whether the creator reserved the right to repossess the copy, 6) whether the creator agreed that the purchaser has the right to possess and use the programs forever regardless of whether the relationship between the parties terminated, and 7) whether the purchaser was free to discard or destroy the copy anytime it wished.[27] The Court in *Vernor* held that "a software user is a licensee rather than an owner of a copy where the copyright owner 1) specifies that the user is granted a license, 2) significantly restricts the user's ability to transfer the software, and 3) imposes notable use restrictions."[28]

EFF cannot and does not demonstrate that vehicle owners own a copy of the computer software that controls a vehicle's ECUs based on the *Krause* factors. Quite to the contrary, EFF itself has identified various license agreements that demonstrate that vehicle manufacturers do not sell copies of their software, but instead license the software in the cars they sell.[29] EFF points to a sole purchase agreement, Tesla's Vehicle Purchase Agreement to arguably demonstrate that the owner of this car owns a copy of the software in the car because "they possess a copy of the software inside, and they retain the ability to transfer and dispose of the software freely along with the vehicle."[30] However, in contrast to this one example, EFF itself points to five other examples of instances where car manufacturers license their software and place restrictions on *inter alia* the use, modification, adaptation, translation, and/or disassembly of the software in their vehicles.[31]

Thus, the record demonstrates that a vehicle owner does not own a copy of the relevant computer programs in the vehicle under *Vernor* as well. EFF attempts to distinguish *Vernor* by arguing that the software at issue was highly transferrable and valuable to any architect, while an ECU comes with the car, is included in the price of the car, and is therefore, more like the sale of goods.[32] However, this distinction is irrelevant to the question of whether vehicle owners own a copy of the software in the car under either the *Krause* or the *Vernor* factors. In view of the foregoing, the Proponents own evidence demonstrates that vehicle owners do not own the vehicle software at issue, and, thus, the affected uses cannot qualify as noninfringing under 17 U.S.C. § 117.

---

[27] 2010 Recommendation at 126 (citing *Krause*, 402 F.3d at 124).
[28] *Vernor*, 621 F.3d at 1111.
[29] EFF Comments 13-14.
[30] *Id.* at 13.
[31] *Id.* at 13-14.
[32] EFF Comments at 14.

b) Proponents Have Also Failed to Demonstrate That Copying or Adapting Computer Programs in Vehicles Is an Essential Step to Utilization of the Programs in the Vehicles

In addition to failing to demonstrate that vehicle owners are owners of the vehicle software, Proponents also fail to demonstrate that the creation of a copy or adaptation is "an *essential step* in the utilization of the computer program in conjunction with a machine and that it is used in no other manner."[33]

EFF's discussion of this element is limited, for good reason, and it cites *Krause* for the proposition that "a copy made for the express purpose of adding new features and capabilities that do not implicate a copyright holder's rights qualifies as an essential step for the purposes of Section 117 protection" because the modifications made the "software helpful or worth using."[34] First, EFF cannot demonstrate that the broad category of security research in the Proposed Exemption is limited to merely adding new features and capabilities, and, further, EFF concedes that making copies of vehicle firmware "is not essential to using the vehicle software for routine driving purposes."[35] Additionally, given the various safety, security and regulatory compliance issues implicated by the Proposed Exemption, the copying in this instance has the opposite of effect from making the software helpful or worth using.

c) Proponents Have Also Failed to Demonstrate that the Affected Uses are for Archival Purposes Only

Further, EFF has also failed to demonstrate that the Proposed Exemption is for uses limited to *archival purposes only* as required by 17 U.S.C. § 117(a)(2). Indeed, the safe harbor for archival uses provided by 17 U.S.C § 117(a)(2) is wholly unrelated to the affected uses under the Proposed Exemption, namely uses for the purposes of security and safety research. EFF unsuccessfully tries to equate allowing a third party to make a copy of a computer program "for car hobbyists who do not have the expertise to engage in firmware modification on their own" or for "research done by those engaging in copying or adaptation to analyze vehicle firmware" with archival purposes.[36] Such comparisons are simply unsupported by the law or the record.

[33] 17 U.S.C. § 117(a)(1)
[34] EFF Comments at 15 (citing *Krause*, 402 F.3d at 127).
[35] EFF Comments at 15.
[36] *See* EFF Comments at 16.

2. *The Affected Uses in the Proposed Exemption Also Do Not Qualify As Fair Uses Under 17 U.S.C. § 107*

EFF also argues that circumvention for the purpose of copying, modifying and distributing vehicle software code in the course of security and safety research is a 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 the affected uses are 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.[37] For the reasons discussed below, Proponents have failed to demonstrate that the affected uses qualify as fair use.

a) Purpose and Character of Use

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."[38] This factor further considers whether the use is commercial. Here, EFF is seeking a broad scope of use – "an individual may copy the code . . . , modify the code . . ., and distribute the code . . . ."[39] EFF merely argues that because uses purportedly serve a public interest, further inquiry into the purpose and character of the use is not required and does not discuss these aspects in any real depth. However, for the reasons discussed above, EFF's premise that the protected uses serve the public interest is not well founded. To the contrary, granting the exemption, will facilitate distribution of otherwise sensitive information relating to the ECUs that control vehicle functions. This information can then easily be accessed by individuals and organizations ranging from mal-intentioned members of the hacker community to hobbyists searching for information online as they modify their vehicles. Irrespective of who uses this information, it cannot be denied that it has the potential to adversely impact safety and security and the regulatory landscape as it relates to automobiles.

b) Nature of Copyrighted Work

[37] *See* 17 U.S.C. § 107; *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596, 602 (9th Cir. 2000).
[38] 2010 Recommendation at 94-95; 2012 Recommendation at 41; 17 U.S.C.§ 107(1).
[39] EFF Comments at 7.

Proponents seek access to computer software in a vehicle's ECUs and EFF claims that the software must be copied in order to ascertain the functional aspects of the software. However, EFF again relies on cases where the Courts determined that attaining the functional aspects of the relevant software was necessary for the purpose of interoperability. Moreover, in each case, the party copying the work clearly indicated how reverse engineering copyrighted software allowed them to identify software code required for the purpose of interoperability. By contrast, even if computer programs contain functional noncopyrightable aspects, EFF has not provided a sufficient factual basis to establish that the affected uses only impact functional aspects of vehicle software.

To the contrary, the vehicle software in ECUs is a highly creative work designed by specialized engineers that have developed a delicate and precise interconnected control system within a vehicle, subject to a complex framework of safety and security needs, regulatory requirements, and quality, performance and reliability standards. This software is a result of years of research and development and a significant investment of resources by GM and other automotive manufacturers. Further, even if such software included in part certain functional elements, something which Proponents have not demonstrated, this does not obviate the need to protect the expressive aspects also encompassed in the work.

c) Amount and Substantiality of Portion Used

Under this factor, courts consider how much of the work was copied. Even in *Sega* and *Sony*, where fair use was ultimately found, this third factor weighed in the copyright owner's favor where an entire work was copied.[40] EFF concedes that all the firmware within an ECU may be used.[41] However, 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.[42] In view of this, Proponents essentially concede that this factor weighs against a finding of fair use.

[40] *See Sony*, 203 F.3d at 606; *Sega Enterprises LTD v. Accolade, Inc.*, 977 F.2d 1510, 1526 (9th Cir. 1992).
[41] EFF Comments at 10.
[42] *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")

d) Market for the Copyrighted Work

The final fair use factor considers whether the use threatens the potential market for, or value of, a copyrighted work"[43] Moreover, it addresses whether "unrestricted and widespread conduct of the sort engaged in by the defendant" would negatively impact the value of copyrighted works. [44] 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 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.

There is no "rule of doubt" favoring an exemption when it is unclear whether a particular use is noninfringing.[45] Here, lack of clarity abounds. In view of the foregoing, EFF has failed to set forth a *prima facie* case that the broad categories of diagnosis, repair and modification activities that could fall within the Proposed Exemption are 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 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.

[43] 2012 Recommendation at 42.
[44] *Campbell v. Acuff Rose Music, Inc*., 510 U.S. 569, 590 (1994).
[45] 2012 Recommendation at 7.

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."[46] The main focus is on whether a "substantial diminuation" of the availability of works for noninfringing uses is "actually occurring".[47] In other words, the Proponents must demonstrate by a preponderance of the evidence that the prohibition on circumvention has or is likely to have a *substantial* adverse effect on noninfringing uses of a particular class of works. [48]

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.[49] Given the availability of programs where manufacturers work with independent researchers to test their products, GM takes the position that no *substantial* adverse impact occurs as a result of the default 1201 prohibition and EFF presents no factual support to the contrary.

EFF argues that the ban on circumvention increases the risk of vehicle-related injury and theft and deprives customers of critical information despite the fact that automotive manufacturers have consistently demonstrated their willingness to consider and address confirmed security issues when they come aware of them. However, EFF does not provide factual evidence that any of the aforementioned adverse effects are *substantial* and has failed to demonstrate "distinct, verifiable, and measurable impacts" occurring in the marketplace. EFF claims that researchers have demonstrated shortcomings in car security networks, but fails to identify any real-world occurrences where a car was stolen or attacked as a result of security vulnerabilities or that such an occurrence is likely to occur in the near future. GM understands

[46] 2014 NOI, 79 Fed. Reg. at 55690.
[47] 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").
[48] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 75 Fed. Reg. 43825, 43826 (2010) ("2010 Final Rule").
[49] 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.")

that certain security researchers do have valuable knowledge and expertise and can assist in identifying security vulnerabilities. Therefore, as previously mentioned, they partner with third party researchers for security testing. EFF has also failed to demonstrate substantial vehicle-related injury as a result of the current prohibition, noting only one example. EFF states that "many high-profile recalls across a number of makes and models have been prompted by software issues."[50] EFF's point is irrelevant. Repairs for vehicle recalls are validated and properly released by the auto manufacturers. Changing the 1201 prohibition will have no effect on this process. Highlighting OEM recalls only goes to show that OEMs provide free software updates when software glitches are identified, and perform required updates when safety issues are identified.

Finally, EFF 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. EFF has provided anecdotal evidence. However, the declarations and evidence EFF provides hardly demonstrate that adverse effects on security research caused by the prohibition on circumventing TPMs results in "distinct, verifiable, and measurable impacts" occurring in the marketplace, and not simply de minimis impacts. The "individual cases" that EFF has set forth "do not satisfy the rulemaking standard".[51]

In view of the foregoing, Proponents have failed to demonstrate sufficient harm to warrant granting an exemption to warrant a shift from default rule 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,

[50] EFF Comments at 17.
[51] 2014 NOI, 79 Fed. Reg. at 55690.

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.[52] 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 noninfringing uses.[53] EFF provides a handful of examples to demonstrate that the prohibition limits access to a vehicle's software, but fails to address the fact that alternative means of accessing vehicle software for security research exist. 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."[54] Manufacturers also contract with researchers. These arrangements can be open to public participation, such as with many standard setting organizations, or may be confidential, when sensitive information about TPMs and operation of 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 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, preservation or education purposes. Therefore, this factor does not weigh in favor of granting an exemption.

---

[52] 17 U.S.C. §1201(a)(1)(C)
[53] *See* 2012 Recommendation at 152 (citing 2010 Recommendation at 56).
[54] www.proservicescorp.com/auto-industry-software -glitches

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

EFF 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. EFF itself has pointed to numerous articles and publications related to vehicle security. 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. 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 an 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 EFF 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. EFF 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."[55] 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

[55] www.reuters.com/article/2014/07/22/cybersecurity-autos-isUSL2N0PX2FH2014722

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."[56] However, the Proposed Exemption is too broad and ill-defined. As currently drafted, if granted, the Proposed Exemption "would allow circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicle for the purpose of researching the security or safety of such vehicles. Under the exemption as proposed, circumvention would be allowed when undertaken by or on behalf of the lawful owner of the vehicle."[57] 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 to permit researchers to access hundreds of computer programs in automotive ECUs without limiting the

[56] 2014 NOI at 55690.
[57] NPRM, 79 Fed. Reg. at 73869.

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, 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