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
	)	Class 17: Jailbreaking—All-Purpose Mobile Computing Devices

COMMENTS OF GENERAL MOTORS LLC

Ari Q. Fitzgerald
Anna Kurian Shaw
Deborah K. Broderson

Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5423
Attorneys for General Motors LLC

Harry M. Lightsey III
Jeffrey M. Stefan

General Motors LLC
25 Massachusetts Avenue, NW
Suite 400
Washington, DC 20001
(202) 775-5039

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
	)	Class 17: Jailbreaking—All-Purpose Mobile Computing Devices

COMMENTS OF GENERAL MOTORS LLC

I. SUMMARY OF 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") prohibition against circumvention of technological protection measures ("TPMs") that control access to copyrighted works.[2]

As discussed in more detail below, the Copyright Office should deny or at least narrow the proposed exemption for Class 17. The proposed exemption is overbroad, and its proponents have failed to establish a prima facie case that an exemption for Class 17 is or is likely to be non-infringing. 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

[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] *Id.* at 73856.

does not need to examine the relevant statutory factors; however, consideration of those factors also supports a decision to deny the proposed exemption.

Proposed Class 17. Two petitioners—the Electronic Frontier Foundation ("EFF") and Maneesh Pangasa ("Pangasa") (collectively, the "Proponents")—filed petitions seeking an exemption from the DMCA to allow the "jailbreaking" of all-purpose mobile computing devices to allow these devices to run lawfully acquired software that TPMs otherwise prevent them from running, or to remove unwanted preinstalled software from the device.[3] The *NPRM* defines "all-purpose mobile computing devices" as all-purpose non-phone devices (such as the Apple iPod touch) and all-purpose tablets (such as the Apple iPad or the Google Nexus).[4] EFF seeks an exemption to allow the owner of an all-purpose mobile computing device to jailbreak or "root" that device for purposes such as to update security patches, to keep software running on a device current after the manufacturer has stopped supporting that software, and to run "important and useful software excluded by the manufacturer."[5] Pangasa seeks a similar exemption.[6]

According to EFF, granting an exemption for proposed Class 17 would allow device owners to bypass access controls affecting the vast majority of devices, whether phones, tablets, or small multipurpose devices, which "continue to stand in the way of owners' ability to run the lawfully acquired software of their choice, to remove software from their devices, to prolong the

[3] *Id*. at 73867.
[4] *Id*. As proposed, Class 17 does not include specialized devices such as e-book readers or handheld gaming devices, or laptop or desktop computers.
[5] EFF seeks an exemption for "[c]omputer programs that enable mobile computing devices, such as…tablets, to execute lawfully obtained software, where circumvention is accomplished for the sole purposes of enabling interoperability of such software with computer programs on the device, or removing software from the device." Petition of Electronic Frontier Foundation at 1-2 ("EFF Petition").
[6] Pangasa seeks an exemption "[f]or jail-breaking or rooting tablets like the Apple iPad Air & iPad Mini, Amazon's Kindle Fire HD, Microsoft Surface line of tablets (particularly the RT version to install hacks that permit running desktop applications on RT devices)." Petition of Maneesh Pangasa at 1 ("Pangasa Petition").

useful life of their devices, and to maintain the security of their personal information."[7] Pangasa argues that jailbreaking is necessary to allow competition and innovation in the marketplace and suggests that the inability to jailbreak devices increases costs for consumers.[8]

Commenters filing in support of the proposed Class 17 exemption generally based their arguments on the similarities between all-purpose mobile computing devices and smartphones, which were subject to an exemption for jailbreaking in the Copyright Office's 2012 decision.[9] For example, New Media Rights argues that all-purpose mobile computing devices and wireless telephone handsets are functionally almost identical, and that consumers demand and deserve the ability to jailbreak both classes.[10] Similarly, Jay Freeman submitted comments in which he suggested that the Copyright Office allow jailbreaking of wireless telephone handsets, all-purpose mobile computing devices, dedicated e-book readers, and smart TV sets because they all use the same operating systems.[11]

Proposed Class 17 Should Be Denied or Narrowed to Exclude In-Vehicle Telematics and Communication Systems. The Copyright Office should deny or at least narrow the proposed exemption. As an initial matter, the class sought by Proponents is overbroad and unsupported by evidence in the record. Although Proponents of Class 17 may not have envisioned including vehicle-based telematics and communication systems in the class, as drafted the Proponents'

[7] Long Comment of Electronic Frontier Foundation Regarding a Proposed Exemption at 2 ("EFF Comments").
[8] Pangasa Petition at 2-3.
[9] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 77 Fed. Reg. 65260, 65264 (2012) ("2012 Final Rule").
[10] Long Comment of New Media Rights Regarding a Proposed Exemption at 24.
[11] Long Comment of Jay Freeman Regarding a Proposed Exemption at 2 ("Freeman Comments"). In addition, the SAE International (formerly Society of Automotive Engineers) 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 consumers should be able to jailbreak any tablet device they own to customize that device. *See* 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.

Class 17 could be construed to encompass in-vehicle telematics and communication systems, including those provided by GM through OnStar.

Moreover, Proponents have failed to establish a prima facie case that jailbreaking or rooting in-vehicle telematics systems is or is likely to be non-infringing, and that TPMs are causing, or are likely to cause in the next three years, a substantial adverse impact on users. Because Proponents 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 any exemption for Class 17 that includes in-vehicle telematics systems.

If the Copyright Office finds that an exemption is generally appropriate, it should narrow Class 17 to exclude in-vehicle telematics systems such as OnStar. Although as drafted the proposed exemption class could be interpreted to include the vehicle-based OnStar system, the Proponents did not mention in-vehicle telematics systems when describing the proposed class and no commenter has submitted evidence in the record that would support an exclusion that includes such systems.

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, and is 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.[12]

Granting the proposed exemption for Class 17 without modification and including within it in-vehicle telematics or communication systems could have a chilling effect on future automotive telematics development and deployment and make it more difficult for vehicle manufacturers to satisfy the demands of consumers and regulators on a wide range of issues. The TPMs that Proponents seek to circumvent are the same TPMs that protect general vehicle functionality, ensure vehicle safety and cybersecurity, protect key consumer privacy interests, and enable compliance with federal safety and emissions requirements. Given their critical role in the many layers of protection and security that GM has incorporated in its in-vehicle telematics systems, the Copyright Office should not allow circumvention of such TPMs.

Unlike smartphones or other all-purpose mobile computing devices, in-vehicle telematics or communication systems are integrated into the vehicle's electronic architecture, and act as a major layer of the vehicle's safety, security, privacy and environmental compliance regime. Using wireless connectivity, the OnStar module can remotely reduce the speed of a stolen vehicle, engage in remote vehicle diagnostics, and provide over-the-air security updates implicating critical aspects of vehicle control. While GM takes great care to maintain the integrity of the OnStar system, allowing jailbreaking could make these applications more vulnerable to safety, privacy and security concerns. The OnStar software also uses TPMs to protect important aspects of vehicle emissions controls, which are required by federal and state law and provide important air quality protections. These TPMs, like those governing safety, privacy and security features, should also not be made vulnerable to circumvention.

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

The TPMs in place in GM vehicles are intended to prevent hackers from accessing important vehicle controls, and the Copyright Office should not approve a class exemption that would circumvent these controls. Because in-vehicle telematics and communication systems serve fundamentally different functions than smartphones or other mobile computing devices, the justification for jailbreaking smartphones or other mobile connectivity devices does not apply to vehicles.

B. Technological Protection Measures in GM Vehicles.

Operations and Importance of TPMs in GM Vehicles. Today's automobiles include, on average, 30 purpose-built Electronic Control Units ("ECUs") with functions that range from controlling the radio to regulating vital engine and safety functions. Many of these systems are critical to the safety, privacy and security of the vehicle and compliance with mandatory federal vehicle regulations. The ECUs are designed to be operated as built by the automobile manufacturers, and not to be modified by circumventing TPMs. Operating the ECUs as built is important to protect vehicle safety, privacy and security, and vehicle regulatory compliance systems. Automobile manufacturers must ensure that these ECUs are protected from tampering and hacking.

Automobile manufacturers employ many different types of TPMs, depending on the availability of the evolving technology and the type of the control system involved.[13] Vehicle ECUs are interconnected via 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. Interconnected OnStar services include system diagnostics and security features such as Remote Door Unlock, Remote

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

Ignition Block, and Stolen Vehicle Slowdown.[14] GM engineers use TPMs to ensure that these features are safe and secure.

The TPMs currently in place in GM vehicles are an integral part of an overall safety, cybersecurity, privacy and emissions regulatory strategy and solution. GM's TPMs are strategically designed and implemented to protect vehicle occupant safety (GM's highest priority) and to maintain mandatory emissions protections, as well as to thwart illegal activities such as cybersecurity attacks, theft, odometer fraud, modifications to air bag systems, and warranty fraud. In addition, TPMs protect information gathered by and stored in vehicle systems that if released, could compromise consumer privacy, including geolocation information, trip history, call history, and contacts.

Allowing a vehicle owner—or a third party, at the direction of a vehicle owner—to modify the OnStar telematics system to jailbreak its underlying software and download new applications, or remove existing software protocols, reduces the protections on networks and systems with which the telematics system is designed to interface. Allowing jailbreaking could also threaten the successful implementation of certain applicable legislative and regulatory goals and introduce risks to vehicle safety, privacy and security.

Alternatives to Circumvention of TPMs in GM Vehicles. An exemption for Class 17 is not necessary, because consumers already have free access to mobile applications not supported by GM. Notably, subject to the Copyright Office's finding in a related proceeding, consumers

[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.

can download applications of their choice on their smartphones or other handheld devices.[15] Other functions of the OnStar service, such as turn-by-turn directions, can similarly be obtained from numerous providers on a wide variety of GPS-enabled hand-held devices.

Both the purpose and function of in-vehicle telematics and communication systems differ significantly from that of hand-held wireless telecommunication devices, and consumers use hand-held mobile devices in very different ways than they use the OnStar system. Allowing circumvention of in-vehicle TPMs to jailbreak telematics systems such as OnStar would deliberately weaken the protections GM has put in place to ensure the operation of important regulatory requirements, vehicle safety, consumer privacy and vehicle security. It could also limit the availability of in-vehicle telematics and communication systems in the future and suppress innovation in the sector. Automobile manufacturers may be forced to rethink whether to offer the affected features absent the ability to protect them with robust TPMs.

C. Effects of Circumvention of TPMs in GM Vehicles.

In-vehicle telematics and communication systems do not function like smartphones or other mobile computing devices, and vehicle TPMs protect important safety, cybersecurity, and emissions systems in GM vehicles; protect personal privacy; prevent fraud and other illegal activities; and enable innovation and consumer choice.

Because GM's in-vehicle mobile computing elements interact with other vehicle ECUs in safety and emissions systems, allowing circumvention would pose needless risks to those

[15] Effective February 11, 2015, all major wireless telephony providers have unlocked their consumer wireless devices pursuant to a voluntary agreement facilitated by the Federal Communications Commission. *See* Roger C. Sherman and Kris Monteith, Blog: *Wireless providers fulfill commitment to let consumers unlock mobile phones* (Feb. 11, 2015), *available at* http://www.fcc.gov/blog/wireless-providers-fulfill-commitment-let-consumers-unlock-mobile-phones.

systems.[16] Allowing consumers and third parties to bypass built-in restrictions on access to the underlying software to upload new software, or remove GM-installed software could increase in-vehicle telematics and communication systems' vulnerabilities.

Placing safety, privacy and security foremost is not just a GM best practice; GM's TPMs also ensure that vehicles meet federally mandated safety and emissions standards. Circumvention of some emissions-oriented TPMs, such as the seed/key access control mechanisms, could violate 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.[17] "Tampering" includes "rendering inoperative" integrated design elements to modify vehicle and/or engine performance without complying with emissions regulations.[18] In addition, the Motor Vehicle Safety Act prohibits the introduction into U.S. commerce of vehicles that do not comply with the Federal Motor Vehicle Safety Standards ("MVSS"), and 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.[19]

Many known tampering methods are used to hide the failed or deactivated operation of an emissions or safety system, rendering these conditions unknown to a subsequent purchaser of the vehicle. As an example of a preferred circumvention, commenter Jay Freeman seeks permission to modify layouts on a device's home screen or change the function of pre-programmed

---

[16] As Jeff Williams, CTO of Contrast Security, observed: "I don't want to be hyperbolic about it, but we are connecting computers to things that can now kill you. Cars are potentially a really deadly thing if you lose control. So we are crossing a threshold into a world where you aren't just losing a spreadsheet or a credit card number, you are talking about directly harming people." Cadie Thompson, "More connected cars may mean more hacked cars," CNBC.com (Feb. 9, 2015), *available at* http://www.cnbc.com/id/102409721# ("*Connected Cars*").

[17] 42 U.S.C. § 7522(a).

[18] *Id.*

[19] 49 U.S.C. §§ 30112(a)(1), 30122(b).

buttons.[20] While such a request might be innocuous for a smartphone, altering displays, buttons, and even some chime behaviors for an in-vehicle telematics system could result in MVSS non-compliance, and unsafe operating conditions. If a vehicle's airbag systems, including any malfunction indicator lights, have been disabled (whether deliberately or inadvertently), a subsequent vehicle owner will have no advance warning that her safety could be in jeopardy. Similarly, a subsequent owner would have no way of knowing if a vehicle's emissions systems have been subject to tampering.[21] For good cause, federal environmental and safety regulations regarding motor vehicles establish a well-recognized policy against tampering with in-vehicle electronic systems designed for safety and emissions control.

GM incorporates TPMs into its vehicle system designs to avoid leaving connected vehicles vulnerable to cyberattack. Allowing consumers of vehicle-based telematics services to jailbreak those systems to upload new software or delete existing programs would remove this protection without offering GM a comparable alternative for ensuring compliance with important regulatory requirements and protecting vehicle safety, privacy and security.

Vehicles equipped with in-vehicle telematics systems may collect information on drivers and their movements, including geolocation information, trip history, call history, and contacts. GM uses TPMs to protect information gathered by and stored in vehicle systems the release of which could compromise consumer privacy, including personally identifiable information ("PII"). GM also relies on TPMs in vehicles to guard against fraud, theft and other illegal activities by vehicle owners and third parties. For example, a frequently-cited GM TPM, the seed/key access control mechanism, is also one of the TPMs used in vehicle security functions such as key learning and anti-theft protection. Maintaining the integrity of in-vehicle TPMs is

[20] Freeman Comments at 7.

[21] For tampering that the subsequent owner eventually discovers, manufacturer warranties do not cover the repair of damage caused by the tampering, placing the repair cost on the subsequent owner.

vitally important to ensure the safety, privacy and security not only of the original vehicle owner, but also of a subsequent purchaser, who might have no way of knowing that a previous owner compromised an important in-vehicle safety, security or privacy protection.

Finally, design, development and production cycles run much more slowly in the automotive sector than they do in the wireless handset sector, with current development cycles taking up to five years. Permitting unlocking of in-vehicle telematics and communication systems could further complicate and prolong this production cycle because this cycle would need to take into account the adverse effects of unlocking. This disrupts innovation and consumer choice, and suppresses the otherwise promising growth in this sector.[22]

In view of the foregoing, GM urges the Copyright Office to deny the proposed exemption as applied to in-vehicle telematics and communication systems. If granted as proposed, the exemption could pointlessly reduce the effectiveness of the TPMs vehicle manufacturers such as GM have developed to promote vehicle safety and security, protect consumer privacy, prevent fraud and theft, and promote innovation. The Proponents have not put forth any rationale to justify such a result.

III. PROPONENTS HAVE FAILED TO ESTABLISH A PRIMA FACIE CASE IN SUPPORT OF THE EXEMPTION

The Proponents have failed to establish a prima facie case in support of an exemption for Class 17. In addition, the proposed class is overbroad, and no commenter has provided evidence that would support an exemption for jailbreaking in-vehicle telematics and communication systems. The Proponents have also failed to establish that the uses for which they seek an exemption are noninfringing under the relevant law, and GM's TPMs do not adversely affect significant numbers of noninfringing users and uses.

[22] *See* McKinsey & Company, *Connected Car, Automotive Value Chain Unbound* at 40 (Sept. 2014).

A. Exemption Proponents Have Not Met Their Required Statutory Burden.

Pursuant to 17 U.S.C. § 1201, proponents of an exemption from the DMCA 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."[23] Thus, to establish a *prima facie* case for the proposed class, Proponents must affirmatively demonstrate that (1) the uses affected by the prohibition on circumvention are or are likely to be *noninfringing* and (2) as a result of a TPM controlling access to the copyrighted work, the prohibition is causing, or in the next three years is likely to cause, a substantial adverse impact on those uses.[24] The proponents must also establish that the harm alleged "is more likely than not" based on a preponderance of the evidence,[25] and the harm must be "distinct and measurable, and more than *de minimis.*"[26]

B. The Proposed Class Is Overly Broad and No Evidence Supports an Exemption for In-Vehicle Telematics and Communication Systems.

A major focus of this rulemaking proceeding is on how to define the excluded class.[27] Congress intended for an excluded class to be "a narrow and focused subset" of the statutory categories, and the Copyright Office must "look to the specific record" to assess the proper scope

[23] 17 U.S.C. § 1201(a); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Notice of Inquiry*, 79 Fed. Reg. 55687, 55689 (2014) ("2014 NOI").
[24] 17 U.S.C. § 1201(a)(1)(B); 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").
[25] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 75 Fed. Reg. 43825, 43826 (2010) ("2010 Final Rule").
[26] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 77 Fed. Reg. 65260, 65261 (2012) ("2012 Final Rule").
[27] 2014 NOI, 79 Fed. Reg. at 55690.

of the class for a recommended exclusion.[28] As proposed, Class 17 is overly broad and should be rejected or refined to exclude in-vehicle telematics and communication systems.

EFF asserts that the broad category of "mobile computing device firmware" is a "unitary, distinct class of copyrighted work.[29] Jay Freeman agrees, claiming that wireless telephone handsets, all-purpose mobile computing devices, dedicated e-book readers, and smart TVs should be included in the same class, because consumers use the same techniques to jailbreak all of these devices.[30] However, no commenter argues in favor of including in-vehicle telematics and communication systems in their proposed class, and no filer has submitted any evidence in the record that would support an exclusion for jailbreaking such systems.

Review of DMCA exemptions is conducted *de novo*, and previously granted exemptions do not factor into the current proceeding.[31] In every DMCA review, "the contours of a class will depend on the factual record established in the rulemaking proceeding."[32] The Copyright Office can refine a proposed class definition to ensure that it is appropriately tailored to its findings, but only where the proponent "has otherwise succeeded in demonstrating that some version of its exemption is warranted."[33] The Copyright Office "cannot delineate the appropriate contours of a class 'in a factual vacuum.'"[34]

In its 2012 decision, the Copyright Office observed that proponents of the handset jailbreaking exception attempted to expand the class to include tablets, but found that the record did not support such an extension.[35] The Copyright Office noted that the proposed class was

[28] *Id*. at 55690-91.
[29] EFF Comments at 2.
[30] Freeman Comments at 2.
[31] 2014 NOI, 79 Fed. Reg. at 55689.
[32] 2012 Final Rule, 77 Fed. Reg. at 65261.
[33] *Id*. at 65276.
[34] *Id*.
[35] *Id.* at 65264.

"broad and ill-defined," and could include a wide range of devices "notwithstanding the significant distinctions among them in terms of the way they operate, their intended purposes, and the nature of the applications they can accommodate."[36] Ultimately, the Copyright Office determined that the record "lacked a sufficient basis to develop an appropriate definition" for tablets, which was a "necessary predicate" to extending the jailbreaking exemption beyond smartphones.[37]

The Copyright Office is again faced with a "factual vacuum" here. The proposed Class 17 proffered by Proponents is overbroad, and no commenter has submitted any evidence that the class should include in-vehicle telematics and communication systems. In the absence of any discussion in the record to support the assertion that the jailbreaking of such systems would be non-infringing and that, absent an exemption, Proponents would be subject to actual or likely harm in the next three years, the Copyright Office must decline to adopt proposed Class 17, or must narrow it to exclude unsupported elements such as in-vehicle telematics and communication systems.

C. Exemption Proponents Have Failed to Establish that the Uses Affected by the Prohibition Are Noninfringing.

Proponents have also failed to demonstrate that the use for which they seek an exemption is noninfringing under relevant law. As a threshold matter, Proponents must demonstrate that their proffered use is or is likely non-infringing; it is not enough to show that a use could be merely plausibly or conceivably non-infringing.[38] The burden of proof remains on the

[36] *Id.*
[37] *Id.*
[38] See 17 U.S.C. § 1201(a)(1)(C); 2012 Final Rule, 77 Fed. Reg. at 65261.

Proponents to establish the noninfringing use; there is no 'rule of doubt' favoring an exemption when it is unclear whether a particular use is a fair use.[39]

1. Proponents' Proposed Uses Do Not Qualify as Fair Uses.

The four factors that make up the Section 107 "fair use" analysis 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 of the protected material used; and (4) the market for the copyrighted work.[40]

The first fair use factor considers whether the proposed use is "transformative" in that it "adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message."[41] For example, in *Sony Computer Entertainment, Inc. v. Connectix Corp.*, the court found that this element suggested fair use when a software maker reverse engineered a gaming system and provided new opportunities for game play in a new environment.[42] In contrast, in 2010 and 2012 the Copyright Office found that jailbreaking was unlikely to be transformative, "in light of the modest modifications" made to the firmware.[43] The Proponents demonstrate no such transformative use here. EFF has offered no evidence that

[39] 2012 Final Rule, 77 Fed. Reg. at 65261. A proponent must show more than that a particular use is noninfringing; it must "establish that the proposed use is likely to qualify as noninfringing under relevant law." 2014 NOI, 79 Fed. Reg. at 55690.
[40] *See* 17 U.S.C. § 107; *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596, 602 (9th Cir. 2000).
[41] 17 U.S.C.§ 107(1); Recommendation of the Register of Copyrights in RM 2008-8; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies at 94-95 (2010), *available at* http://www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf ("2010 Recommendation"); 2012 Recommendation at 41.
[42] 203 F.3d at 606-607.
[43] 2012 Recommendation at 72; 2010 Recommendation at 95.

jailbreaking in-vehicle telematics or communication systems would be transformative; mere assertions fail to meet the Section 107 evidentiary standard.[44]

The second inquiry is the nature of the copyrighted work. Although EFF cites *Sega v. Accolade* to support its claim that a court will find that copying for purposes of reverse engineering constitutes fair use,[45] that same court found that because they mix function with expression, computer programs and software provide unique challenges in analyzing this prong of the fair use test.[46] According to EFF, the modifications that constitute jailbreaking concern "only the functional aspects of the device firmware," and failing to grant the exemption would create "a de facto monopoly over the functional aspects" of the work.[47] However, the mere existence of certain functional elements does not obviate the need to protect the expressive aspects also encompassed in the work.[48] The in-vehicle software protected by GM's TPMs is a highly creative work designed by specialized engineers who have developed a delicate and precise controlling system within a vehicle, subject to a complex framework of security needs, regulatory requirements, and quality, performance and reliability standards. This software is the result of many years of research and development and a significant investment of resources by GM. The mere existence of certain functional elements does not obviate the need to protect the expressive aspects also encompassed in the work.

The third fair use factor is the amount of the work used; copying a greater percentage of the work argues against fair use. Even in *Sega Enterprises v. Accolade* and *Sony v. Connectix*,

---

[44] Pangasa does not provide any explanation of how his proposed exemption would constitute "fair use," and so fails to establish a prima facie case for the exemption. *See* Pangasa Petition at 4 (simply alleging that fair uses "should be acknowledged and protected with an exemption").
[45] EFF Comments at 11.
[46] *Sega Enterprises LTD v. Accolade, Inc.*, 977 F.2d 1510, 1524 (9th Cir. 1993).
[47] EFF Petition at 4, citing cases.
[48] *See, e.g.*, *Sony v. Connectix*, 203 F.3d at 603 (noting that the Copyright Act protects expression, rather than ideas or the functional aspects of a software program).

where fair use was ultimately found, this factor weighed in the plaintiff's favor where an entire work was copied.[49] The Copyright Office has previously found that this factor weighs against a finding of fair use for jailbreaking of smartphones, because any modifications were *de minimis*, and the firmware is "ultimately used for the very same purpose for which it was originally intended."[50] Even EFF observes that the amount of firmware that must be copied to jailbreak a device varies between devices, and acknowledges that this factor should be afforded minimal weight.[51]

The final fair use factor considers whether the infringing use threatens the potential market for, or value of, a copyrighted work. Under this factor the Copyright Office addresses whether "unrestricted and widespread conduct of the sort" proposed by the Proponents would negatively impact the value of copyrighted works.[52] Because fair use is an affirmative defense, a proponent would have difficulty securing a favorable assessment on this fourth prong "without favorable evidence about relevant markets."[53] Proponents have offered no such evidence here. To the contrary, an exemption for Class 17 could pose a credible threat to the market for in-vehicle telematics and communication systems if, as a result of jailbreaking, consumers believed that vehicle safety, security, privacy or emissions systems were compromised or placed at increased jeopardy of being compromised, and rejected the integration of such systems in their vehicles.

[49] *Sega Enterprises LTD v. Accolade, Inc.*, 977 F.2d at 1526-1527; *Sony v. Connectix*, 203 F.3d at 605-606.
[50] 2012 Recommendation at 73.
[51] EFF Petition at 5; EFF Comments at 13.
[52] *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 590 (1994).
[53] *Id.*

D. GM's TPMs and the Prohibition on Circumvention Do Not Adversely Affect Significant Numbers of Noninfringing Users and Uses.

In addition to establishing that the proposed uses are noninfringing, Proponents must also demonstrate that the alleged adverse effects caused by the prohibition on circumvention on the use of the copyrighted works are "distinct, verifiable, and measurable impacts" occurring in the marketplace; an exemption "should not be based on *de minimis* impacts."[54] With respect to this element, the Copyright Office's main focus must be on whether a "substantial diminution" of the availability of works for noninfringing uses is "actually occurring."[55] Proponents must demonstrate that the prohibition on circumvention has or is likely to have a *substantial* adverse effect on noninfringing uses of a particular class of works.[56] "[M]ere inconveniences, or individual cases that do not rise to the level of a substantial adverse impact" are outside the scope of the Copyright Office's review.[57] EFF has not met this standard.

EFF argues that the threat of copyright violation will "discourage users from engaging in legitimate, non-infringing modification of their devices" and hinder innovation.[58] According to EFF, denying the exemption for proposed Class 17 "would mean that security fixes, enhanced functionality, and in the case of iOS devices, all software, would be limited by operation of the DMCA to what the manufacturer and carrier choose to provide."[59] There is no evidence in the record, however, that a "substantial diminution" of the availability of in-vehicle telematics and communication systems is actually taking place—in fact, there is no evidence regarding the

[54] 2014 NOI, 79 Fed. Reg. at 55690, citing *Report of the H. Comm. on Commerce on the Digital Millennium Copyright Act of 1998*, H.R. Rep. No. 105-551, pt. 2, at 37 (1998) ("Committee Report").
[55] 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").
[56] 2010 Final Rule, 75 Fed. Reg. at 43826.
[57] House Manager's Report at 6.
[58] EFF Petition at 5.
[59] EFF Comments at 15.

market for such systems at all. In addition, no filer has commented on, let alone attempted to quantify, any adverse effects arising from the current unavailability of an exemption. For these reasons, the Proponents have failed to satisfy their burden of establishing a prima facie case for the proposed exemption, and the exemption for Class 17 as applied to in-vehicle telematics and communication systems should be denied.

IV. THE SECTION 1201(A)(1)(C) FACTORS ARE NEUTRAL OR WEIGH AGAINST GRANTING AN EXEMPTION

Although because Proponents have failed to establish a prima facie case in support of the exemption the Copyright Office does not need to address the Section 1201 test, those factors also weigh in favor of denying the proposed exemption.

Section 1201(a)(1)(C) directs that the rulemaking proceeding examine, as appropriate: (1) the availability for use of copyrighted works; (2) the availability for use of works for nonprofit archival, preservation, and educational purposes; (3) 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; (4) the effect of circumvention of technological measures on the market for or value of copyrighted works; and (5) such other factors as the Librarian considers appropriate.[60] The first and fourth factors argue in favor of denying the exemption as it would apply to in-vehicle telematics and communication systems. The second, third and fifth factors are not relevant here.[61] Finally, the Copyright Office should consider the benefits that TPMs provide, which outweigh any inconvenience to consumers.

[60] 17 U.S.C. § 1201(a)(1)(C).
[61] See 2010 Recommendation at 102; 2012 Recommendation at 77.

A. The Protections Enable Public Access to Copyrighted Works that Would Otherwise Be Threatened.

The most important aspect of the "availability" test is whether the availability of the work in a protected format "enhances or inhibits public use of the work."[62] This factor argues against granting an exemption to allow jailbreaking of in-vehicle telematics and communication systems. Granting an exemption would threaten the availability of software for such systems, and contrary to EFF's claims, would decrease their appeal for many consumers and innovators by reducing the security, safety, and privacy and emissions protections of the vehicles in which the systems were installed.[63]

In support of its position EFF argues that we are in a "golden age" of mobile devices, firmware and applications, and granting the exemption will allow increased innovation in this sector.[64] However, in-vehicle telematics and communication systems are not part of the same ecosystem as all-purpose mobile computing devices, and allowing consumers and third parties to breach the complex and critical relationship between OnStar and all other vehicle safety, security, privacy and emissions systems would offer a serious, and potentially fatal, blow to the future of automotive telematics. Protecting the underlying software by declining to extend the proposed exemption for Class 17 to in-vehicle telematics and communication systems would ensure that these systems continue to remain available and reliable. Absent this protection, vehicle manufacturers, including GM, may be forced to consider reducing offerings or withdrawing these systems from the market, rather than risk creating serious vehicle safety,

[62] 2012 Recommendation at 97 (noting that other important elements include whether the protected work is available in other formats, and, if so, whether such formats are sufficient to accommodate noninfringing uses).
[63] EFF Comments at 22.
[64] *Id.* at 21.

security, privacy and emissions risks. This statutory factor argues in favor of denying the proposed exemption.

B. The Circumvention of Technological Measures Would Harm the Market for and Value of Copyrighted Works.

The fourth statutory factor requires the Copyright Office to consider the impact of circumvention on the market for or value of the copyrighted works. EFF argues that the proposed exemption would increase the value of the copyrighted works because it would encourage innovation in the form of third parties developing applications, which in turn could make the devices more attractive to consumers.[65] However, as GM has previously noted, the market for in-vehicle telematics and communication systems is considerably different from that of other mobile communication devices. Consumers do not purchase a GM vehicle because of the availability of, or ability to remove, certain apps, and OnStar connectivity is at most a supplement to the primary function of the car, which is transportation. It is highly improbable that requiring jailbreaking of in-vehicle telematics and communication systems would increase the retail, or resale, value of automobiles. To the contrary, allowing jailbreaking could give rise to the perception of security, privacy and safety vulnerabilities that could in turn dampen the market for connected vehicles, making the presence of an in-vehicle telematics and communication system a liability rather than, as GM hopes will be the case in the future, an asset.

C. The Benefits of TPMs for Vehicle Safety Outweigh Any Chilling Effect on Consumers.

As a final consideration, Congress directed the Copyright Office in undertaking DMCA rulemaking proceedings to "consider the positive as well as the adverse effects" of TPMs on the availability of copyrighted materials. Weighing the statutory factors requires consideration of

[65] *Id.* at 24.

"the benefits that [TPMs] bring[] with respect to the overall creation and dissemination of works in the marketplace."[66] In this case, the benefits of TPMs vastly outweigh any minor inconvenience to consumers.

EFF argues that the current ban on circumvention prevents users from improving the performance of their devices by removing unwanted software.[67] However, the software that GM includes as part of the OnStar service is a critical, integrated part of the safety, security, privacy and emissions systems that control each OnStar-equipped vehicle. More is at stake than being able to upload a new video game, or remove a disfavored weather application. TPMs allow automobile manufacturers such as GM to protect the in-vehicle safety, security, privacy and emissions control features of their automobiles, which in turn enhances the safety, privacy and security of drivers, passengers, and pedestrians. Allowing consumers to breach these protective measures could lead to the reduction or elimination of these benefits, without providing any corresponding benefit for which there is any documented consumer demand. In the absence of any evidence of consumer desire to jailbreak in-vehicle telematics and communication systems, or of any harm arising from the current unavailability of this exemption, this factor weighs against granting the requested exemption.

V. CONCLUSION

Congress anticipated that exemptions from the DMCA's protections would be made "only in exceptional cases."[68] The Copyright Office should deny the proposed Class 17 exemption, or refine the class to exclude the circumvention of automotive TPMs, including jailbreaking of in-vehicle telematics and communication systems, because of unique and

[66] House Manager's Report at 6.
[67] EFF Comments at 17.
[68] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 65 Fed. Reg. 64556, 64563 (2000).

significant safety, environmental, privacy and cybersecurity risks presented in the automobile environment that do not arise in the context of jailbreaking other consumer devices such as smartphones or tablets. The Proponents have failed to establish a prima facie case for an exemption, and the statutory factors also weigh against circumvention of this important protective mechanism.

Respectfully submitted,

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

Ari Q. Fitzgerald
Anna Kurian Shaw
Deborah K. Broderson

Hogan Lovells US LLP
555 Thirteenth Street, NW
Washington, DC 20004
(202) 637-5423
Attorneys for General Motors LLC

Harry M. Lightsey III
Jeffrey M. Stefan

General Motors LLC
25 Massachusetts Avenue, NW
Suite 400
Washington, DC 20001
(202) 775-5039

March 27, 2015