Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201 (Proposed Class #22)

[ ] Check here if multimedia evidence is being provided in connection with this comment

Item 1. Commenter Information

This Comment is submitted on behalf of The Alliance of Automobile Manufacturers ("Auto Alliance"), the leading advocacy group for the auto industry. Auto Alliance represents 77% of all car and light truck sales in the United States, including the BMW Group, FCA US LLC, Ford Motor Company, General Motors Company, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche, Toyota, Volkswagen Group of America and Volvo Cars North America. For further details, see http://www.autoalliance.org/.

The Auto Alliance is represented in this proceeding by Mitchell Silberberg & Knupp LLP. Contact points for further information:

Jessica L. Simmons, Attorney, Alliance of Automobile Manufacturers, JSimmons@autoalliance.org

Steven J. Metalitz, Partner, Mitchell Silberberg & Knupp LLP, met@msk.com.

Item 2. Proposed Class Addressed

Proposed Class 22: Vehicle Software—security and safety research.

The December 12, 2014 Notice of Proposed Rulemaking ("NPRM") described this proposed class as allowing circumvention of technological protection measures ("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."[1] The exemption as proposed required any circumvention to be undertaken by or on behalf of the owner of the vehicle.[2]

Electronic Frontier Foundation ("EFF") proposes to further extend the exemption to cover "computer programs actually embedded or designed to be embedded in a motorized land vehicle ... [and] computer programs designed to modify the memory of embedded hardware … [in so far as s]uch software, such as updates and proprietary tools, raises the same security and safety concerns and is often encrypted."[3]

---

[1] 79 Fed. Reg. 73,856, 73,869 (Dec. 12, 2014).

[2] *Id.*

[3] EFF Class 22 Comment at 1.

EFF submitted the only long-form comment with evidence supporting this exemption. Professor Matthew D. Green submitted a short-form comment supporting proposed class #22 but also arguing for a broad exemption covering all good faith security research.[4]

Item 3. Overview

Auto Alliance opposes recognition of proposed class #22. In the name of encouraging efforts to improve the security of motor vehicle computer systems computer systems by "identify[ing] flaws in critical code on which hundreds of millions of Americans depend in their travels,"[5] proponents of class #22 ask the Copyright Office to recommend recognition of an exemption that seriously risks the opposite: making American motorists, passengers, pedestrians and the general public less secure and more vulnerable to threats to their personal safety.

The proposal is built on the premise that a broad exemption is needed to dispel "a legal cloud" that hovers over legitimate independent research into the security of vehicle-based systems and software. But proponents present virtually no evidence that such a cloud is impeding legitimate research. To the contrary, in numerous cases industry and independent researchers have collaborated to make vehicle systems safer and more secure. Proponents also draw the wrong conclusions from the recognition of security-related exemptions in the 2006 and 2010 rulemakings. Those exemptions targeted access control measures that themselves created security vulnerabilities, a critical feature that is completely absent here.

By arguing that the current legal landscape is too treacherous for independent researchers, proponents are in effect seeking to be freed from existing statutory constraints that are biased in favor of prudent and responsible practices – such as managing disclosure of security vulnerabilities to minimize the risk of legal violations and exploitation of those vulnerabilities by bad actors – to protect the safety and security of members of the public. For instance, under the proposed exemption, researchers who publish detailed analyses of vulnerabilities before sharing their findings with manufacturers would nonetheless benefit from a blanket exemption to circumvention liability, even though such premature publication could dramatically increase the risk of such harmful exploitations.

While some of these considerations may go beyond those "copyright interests" on which this rulemaking process has focused in recent cycles, their importance requires that they be weighed in the "balance of harms" that this proceeding requires. Under a fair calibration of that balance, this proposed exemption should be rejected. While independent security research into vehicle systems has an important role to play in protecting the safety and security of drivers, passengers, and pedestrians, that role is best advanced through collaborative efforts within the current legal landscape, rather than exposing a huge new vulnerability through a broad anti-circumvention exemption.

---

[4] Green Class 22 Comment at 1.

[5] EFF Class 22 Comment at 2.

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

N/A.

Item 5. Asserted Noninfringing Use(s)

As spelled out in the Notice of Inquiry with which this proceeding commenced, the burden which the statute imposes on a proponent with regard to claimed noninfringing uses is significant:

> A proponent must show more than that a particular use could be noninfringing. Instead, the proponent must establish that the proposed use is likely to qualify as noninfringing under relevant law. As the Register has stated previously, there is no "rule of doubt" favoring an exemption when it is unclear that a particular use is a fair use. Rather the statutory language required that the use is or is likely to be noninfringing, not merely that the use might plausibly be considered noninfringing. And, as noted above, the burden of proving that a particular use is or is likely to be noninfringing belongs to the proponent.[6]

Proponents fall well short of satisfying this burden with respect to proposed class #22. Their theory that the uses they wish to make of the vehicle firmware might plausibly be considered noninfringing under the software-specific exception in Section 117 of the Copyright Act does not rise to the level of "proving that a particular use is or is likely to be noninfringing." While their fair use argument may be stronger, it is undermined by an unjustified reliance on previous exemptions granted in this proceeding that were labeled as applying to security research, but that actually addressed a significantly different problem – security vulnerabilities *caused by access controls* – that is not present here.

A. Proponents have failed to prove that vehicle owners are owners of copies of Electronic Control Unit ("ECU") firmware within the meaning of 17 U.S.C. § 117.

Under Section 117, the unauthorized exercise of certain exclusive rights in computer programs[7] is declared noninfringing under specified circumstances, but only if carried out or authorized by "the owner of a copy of a computer program." In several past rule-making cycles, the Copyright Office has grappled with the issue of determining when a party in possession of a copy of (and authorized to use) a computer program is an owner of that copy, and when she is

---

[6] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies; Notice of Inquiry and Request for Petitions, 79 Fed. Reg. 55,687, 55,690 (Sept. 17, 2014) ("2014 NOI") (citations omitted, emphasis in original).

[7] Since Section 117 applies only to computer programs, EFF cannot rely upon it at all to establish that activities undertaken after circumventing access controls on "compilations of data" are or are likely to be noninfringing. *See* EFF Class 22 Comment at 1.

merely a licensee.[8] Only in the most recent (2012) rulemaking cycle did the Copyright Office have to analyze the Ninth Circuit decision in *Vernor v. Autodesk, Inc.*, 621 F.3d 1102 (9th Cir. 2010), in which the court spelled out three clear criteria for making this determination:

> We hold today 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.[9]

Measured against these criteria, proponents' own submission makes it quite clear that under the *Vernor* analysis, vehicle owners are licensees of the firmware embodied in the ECUs of their vehicles, and not owners of copies of these programs. Therefore, Section 117 does not apply. Pages 13-14 of the EFF submission quote at length from end use license agreements ("EULAs") for auto-related software programs, most of which characterize themselves as a grant of a license; most of which specifically prohibit transferring or otherwise making available the software to others; and all of which impose use restrictions that can only be described as "notable," including in particular prohibitions on reverse engineering.[10]

In the most recent (2012) rulemaking cycle (the first since V*ernor* was decided), in the context of a proposed exemption for circumvention of firmware on smartphones, the Copyright Office noted that "proponents have made only a cursory attempt at responding to *Vernor*."[11] In this cycle, proponent EFF has fallen even farther short of succeeding in distinguishing *Vernor*: it has completely mis-stated the holding of that case. *Vernor*'s holding is correctly stated above as a verbatim quotation. *Vernor* emphatically did <u>not</u> hold what EFF says on page 12 of its submission that it held: that a list of five "formal and informal factors" needs to be considered. Instead, EFF's submission directly paraphrases the *Vernor* court's summary of a Ninth Circuit case decided 35 years earlier (three years before Section 117 was even enacted), *United States v. Wise*, 550 F.2d 1180 (9th Cir. 1977). The *Vernor* court specifically <u>rejected</u> the argument that "*Wise* is the controlling precedent."[12]

EFF also cites to *Krause v. Titleserv* 402 F.3d 119 (2nd Cir. 2005), a Second Circuit decision that is arguably more favorable to their position that vehicle owners own the firmware copies embodied in the vehicle ECUs. However, the sharp factual disjunction between the

---

[8] *See, e.g.*, Recommendation of the Register of Copyrights, Section 1201 Rulemaking: Fifth Triennial Proceeding, 91-93 (Oct. 12, 2012) ("2012 Recommendation"). All cited materials from previous rulemaking cycles can be accessed via the U.S. Copyright Office website at http://www.copyright.gov/1201/ under "Past Proceedings."

[9] 621 F.3d at 1111.

[10] *See, e.g.*, EFF Class 21 Comment at 13-14 (quoting EULAs accompanying various ECUs, and the use restrictions imposed on them, including for OnStar, Ford Sync, Toyota Safety Connect, and the Mercedes-Benz mbracy System)

[11] 2012 Recommendation at 92.

[12] *Vernor*, 621 F.3d at 1113.

scenario in *Krause* and the one applicable here counsels against reliance on that case. Unlike in *Krause*, the copyright owners here are not claiming that they wrote the firmware as employees of the would-be "tinkerers" and that they received significant compensation for doing so. Nor is this a case, like *Krause*, in which there is no written license agreement to point to as evidence of the intent of the parties in defining their relationship. Clearly the facts here are far more similar to those surrounding the shrink-wrap mass market licenses in *Vernor* than to the custom software, employer-employee relationship in *Krause*. For the reasons well stated by the *Vernor* court itself,[13] the *Krause* decision is distinguishable, and proponents have failed to make a persuasive case why it should be controlling.

Auto Alliance is aware that in the portion of the 2012 Recommendation dealing with Section 117, even though proponents of the smartphone unlocking exemption "failed to present any evidence in support of ownership," the Copyright Office elected to excuse them from doing so, on the grounds that the law was too uncertain to enable an evaluation of any such evidence, even if the proponents had chosen to offer it. The Copyright Office then declared itself "compel[led]" to find that "some subset of wireless customers – that is anyone considered to own the software on their phone under applicable precedent – is entitled to exercise the Section 117 privilege."[14] While we find it difficult to square this reasoning with the benchmark principle that the proponents must prove through their evidence that each use that they wish to make "is or is likely to be noninfringing," we, of course, have neither desire nor standing to re-litigate that aspect of the Copyright Office's 2012 Recommendation, and note that the particular instance in which the Copyright Office followed this path three years ago has at least been overtaken, if not rendered moot, by intervening legislation.[15] Under these circumstances, we simply urge the Copyright Office not to repeat this practice here. Just as somewhere, somehow, some smartphone user might be able to establish that she was under applicable law the owner of the firmware in her phone, and thus entitled to exercise the Section 117 privileges, the same could conceivably be true of some motor vehicle owner; but in the absence of specific evidence in the record demonstrating the likelihood of such a finding in more than isolated instances, the proponents' burden of proof has not been met, and Section 117 cannot be relied upon to prove noninfringing use.

B. <u>Even if they are owners of copies, "tinkerers" have not established that their proposed uses are noninfringing under Section 117</u>.

To the extent that some would-be "tinkerers" could demonstrate that they are owners of the copies of firmware in the ECUs of their vehicles, their use would be noninfringing only if it fell within one of the categories specified in Section 117. Proponents' evidence falls well short of establishing that any of the statutorily permitted uses is involved here.

---

[13] *Vernor*, 621 F.3d at 1114.

[14] 2012 Recommendation at 92-93.

[15] Unlocking Consumer Choice and Wireless Competition Act, 128 Stat. 1751 (February 26, 2014).

Section 117(a)(1) permits the making of copies or adaptations by (or authorized by) the owner of the copy "as an essential step in the utilization of the computer program in conjunction with a machine." Proponents concede that the modifications they wish to make are "not essential to using the vehicle software for routine driving purposes"; but they argue that making a copy or adaptation on an entirely distinct and separate "machine," such as "a commercial reflash tool or a general purpose computer on which the code will be analyzed in order to understand its functionality," satisfies Section 117(a)(1).[16] While some courts have been fairly liberal in interpreting this phrase to apply not only to the original computer system on which the software was first installed, but also to subsequent versions or upgrades of that computer system,[17] proponents point to no case in which the "machine" in question was so markedly different than the one on which the software before copying or adaptation was designed to run.

Section 117(a)(2) allows the making of copies or adaptations by (or authorized by) the owner of the copy "for archival purposes only and [provided] that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful." Archival copies are defined as only those copies that "guard against destruction or damage by mechanical or electrical failure;" the Section 117(a)(2) exception does "not extend to other copies of the program."[18] Most of EFF's argument on this point deals with circumvention for the purpose of modification (proposed class #21) rather than for security research, but it does seem to argue that for security researchers, "[b]ackup copies are important to establish a baseline if modifications are to be made, and to ensure that an ECU can be restored to its original state if it is compromised by *experimentation*."[19] Experimentation, whether by owners or by independent security researchers acting on behalf of an owner of the copy, falls well outside the exemption allowed by Section 117(a)(2) for protection from mechanical or electrical failure.

C. Proponents' fair use argument fails because it is based on a false premise about prior exemptions recognized in this proceeding.

The gravamen of EFF's fair use argument in the context of proposed class #22 is one based on precedent in this proceeding. EFF's submission calls the exemption recognized by the Librarian in 2010, related to security flaws or vulnerabilities in video games, "comparable" to the one it seeks in this proceeding.[20] EFF's view is that because the Copyright Office found that, in the circumstances of that exemption, it was likely that the activities of the security researcher constituted fair use, the same path should be followed to the same conclusion with regard to this proposed class. This argument is unpersuasive, because its basic premise is false. In fact, the 2010 exemption, as well as a similar security-related exemption recognized by the Librarian in

---

[16] EFF Class 22 Comment at 15.

[17] *E.g.*, *Krause*, 402 F.3d at 125-26.

[18] *Atari, Inc. v. JS & A Grp., Inc.*, 597 F. Supp. 5, 9 (N.D. Ill. 1983) (quoting CONTU Report at 31).

[19] EFF Class 22 Comment at 16 (emphasis added).

[20] EFF Class 22 Comment at 8.

2006, fundamentally differ from proposed exemption #22 in this proceeding. Both the previous exemptions targeted security vulnerabilities caused by access controls themselves. This key fact shaped not only the Copyright Office's fair use analysis, but also its consideration of the applicability of statutory exceptions (notably Section 1201(j) for security testing), and of the evidentiary record that the existence of possible liability under Section 1201(a)(1)(A) was discouraging legitimate security research. But nothing in the record for proposed exemption #22 suggests that the access controls that proponents seek to circumvent play any role in causing the security vulnerabilities which they wish to research.

Both the 2006 and 2010 security-related exemptions were limited to testing, investigating and correcting security flaws that were caused by access controls. The 2006 exemption targeted "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."[21] One such access control was part of the XCP software, which included a "rootkit [that] creates security vulnerabilities by providing a cloak that conceals malicious software."[22] The Register specifically found that "a significant number of sound recordings have been distributed on CDs with access controls that create security vulnerabilities," and that this "deployment by copyright owners of such dangerous DRM software shifts the balance in favor of an exemption."[23]

Similarly, in 2010, the Register's Recommendation stated that the "starting point in this analysis is limited to video games on personal computers protected by technological protection measures that control access to lawfully obtained works and create or exploit security flaws or vulnerabilities that compromise the security of personal computers."[24] The Register was asked to recognize a broader class, covering works other than videogames, but she declined to do so, because with respect to such works "there is no evidence that such measures are likely to create security flaws or vulnerabilities."[25] The Register proceeded to consider the evidence about "two types of access controls applied to video games," but found that as to one of these (SecuROM) "there is no clear evidence in the record that tends to prove that SecuROM is creating or is likely to create, security flaws or vulnerabilities," and consequently the record on SecuROM was

---

[21] Recommendation of the Register of Copyrights in RM 2005-11; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 53-54 (Nov. 17, 2006) ("2006 Recommendation") (emphasis added).

[22] *Id.* at 55.

[23] *Id.* at 61, 63.

[24] 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, 178 (June 11, 2010) ("2010 Recommendation").

[25] *Id*. at 177 (emphasis added). *See also id*. at n. 574 (dismissing a cited article because it "does not reveal any evidence of security flaws or vulnerabilities caused by [Microsoft's Silverlight] technology")

"insufficient to support the recommendation of an exemption."[26] However, the Register did find that the other videogame access control, SafeDisc, "has created a verifiable security vulnerability on a large number of computers" – indeed, a vulnerability "affecting potentially a billion personal computers."[27]

The evidence in this proceeding is completely different from that which led the Register to recommend, and the Librarian to recognize, security-related exemptions in 2006 and 2010. The access controls assertedly at issue in proposed class #22 are challenge-response mechanisms, encryption, and physical configurations such as the disabling of access ports.[28] Proponents complain about these access controls because they are more or less difficult to circumvent in order to gain access to the computer programs they protect (and which proponents wish to copy). In some cases, they say that the access controls in place are insufficiently robust. Proponents have put forward considerable evidence to buttress their view that ECUs and other elements of motor vehicle computer networks are not as secure as they should be, and are vulnerable to various kinds of attacks. But there is not a whisper in the record that the use of these particular access controls has caused these vulnerabilities, or that these forms of access controls exploit other vulnerabilities which were previously lying dormant in the network.

In short, this proposed security-related exemption is entirely different from any that the Copyright Office has previously recommended or that the Librarian has previously recognized. A simple test illustrates the difference: would users of the systems in question (personal computers, in 2006 and 2010; cars, today) be more secure if the access controls in question were simply removed and discarded? The Register's answer in the earlier proceedings was clearly yes; but no proponent has asserted that the answer is yes with regard to this proceeding. The records of the 2006 and 2010 proceedings, far from establishing a precedent that the current proposal should be adopted, in fact tend to support its rejection.

Clarifying the basis for the previously recognized security-related exemptions is also critical to an understanding of the Register's previous pronouncements on the applicability of the statutory exception for security testing (Section 1201(j)). When an access control measure, like the Sony XCP rootkit or the Microsoft SafeDisc, causes a security vulnerability, the way to cure that problem is to remove the access control. Accordingly, as the Register phrased it in her 2006 Recommendation, "The question, then, is whether the exemption in §1201(j) offers sufficient protection for persons who remove or inactivate access controls that pose threats to the security of a computer."[29] In the 2006 proceeding, the proponents of the security-related exemption "argued that § 1201(j) 'appears to permit the ethical hacking into a computer system for the purpose of detecting security flaws in the firewall protecting the system. It is not clear that it permits the permanent disabling of a technological measure on a specific work when the measure

---

[26] *Id.* at 187-88 (emphasis added).

[27] *Id.* at 188, 194 (emphasis added).

[28] EFF Class 22 Comment at 4-6.

[29] 2006 Recommendation at 57.

causes a vulnerability.'"[30] The Register ultimately concluded that she shared "the uncertainty whether § 1201(j) addresses the situation presented by this proposal," *i.e.*, circumvention for the purpose of disabling a harmful access control.[31] Similarly, in 2010, the Register focused on the question whether Congress, in enacting Section 1201(j), had "anticipate[d] this precise scenario involving access controls creating vulnerabilities."[32] She concluded that "Congress, at the time of enactment, had no reason to be concerned about flaws or vulnerabilities that might be introduced into the computer, system or network ecosystem by a technological protection measure itself."[33]

The questions posed by the Register in 2006 and 2010 about the scope of Section 1201(j) are completely irrelevant to the question at hand in this proceeding, which does not involve security vulnerabilities created by access controls, and in which no security researcher is seeking simply to extract from an ECU an access control and discard it in order to address a security problem. Thus, a *de novo* consideration of the full landscape surrounding security research on software resident in automobiles, including the role of the security testing exception in that context, is required.

Item 6. Asserted Adverse Effects

Proponents have failed to demonstrate that Section 1201(a)(1)(A) is impeding or "chilling" any legitimate security research – the main thrust of their argument about adverse effects.

Perhaps because the security vulnerabilities at issue in the 2006 and 2010 rulemakings were inherent features of commercial products that were actively marketed for use with music CDs (in 2006) and PC videogames (in 2010), proponents were able to present "comments and testimony…to show that some legitimate research has been, or is likely to be, adversely affected" by the prohibition on circumvention.[34] The principal proponent of the 2010 exemption made much of the assertion that he had previously been threatened with a lawsuit by a "manufacturer of insecure technological measures,"[35] and cited "a regime of panic, protests and litigation" surrounding SecuROM.[36] Nothing remotely similar can be gleaned from the record in this proceeding.

---

[30] *Id.* at 58-59.

[31] *Id.* at 59.

[32] 2010 Recommendation at 196.

[33] *Id.* at 199.

[34] *Id.* at 195.

[35] 2010 Proceeding, Halderman Comment 8A at 18 (Dec. 2, 2008). The threat (later withdrawn) was said to have occurred "prior to the third rulemaking," *i.e.*, before 2005, or at least a decade ago. *See* Halderman Comment 8A at 2.

[36] 2010 Recommendation at 201 (citing Halderman Comment 8A at 7).

In fact, although proponents repetitively assert that Section 1201 is "casting a legal cloud over otherwise-lawful security and safety research," on closer inspection this cloud more closely resembles vaporware.[37] While in one statement submitted by EFF, one security researcher states "I live in constant fear that the DMCA will be used as a tool by the manufacturers to stop this safety critical research from continuing," no evidence whatsoever has been submitted that would tend to show that this fear is reasonable.[38] The only other security researcher whose statement is submitted by EFF describes "several barriers" that he had to overcome, but none of these barriers involve the threat of legal proceedings or liability, and the statement makes no mention of these.[39] Another proponent refers to the need for researchers to "undertake good faith studies of vehicle software … without fear of prosecution under Section 1201," but provides no evidence that any such prosecutions have ever been threatened, or even contemplated, much less initiated.[40]

The EFF submission cites to a PC World article about a BMW remote unlocking issue, in which one Joshua Corman is quoted as saying that "because of laws like the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act, some researchers are hesitant to come forward with vulnerabilities lest they be accused of hacking and prosecuted."[41] No specifics are provided to buttress this observation, which of course mentions two statutes, only one of which is relevant to this proceeding.[42] Certainly if there is an objective basis for these fears, worries and accusations, it is part of proponents' burden to fully and persuasively document it. That has not been done here.

In fact, independent research into the safety and security of computer systems in motor vehicles appears to be a growth business, thriving and even attracting federal government

---

[37] EFF Class 22 Comment at 3; *see also id.* at 18, 21.

[38] EFF Class 22 Comment, Appendix B, Statement of Charlie Miller ("Miller Statement") at ¶ 9.

[39] EFF Class 22 Comment, Appendix D, Statement of Chris Valasek ("Valasek Statement") at ¶ 3-4.

[40] Green Class 22 Comment at 1.

[41] EFF Class 22 Comment at 18, n. 123 (citing Martyn Williams, *BMW Cars Found Vulnerable in 'Connected Drive' Hack*, PCWORLD (Jan. 30, 2015), http://www.pcworld.com/article/2878437/bmw-cars-found-vulnerable-in-connected-drive-hack.html). Although the statement is surrounded by quotation marks in the EFF submission, it is not presented as a direct quote in the underlying article.

[42] It has been clear since its inception that adverse impacts that are "not clearly attributable to … [the] prohibition" in Section 1201(a)(1)(A) "are outside the scope of the rulemaking." Staff of House Committee 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, 6 (Comm. Print 1998), *reprinted in* 46 J. COPYRIGHT SOC'Y U.S.A. 635 (1999) ("Manager's Rep."). This would include adverse impacts attributable to another statute, such as the Computer Fraud and Abuse Act.

support.[43] EFF asserts that "this research is of such crucial importance that experts have received funding from multiple government agencies to support it,"[44] and repeatedly references the federal agency funding sources of the research they say epitomizes the activities in need of an exemption.[45] Proponents have submitted virtually no evidence that the existence of the anti-circumvention prohibition in Section 1201(a)(1) – as constrained by the existing statutory exceptions, including but not limited to Section 1201(j)(2) – has impeded or hindered in any meaningful way the ability of responsible independent researchers to conduct the research they describe in their submissions, and to publicize the results both through academic or technical publications and in the popular media.

Nor is there any evidence in the record of industry actions or pronouncements that could be perceived as hostile to the concept of input from independent security researchers in addressing the significant safety and security challenges that inevitably accompany the growing computerization of modern motor vehicles. To the contrary, while there may have been frictions and disagreements in specific cases about how and when independent research results should be publicly presented, the auto industry clearly recognizes that independent researchers have an important role to play in flagging potential vulnerabilities, and works with them in a number of fora to learn about the problems they have identified and to devise solutions to them. Among these fora are the relevant committees of SAE International (formerly the Society of Automotive Engineers), such as the SAE Vehicle Electrical System Security Committee ("VESSC"), in which academics, consulting firms, government entities and other interested parties participate.[46] Technical experts from auto manufacturers also participate in major gatherings of "ethical hackers" such as DEF Con and Black Hat. High levels of industry participation in the annual SAE Battelle Cyber Auto Challenge, which brings together teams of students, auto industry professionals, government personnel, hackers, researchers, and STEM (science, technology, engineering, and mathematics) educators to tackle real-world cybersecurity problems (such as those posed by connected vehicle systems) is further evidence of industry commitment to supporting "both formal and experiential platforms to allow auto engineers, designers, tech and communications security experts to coalesce."[47]

---

[43] *See, e.g.*, EFF Class 22 Comment at 18, n. 127 (citing Ishtiaq Rouf *et al.*, *Security and Privacy Vulnerabilities of InCar Wireless Networks: A Tire Pressure Monitoring System Case Study*, USENIX SECURITY 2010, 1, http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf ("This study was supported in part by the US National Science Foundation…and [the] Army Research Office."); *see also* EFF Class 22 Comment at 2, 6.

[44] EFF Class 22 Comment at 2.

[45] EFF Class 22 Comment at 2, 6, 8.

[46] *See* SAE VESSC Class 22 Comment.

[47] Stephen E. Kelly, *Diversity of opinions makes for stronger car data security*, THE HILL (Mar. 6, 2015), http://thehill.com/blogs/congress-blog/technology/234800-diversity-of-opinions-makes-for-stronger-car-data-security.

The BMW remote unlocking issue in the article cited by EFF provides a useful but far from unique illustration. After learning of the vulnerability identified by independent researchers, BMW promptly "collaborated with [the] researchers to understand and develop a fix for two of the most critical flaws. BMW remotely updated its customers' vehicles, adding HTTPS encryption and server authentication checks. BMW then announced the details of what they found, how they fixed it, and what other measures they have already taken to protect the safety of drivers, passengers, other vehicles, pedestrians, etc." Joshua Corman – the same Joshua Corman quoted by EFF for the proposition that some researchers hesitate to disclose vulnerabilities "lest they be accused of hacking and prosecuted" – concluded last month that "this is a big, positive step forward for cyber safety in automobiles."[48]

As another step forward toward greater collaboration with diverse sources in addressing these issues, the Auto Alliance is collaborating with the Association of Global Automakers,[49] and with the encouragement of the leading federal regulatory agency, the National Highway Traffic Safety Administration, to establish a voluntary automobile industry sector information sharing and analysis center ("Auto-ISAC"), along the lines of those in successful operation in some other industry sectors.[50] Once in operation, the Auto-ISAC will provide yet another forum for ingesting the results of independent research on auto cybersecurity and cybersafety issues and disseminating these across the industry for response, as part of the industry's overall efforts to more effectively counter cyber threats in real time by safeguarding vehicle computer systems.

Item 7. Statutory Factors

As the Copyright Office recognized in setting the ground rules for a previous rulemaking cycle of this proceeding, "the harm identified by a proponent of an exemption must be balanced with the harm that would result from an exemption. In some circumstances, the adverse effect of a proposed exemption in light of these considerations may be greater than the harm posed by the prohibition on circumvention of works in the proposed class."[51] The Auto Alliance urges the Copyright Office to acknowledge that this proposal presents one of those circumstances, in which the balance of harms counsels rejection of the proposed exemption.

The preceding section of this comment demonstrated that "the harm posed by the prohibition" to the performance of legitimate security research is minimal. But even if it were

---

[48] *Assessment of BMW Door Lock Security Updates*, I AM THE CAVALRY (Feb. 12, 2015), https://www.iamthecavalry.org/news/

[49] Global Automakers represents international automakers that design, build, and sell automobiles in the U.S. It currently represents 12 automakers including: Hyundai, Honda, Toyota, Aston Martin, Kia, McLaren, Subaru, Ferrari and others. *See* http://www.globalautomakers.org/about.

[50] Kelly, *Diversity of opinions makes for stronger car data security*, *supra* note 47.

[51] Exemption to the Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies; Notice of Inquiry and Request for Petitions, 76 Fed. Reg. 60,398, 60,403 (Sept. 29, 2011) ("2011 NOI").

considerably greater, it would be outweighed by the harms that would result from granting the exemption proponents seek. These harms include greatly increased risks to the safety and security of every American motorist, passenger, and pedestrian.

In the statutory exceptions to the prohibition on circumvention of access controls, notably Section 1201(j), Congress anticipated the need for responsible independent security research to investigate vulnerabilities of computer systems or networks, and to correct those vulnerabilities that were identified. The statute also communicates a strong Congressional bias toward prudence and caution in disclosing results, lest disclosure degrade the security of all current and future users of that system or network

Clearly the proponents of this exemption find the existing environment too constricting, and seek to persuade the Copyright Office that in order to carry out their activities, a further administrative exemption is required to allow them to venture farther afield. The goal of their bushwhacking itinerary seems to be unrestricted disclosure of security vulnerabilities on their own terms and timetable. As part of its assertion that none of the statutory exceptions to the Section 1201(a)(1)(A) prohibition, even taken together, are sufficient to "mitigate" what it considers to be the adverse effects of the prohibition,[52] EFF's discussion of Section 1201(j) centers on the issue of disclosure.[53] It is essentially because proponents of the exemption wish to publish their findings "to advance the state of knowledge for all" that they assert that Section 1201(j) does not provide sufficient shelter for their activities.[54] In fact, unless one accepts proponents' premise that any publication of security research results is necessarily incompatible with Section 1201(j), their claimed need to exceed the limits of the statutory exception appears to

---

[52] *See* EFF Class 22 Comment at 19-22. EFF addresses Section 1201(j) along with the two statutory exceptions identified by the Copyright Office in the NPRM as potentially relevant to this proposed administrative exemption. *See* NPRM at 73,869 ("The applicability (or not) of the statutory exemptions for reverse engineering in 17 U.S.C. 1201(f) and encryption research in 17 U.S.C. 1201(g) to the proposed uses."). In considering whether proponents of Class #22 have met their burden in this proceeding to demonstrate persuasively that their activities are not covered by any applicable statutory exception, the Copyright Office should take into account EFF's failure even to mention Section 1201(e), which provides a blanket exception for "information security … activity of … a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State." 17 U.S.C. § 1201(e). In light of EFF's repeated references to the federal agency funding sources of the research they say epitomizes the activities in need of an exemption, this omission is striking.

[53] EFF's other arguments turn largely on the precedent of the security-related exemptions recognized in the 2006 and 2010 cycles. *See* EFF Class 22 Comment at 22. As discussed in Item 5 of this comment, those exemptions, and the analysis of section 1201(j) that supported their recognition, addressed a wholly distinct factual scenario – access controls that caused security vulnerabilities – than is presented here, and thus provide no support for recognition of proposed class #22.

[54] EFF Class 22 Comment at 22.

boil down to a desire to publicize the security vulnerabilities they have identified at a time and in a level of practical detail that they unilaterally choose, without regard for the consequential risks.

Proponents' position, if adopted, would result in disclosure of research results in a manner that would facilitate violations of applicable law. Premature publication of security vulnerabilities in auto-based computer systems dramatically increases the risks of just such an outcome. When researchers choose to publish detailed analyses of vulnerabilities before communicating their findings to system operators or developers – in this case, to manufacturers who are in a position to develop and implement corrective measures – they are "advancing the state of knowledge" for bad actors as well as for the general public. EFF may be correct that "bad actors seeking to harm persons or property in violation of criminal law are unlikely to be deterred by the legal ban on circumvention,"[55] but that is no reason for the Copyright Office to recommend modifying that ban in a way that will make the job of such bad actors easier.

EFF's submission details a long list of reported vulnerabilities whose exploitation could directly threaten driver, passenger and public safety as well as privacy. The list includes remote disabling of brakes and other critical functions; remote control of ECUs; delay or non-deployment of seat belt pre-tensioners and airbags; unintended acceleration; inability to start or turn off the car; remote spoofing of safety messages; and many more.[56] Without commenting on the credibility or risk level of any particular allegation, it is ironic that in the name of some of those who have helped to bring these deficiencies to light, the Copyright Office is being asked to approve a new exemption that is likely to increase the risk that these deficiencies will be exploited to harm others.

In the Notice of Proposed Rulemaking, the Copyright Office asked proponents of this exemption "whether granting the exemption could have negative repercussions with respect to the safety or security of vehicles, for example, by making it easier for wrongdoers to access a vehicle's software."[57] EFF's brief and superficial response paints a false dichotomy between "widespread testing and challenging of systems" and "concealing vulnerabilities," leaving no room for the realities summarized in Item 6 above, in which systems are being robustly tested (both by auto manufacturers themselves and by independent researchers) and vulnerabilities, once identified, are addressed.[58] EFF then recycles the argument that legitimate researchers are

---

[55] EFF Class 22 Comment at 24.

[56] *See* EFF Class 22 Comment at 16-17.

[57] NPRM at 73,869.

[58] EFF Class 22 Comment at 24. One of the researchers cited in EFF's response complains that after the encryption algorithm used to prevent tampering with immobilizer systems was hacked, the proprietor substituted a more robust encryption algorithm, which "increases the time and cost necessary to do valid research." EFF Class 22 Comment, Appendix C, Statement of Craig Smith ("Smith Statement") at ¶ 8 (cited in EFF Class 22 comment at 24, n. 146). Since the purpose of the access control is to provide security, not to provide short-cuts to researchers, and since EFF acknowledges that more robust encryption is harder to break, see EFF Class 22 Comment at 5, this complaint substantially undermines EFF's argument.

deterred by "legal uncertainty." While granting the proposed exemption would in a sense increase certainty – any circumvention of access controls in autos carried out by anyone claiming to be a researcher would more certainly be immunized from liability – the actual impact of any existing "uncertainty" on legitimate research seems barely perceptible, as discussed in Item 6 above.

The common ground here between proponents of this exemption and its opponents is the general proposition that independent security research is the type of activity that could discover potential vulnerabilities whose exploitation could compromise the safety and security of drivers, passengers, pedestrians, and the general public. The divergence, however, is whether this reality is best managed through collaborative efforts within the current legal landscape, as summarized in Item 6 above, or whether an additional exemption is needed, whose foreseeable consequence is to increase the risk that such harmful exploitation of the vulnerabilities will occur. Auto Alliance urges the Copyright Office to take these risks fully into account in striking the balance of harms identified in the 2011 NOI.

Auto Alliance is aware that in past rulemaking cycles, the Copyright Office has been unreceptive to objections to proposed exemptions that it perceives to be motivated by harms to "business interests" rather than "copyright interests." Without regard to whether that distinction – which is not mandated or even referenced in the statute – was appropriately applied in the past, Auto Alliance urges the Copyright Office not to do so here to exclude or to deprecate consideration of the risks to public safety and security that could flow from a decision to allow unrestricted circumvention of access controls on vehicle firmware in order to carry out security research that exceeds the boundaries within which such activities are already exempted by statute from the prohibition on such circumvention. A major purpose of these access controls is to reduce the risk that unauthorized third parties will gain control over critical vehicle systems and introduce safety critical faults into vehicle operation.

EFF is correct that "code is necessary for vehicles to function and is produced for non-copyright related reasons."[59] But they are wrong to assert that allowing unrestricted circumvention of access controls protecting that code will produce "no market harm cognizable by copyright law." Auto Alliance submits that, as part of his discretion to consider additional "appropriate" factors in this proceeding, the Librarian can and should take fully into account the vital "non-copyright" risks that granting an exemption for proposed class #22 would create or exacerbate; and that at this stage of the proceeding, the Copyright Office should strongly recommend that he do so, as part of the reason for rejecting the proposed exemption.[60]

[59] EFF Class 22 Comment at 22-23.

[60] 17 U.S.C. § 1201(a)(1)(C)(v).

Item 8. Documentary Evidence

None submitted.