UNITED STATES COPYRIGHT OFFICE

Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201

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

ITEM A. COMMENTER INFORMATION

The Alliance of Automobile Manufacturers ("Auto Alliance") submits this comment in opposition to the adoption of the proposed exemption of Class 10. The Auto Alliance is 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, Assistant General Counsel, Alliance of Automobile Manufacturers, JSimmons@autoalliance.org

Kevin M. Rosenbaum, Of Counsel, Mitchell Silberberg & Knupp LLP, kmr@msk.com

This comment is joined by The Association of Global Automakers ("Global Automakers"):[1] 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, Nissan, Subaru, Ferrari and others.

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 10: Computer Programs – Security Research

The existing exemption codified at 37 CFR 201.40(b)(7) allows circumvention of access controls on motor vehicle software for good-faith security research of computer programs, subject to a number of limitations ("existing exemption"). The December 18, 2017 Notice of Proposed Rulemaking (NPRM) described Class 10 as expanding the existing exemption.[2] The NPRM further identified petitions seeking to remove the following limitations from the existing exemption: (1) the categories of devices listed in the existing exemption ("Device Limitation"); (2) the requirement that circumvention is done on a "lawfully acquired device or machine" ("Lawfully Acquired Limitation"); (3) the requirement that circumvention is done "solely" for the purpose of good-faith security research ("Good Faith Limitation"); (4) the requirement that circumvention "not violate applicable law" ("Illegality Limitation"); (5) the requirement that

[1] *See About Us*, GLOBALAUTOMAKERS, http://www.globalautomakers.org/about (last visited Feb. 8, 2018).
[2] *See Exemptions To Permit Circumvention of Access Controls on Copyrighted Works: Notice of Proposed Rulemaking*, 82 Fed. Reg. 49550, 49562 (Oct. 26, 2017) ("NPRM").

security research is "carried out in a controlled environment designed to avoid any harm to individuals or the public" ("Controlled Environment Limitation"); and (6) the requirement that "information derived from the activity is used primarily to promote . . . security or safety . . . and is not used or maintained in a manner that facilitates copyright infringement" ("Use Limitation").[3]

In their comments on the proposed exemption of Class 10, Center for Democracy and Technology (CDT), Professors Ed Felten and J. Alex Halderman (FH), and the U.S. Public Policy Council of The Association for Computing Machinery (USACM) argue that all limitations identified in the Notice to the existing exemption should be eliminated. Other proponents advocate for removal of one or more of the limitations.

This comment addresses only aspects of the proposed exemption that directly impact the automobile industry, and takes no position on any other issues raised by proponents. Since motorized land vehicles are already listed in the existing exemption as devices on which circumvention is allowed (despite the prohibition in Section 1201(a)(1)(A)), Auto Alliance and Global Automakers take no position on modification of the Device Limitation. For the reasons stated below, we oppose relaxation or removal of the other limitations, with respect to circumvention for security research on automobiles. These comments do not address whether any of the other limitations should be relaxed or removed with respect to circumvention for security research on any other devices.

ITEM C. OVERVIEW

In the name of improving "both the security of our nation and the security of our lives,"[4] proponents of Class 10 ask the Copyright Office to radically expand the existing exemption in a manner 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 and security. The proposal is built on the premise that a broader exemption is needed so that independent security researchers can "work without fear of substantial legal liability."[5] But proponents present virtually no evidence that this supposed fear is impeding legitimate research to enhance automotive security. To the contrary, collaboration between industry and independent researchers is flourishing, resulting in vehicle systems that are safer and more secure.

By arguing that the existing exemption impedes independent research, proponents are in effect seeking to jettison prudent and responsible practices that protect the safety and security of

[3] Although the NPRM characterized the Use Limitation as "information derived from the activity . . . is not used or maintained in a manner that facilitates copyright infringement," the two petitions referenced in the NPRM, Felten & Halderman (FH) Class 10 Petition and Center for Democracy and Technology (CDT) Class 10 Petition, appear to identify both prongs of the "use" clause ("the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement") and their comments also clearly advocate for removal of the broader clause. *See* Felten and Halderman, Class 10 Long Comment at 25 (Dec. 18, 2017) ("FH Comment"); CDT, Class 10 Long Comment at 5 (Dec. 18, 2017) ("CDT Comment"). In this comment, therefore, the Auto Alliance and Global Automakers respond to proponents' arguments for removal of both prongs of this clause.
[4] *See* FH Comment at 3.
[5] *See id.* at 4.

members of the public. These common-sense practices include managing disclosure of security vulnerabilities to minimize the risk of legal violations and exploitation of those vulnerabilities by bad actors, and taking reasonable safety precautions when interfering with motor vehicle systems. For instance, by removing the Use Limitation, researchers who adhere to a rigid program of publishing 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 destructive exploitations. This would undermine the numerous vulnerability disclosure programs that automobile manufacturers have developed with third party security researchers. Such programs provide the framework for substantially increased collaboration between automobile manufacturers and security researchers, allowing manufacturers the opportunity to remedy vulnerabilities before the information can fall into the wrong hands.

Even if there were any significant evidence in the record that anything in the existing exemption impedes legitimate noninfringing activities regarding automobile security research – which there is not – the Office should reject these proposals, because their adoption would threaten, not enhance, public safety. While some of these considerations may go beyond those "copyright concerns" on which the Copyright Office has indicated this rulemaking process should be principally focused, 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 new vulnerabilities through a broadened anti-circumvention exemption.

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

N/A

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

I. Uses Enabled By Radically Expanded Exemption Not Likely To Be Noninfringing

As the Copyright Office noted in its 2017 Report on Section 1201 (1201 Report), proponent has the burden to demonstrate that "uses affected by the prohibition on circumvention are or are likely to be noninfringing."[6] The 1201 Report further spells out the significant burden which the statute imposes on a proponent regarding claimed non-infringing uses: "In determining whether a use is likely noninfringing, the office has stated that '[t]he statutory language requires

[6] *See* U.S. Copyright Office, *Section 1201 of Title 17: A Report of the Register of Copyrights* 27 (2017) ("1201 Report"). The NPRM refers to the 1201 Report as well as prior recommendations for "the substantive legal and evidentiary standard for the granting of an exemption under section 1201(a)(1)." *See* NPRM at 49551.

that the use is or is likely to be noninfringing, not merely that the use might plausibly be considered noninfringing.'"[7] Proponents have failed to meet this burden.

Although acknowledging that this class includes at least some works protected by copyright, FH argue, without providing any evidentiary support, that "[a] significant proportion of computer security research does not constitute an infringing act because it simply involves accessing functional, non-copyrighted elements" and that while "there may be some incidental reproduction, distribution, or adaptation," "[m]ost relevant security research focuses . . . on the investigation of those works."[8] These arguments fall well short of FH's burden to show that a use "is or is likely to be noninfringing," rather than a use that "might plausibly be considered noninfringing."[9] In support, FH refers to the Copyright Office's statement in the 2015 Recommendations that the computer programs at issue are "largely functional in nature."[10] But that description was part of the discussion of the second fair use factor and certainly was not intended to question whether vehicle Electronic Control Units (ECUs) are subject to copyright protection, or whether accessing the ECUs for security research implicated exclusive rights. Indeed, the Copyright Office in the 2015 Recommendations clearly stated that that the computer programs at issue were "copyrighted computer programs" and determined that accessing copyrighted computer programs for purposes of security research implicated the exclusive rights of copyright holders.[11] FH has not provided any evidence to alter this conclusion, which is based on well-established principles of U.S. copyright law.[12]

Proponents suggest that the Copyright Office, in assessing the issue of whether the activities enabled by circumvention are noninfringing, should simply apply the fair use factors, and the exception to exclusive rights for computer programs under 17 U.S.C. § 117, in largely the same way it did in the 2015 Recommendations.[13] This ignores the extent to which removal of the limitations from the existing exemption would significantly alter the analysis. For example, the Copyright Office's analysis of the first fair use factor depended on uses limited to solely good faith and security research.[14] Removal of the Good Faith Limitation and Use Limitation would weigh against the first fair use factor because the expanded exemption would then apply to a broader range of uses, including commercial activities, that may not be transformative. For example, it could allow researchers to conduct security research with the intent to also create a

[7] *See* 1201 report at 28 (quoting U.S. Copyright Office, *Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights* (2015) ("2015 Recommendation")).
[8] *See* FH Comment at 11.
[9] *See* 1201 Report at 28.
[10] *See* 2015 Recommendation at 301.
[11] Although the Copyright Office determined that accessing and reproducing computer programs pursuant to the existing exemption were likely to be fair uses or noninfringing uses under the exception in section 117, this determination clearly presumes that accessing these computer programs for good-faith security research implicated the exclusive rights of rights holders. *See* 2015 Recommendation at 299-300.
[12] *See, e.g., Whelan Assocs., Inc. v. Jaslow Dental Lab., Inc.*, 797 F.2d 1222, 1233 (3d Cir. 1986), *cert. denied*, 479 U.S. 1031 (1987) ("It is well . . . established that copyright protection extends to a program's source and object codes.").
[13] *See, e.g.*, FH Comment at 13 (arguing "[t]he uses proposed by this modification petition are the same as those uses proposed in 2015").
[14] *See* 2015 Recommendations at 300 (noting "good-faith security research encompasses several of the favored activities listed in the preamble of section 107").

commercial product, such as a tool for analyzing vehicle software. Likewise, the Copyright Office in 2015 concluded "the desired security research will not usurp the market for any original works subject to that research, as they will be lawfully obtaining copies of those works for analysis."[15] But removal of the Lawfully Acquired Limitation would negate the premise of this analysis, since the copies would no longer have to be lawfully obtained. Furthermore, the Register's 2015 Recommendation did not address the possibility that, as a result of the circumvention, third parties could obtain copies of the works. But a broadened exemption, shorn of the Good Faith Limitation or the Use Limitation, could negatively impact the market, because, for example, the exemption would permit researchers to circumvent for the purpose of disseminating information to third parties with a known incentive and propensity to infringe, which would likely contribute to copyright infringement and damage the market. For another example, a company's proprietary copyrighted software could be accessed (through circumvention) by an academic researcher who receives funding from a competitor, and who could misuse the software to benefit that competitor and harm the market for the original product. Moreover, removal of the Controlled Environment Limitation and the Lawfully Acquired Limitation would raise safety concerns, because such a broadened exemption would permit researchers to interfere with automobiles on public roads, even cars that researchers do not lawfully own. This safety hazard could substantially chill the market for the targeted automobiles and the software they contain. In addition, removal of the Use Limitation or the Good Faith Limitation raises questions regarding whether the copy or adaptation of a computer program enabled by circumvention will be used in "no other manner" than in conjunction with a machine, as required by 17 USC § 117(a)(1) in order for the activity to be non-infringing. Therefore, any expansion of the existing exemption must be carefully examined to determine whether it enables uses likely to be noninfringing. The proposed radically expanded exemption fails this examination.

II. Limitations in the Existing Exemption Have No Adverse Impact on Security Research on Automobiles

Proponents submitted virtually no evidence supporting their assertion that the existing exemption is impeding or "chilling" legitimate security research, at least regarding automobiles. As explained in the 1201 Report, proponents must demonstrate "that as a result of a technological measure controlling access to a copyrighted work, the prohibition is causing, or in the next three years is likely to cause, an adverse impact on [non-infringing] uses."[16] The NPRM indicates that proponents must show "'distinct, verifiable, and measurable impacts'" compared to 'de minimis impacts.'"[17] The 1201 Report further clarifies that "[l]ikely adverse impacts must be more than speculative or theoretical harms," and "mere inconveniences, or individual cases . . . do not rise to the level of a substantial adverse impact."[18]

Only one of proponents – CDT – submitted *any* examples of the purported impact of the existing exemption on security research into automobiles; and CDT's examples fall far short of meeting the benchmarks required in this proceeding. CDT does not demonstrate *any* chilling

[15] *See id.* at 302.
[16] *See* 1201 Report at 27-28 (quoting the 2015 Recommendation).
[17] *See* NPRM at 49551-52.
[18] *See* 1201 Report at 28 (quoting the *Commerce Committee Report* and the *House Manager's Report*).

effect or harm to research attributable to the fact that the existing exemption contains limitations; instead, they show that independent researchers are fully capable under the current legal landscape of collaborating with automobile manufacturers to address security vulnerabilities. CDT's evidence consists of its own publication that identifies several instances of independent researchers identifying flaws in automobile systems.[19] But rather than demonstrating harm, these examples indicate that independent researchers are in fact fully able to conduct research and identify flaws in automobile software, and that the evolving ecosystem for collaboration among independent researchers and automobile manufacturers is functioning well to protect public safety and security. Indeed, the security vulnerabilities in most, if not all of these examples were discovered under the more restrictive legal environment that existed prior to the October 2016 effective date of the existing exemption. These examples provide no support for the proposition that the existing exemption is insufficient or must be broadened.

The example described in CDT's publication of the researchers at UC San Diego finding flaws on Toyota Priuses and the Chevrolet Corvettes is illustrative. The article cited in support, which was published just after the existing exemption was adopted, indicates that while it may have been questionable whether the research was permitted prior to the effective date of the existing exemption, the researchers "won't have to worry about that accusation once the new exemptions security researchers won . . . go into effect."[20] CDT does not provide any evidence in this example or any of the others indicating that any of the limitations of the existing exemption have impeded or hindered in any meaningful way the ability of responsible independent researchers to conduct research into automobile security. To the contrary, the CDT examples are evidence that independent research into the safety and security of computer systems in motor vehicles is thriving.

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. Below are some examples of these fora:

[19] *See* CDT Comment Documentary Evidence, Joseph Lorenzo Hall et al., *The Importance of Security Research: Four Case Studies* 2-4 (Dec. 2017) ("CDT Publication").
[20] *See* David Wagner, *Car Hacking Research Accelerates at UC San Diego*, KPBS PUBLIC MEDIA (October 29, 2015) http://www.kpbs.org/news/2015/oct/29/car-hacking-research-accelerates-uc-san-diego/. The security issue that is the subject of this article involved a third-party wireless dongle that needed to be connected into the on-board diagnostics (OBD II) port; thus, physical access to the vehicle was required to exploit the vulnerability. Manufacturers have warned against use of such devices and have taken measures to increase protections against their use.

- 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.

- Technical experts from auto manufacturers 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."[21]

- In 2016, Fiat Chrysler Automobiles (FCA) launched a "Bug Bounty" program, which crowdsources a community of independent cybersecurity researchers to promote a public channel for responsible disclosure of potential vulnerabilities. Under this program, FCA has offered to pay up to $1,500 to any researcher who discovers a flaw (or bug) in one of its automotive systems.[22]

- Since January 2016, General Motors (GM) has been collaborating with security researchers through a coordinated disclosure platform hosted on HackerOne. HackerOne is an online platform that facilitates responsible disclosure of vulnerabilities discovered by third-party hackers, organizes hacker challenges involving ethical hackers that look for severe vulnerabilities, and organizes a bug bounty program where trusted hackers are incentivized to continuously test for critical vulnerabilities.[23]

- GM engages in a number of other activities to further collaboration with independent researchers. GM sponsors and participates in car hacking "villages" in which GM cyber experts share GM vehicle systems with security researchers in order to collaborate, learn, and teach. GM sponsors and participates in the SAE Battelle CyberAuto Challenge described above. GM also participates in numerous security industry events, such as the B-Sides annual conference on

[21] *See* 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.
[22] *See FCA US Launches Bug Bounty Program to Advance Vehicle Cybersecurity*, FCA http://media.fcanorthamerica.com/newsrelease.do?id=17719&mid=1 (last visited Feb. 8, 2018).
[23] For more information, *see Product Overview*, HACKERONE, https://www.hackerone.com/product/overview (last visited Feb. 8, 2018).

information security, the RSA Conference on cybersecurity, and the GrrCon Hacker Conference.

- Ford and other automobile manufacturers regularly collaborate with government agencies and academic institutions on security research issues as part of groups, such as the Crash Avoidance Metrics Partnership (CAMP), Transport Research Institute of the University of Michigan (UMTRI), and the Mcity research group of the University of Michigan.

- The leading federal regulatory agency, the National Highway Traffic Safety Administration (NHTSA), regularly supports a number of security research activities, including in partnership with automobile manufacturers and suppliers.[24]

In a significant step forward toward greater collaboration with diverse sources in addressing these issues, in August 2015 the Auto Alliance and Global Automakers began collaborating, with the encouragement of NHTSA, as part of 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.[25] The Auto-ISAC operates a central hub for sharing, tracking and analyzing intelligence about cyber threats, vulnerabilities and incidents related to motor vehicles. Currently, Auto-ISAC members account for more than 99 percent of light-duty vehicles in North America, with over 30 global Original Equipment Manufacturer (OEM) and supplier members. Building upon the success of this collaboration, Auto-ISAC expanded membership to heavy trucking OEMs and their suppliers, as well as the commercial vehicle sector—including fleets and carriers.

The Auto-ISAC has become a significant 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. Attached as Exhibit A is a letter from the Executive Director of the Auto-ISAC to the Assistant General Counsel of the Auto Alliance (Auto-ISAC Letter) that provides background on the Auto-ISAC and describes how Auto-ISAC collaborates with researchers from academia, government, and other research and non-profit organizations to further its goal of enhancing the security of automotive systems. The Auto-ISAC Letter outlines specific examples of collaboration among OEMs and independent security researchers to address security vulnerabilities prior to their public disclosure.[26] Furthermore, as discussed in the Auto-ISAC Letter, Auto-ISAC collaboration with independent security researchers has been enhanced through partnership with the HackerOne platform, which, as discussed above, provides a framework for responsible disclosure of security vulnerabilities.[27]

It is notable that in many of the examples cited by CDT, the automobile manufacturer took prompt action to address the problem, including cooperating with the independent

[24] *See NHTSA and Vehicle Cybersecurity* at 8, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/nhtsavehiclecybersecurity2016.pdf (last visited Feb. 8, 2018).
[25] For additional information, *see Start Your Engines*, AUTO-ISAC, https://www.automotiveisac.com/.
[26] *See* Exhibit A attached hereto, Auto-ISAC Letter at 2.
[27] *See id*.

researcher who discovered the vulnerability. In the example involving the Nissan Leaf, CDT acknowledges that the company "immediately" took action to address the vulnerability.[28] In another example, FCA took a number of measures, including recalling 1.4 million vehicles, as a result of the research by Mr. Miller and Mr. Valasek into issues with the UConnect system.[29] Regarding the UConnect issue, CDT suggests that "similar flaws were found by academic security researchers" that "were not acted upon," but in support, CDT simply cites three publicly available research papers.[30] As an initial matter, without a detailed technical analysis, there is no way of knowing if these papers actually do disclose "similar flaws" to the issues uncovered by Miller and Valasek. Secondly, while these papers are publicly available, there is no evidence that they were ever brought to the attention of FCA, or any other automobile manufacturer. Crucially, even if CDT is correct that these three research papers do in fact disclose "similar flaws," CDT does not provide any evidence that any of the limitations in the existing exemption impeded the research disclosed in these papers or the publication of the research results. Moreover, exemplifying the increased collaboration between the automotive industry and the security research community, Mr. Miller and Mr. Valasek are presently working for Cruise LLC, a wholly owned subsidiary of GM, assisting GM in improving vehicle security.

The example involving the Mitsubishi Outlander provides a very good illustration of the way in which automobile manufacturers are seeking to cooperate with independent researchers to address security issues. Although CDT suggests that Mitsubishi did not take action in response to a concern raised by independent security researcher Ken Munro, the article CDT cites actually states that Mitsubishi was "keen to get Mr. Munro talking to its engineers in Japan to understand what he found and how it could be remedied" and that Mitsubishi took immediate steps to remedy the problem while it investigated.[31]

To the extent that steps taken to address some of the issues highlighted in the CDT examples were unsuccessful or delayed, it is because (as previously noted) many of the examples date from years ago, when the issue of automotive security was very new and many of the mechanisms for addressing the problem described above had not yet been developed. For example, the issue with the GM OnStar system was first discovered in 2010, using innovative methods described as a "brilliant hack . . . ahead of its time." [32] The hack occurred when the issue of security research into automobiles was embryonic, and the mechanisms to address the problem had not yet been developed or been implemented. While GM made efforts to fix the vulnerability as soon as it learned of the issue, those efforts did not at first fully resolve the problem, although it was ultimately resolved.[33] One of the researchers who identified the vulnerability, UCSD professor Stefan Savage, even acknowledged that in 2010 the issue "was so damn new to everybody," and it was difficult for everybody, including manufacturers, to

[28] *See* CDT Publication at 4.
[29] *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me In It*, WIRED, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Jul. 21, 2015).
[30] *See* CDT Publication at 3.
[31] *See* Dave Lee, *Mitsubishi Car Alarm System "Hacked"*, BBC NEWS (Jun. 6, 2016) http://www.bbc.com/news/technology-36444586.
[32] *See* Andy Greenberg, *GM Took 5 Years to Fix a Full-Takeover Hack in Millions of OnStar Cars*, WIRED (Sept. 10, 2015) https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/.
[33] *See id.*

understand the problem.[34] He further maintained that to have publicly disclosed the research at the moment it occurred – precisely the conduct that removal of the limitations in the existing exemption would encourage – would have done more harm than good, because it could have enabled malicious hackers to exploit the flaw.[35] Although Mr. Savage indicates his calculus may be different today, he at least recognizes the serious risks of irresponsible public disclosure of a security vulnerability.[36] Similarly, the example CDT cites involving the key fob systems for Audi, BMW, Toyota, and Ford cars was, based on their description, first identified at least three years prior to the release of the 2017 CDT publication, and, because that issue apparently impacted multiple manufacturers, was likely more complicated to address.[37] Automobile manufacturers have been working, including through the collaborative mechanisms discussed above, to improve the security of key fob systems. As described above, in recent years, many mechanisms, including the Auto-ISAC, have developed to increase cooperation across the industry and with government and independent researchers to address these issues.

Whatever the CDT examples may indicate regarding industry cooperation with independent researchers, as noted above, these examples clearly show that independent security research into motor vehicles has not been chilled but instead is flourishing. Yet FH and CDT still argue that each limitation of the existing exemption is harmful to researchers' noninfringing uses. The only other "evidence" they have provided in support, besides the CDT examples discussed above, is a personal statement by FH that is essentially nothing more than a restatement of the arguments in their comment.[38] It does not include any concrete examples or actual evidence relating to automobiles. Auto Alliance and Global Automakers respond below to their assertions regarding each limitation at issue.[39]

A. Lawfully Acquired Limitation

Proponents have provided no evidence that requiring researchers to undertake circumvention on a lawfully acquired automobile is in any way impeding security research on motor vehicles.[40] FH and CDT object to the Lawfully Acquired Limitation because they assert

[34] *See id.*
[35] *See id.* ("Even if key elements had been hidden, any publicity could have still enabled malicious hackers to rebuild the attack at a time when GM was unprepared to protect drivers from it.").
[36] *See id.* (noting that when Mr. Savage and other researchers discovered a "car hacking technique" in 2015, they publicly named the relevant companies, but apparently did not disclose details of the vulnerability).
[37] *See* CDT Publication at 3. Note the only evidence for this purported incident is the description in the CDT publication because the article cited in support does not relate to this issue. *See* Larry Greenmeier, *Recall Shows That a Hack Attack on Car Controls is a Credible Threat*, SCIENTIFIC AMERICAN (Jul. 28, 2015) https://www.scientificamerican.com/article/recall-shows-that-a-hack-attack-on-car-controls-is-a-credible-threat/ (discussing the FCA UConnect issue, not the key fob system issue).
[38] *See* FH Comment at 36-40.
[39] Expansion of the existing exemption to include additional devices does not impact the automobile industry because motor vehicles are already covered; therefore, the Auto Alliance and Global Automakers do not take a position on whether to expand the exemption to other devices. But should the Copyright Office expand the existing exemption by removing one or more of the other limitations, such an expansion should not apply to motor vehicles, for the reasons stated in this submission.
[40] The NPRM clearly states, "Proponents of exemptions should present their complete affirmative case for an exemption during the initial round of public comment, including all legal and evidentiary support for the proposal . . . Reply comments should not raise new issues . . ." *See* NPRM at 49558. Proponents have had ample opportunities to bring forward any evidence that may exist to support their assertions, including the opportunity to

that complicated disputes over acquisition of physical property should not be part of this proceeding. But they have not provided evidence that disputes over the acquisition of automobiles have had any impact on security research. What purported harm they do describe is purely theoretical and speculative, and does not come close to meeting their statutory burden.[41] It is usually very clear when a person has lawfully acquired a motor vehicle, since it typically requires registration with government authorities. It is difficult to understand how this limitation impedes research on automobile security at all, or how making it easier for researchers to experiment on automobiles that they do not own or control would advance the goals of the existing exemption while preserving public safety. The proposed removal of both this limitation and the Controlled Environment Limitation raises the prospect of bad actors taking control of other people's vehicles "in the wild." While this could violate other applicable laws, that is no reason for the Copyright Office to recommend modifying this exemption in a way that will make the job of such bad actors easier.[42]

B. Good Faith Limitation

Proponents have not provided any evidence that good-faith security research on automobiles has been chilled because circumvention is permitted "solely" for this purpose.[43] FH and CDT recycle the argument that this limitation creates ambiguity regarding the activities in which a researcher may lawfully engage. Yet, to the extent there is any ambiguity, it is not clear how removing the Good Faith Limitation would reduce the ambiguity, since the specific range of activities permitted, while broader, would still be just as uncertain. FH asserts (without providing any concrete examples) that the Good Faith Limitation prevents researchers from engaging in "broader aims," including "scientific dialogue, academic peer review, and classroom teaching."[44] While FH do not explain why such activities are necessarily antithetical to the goal of "good faith security research," defined in the existing exemption to include "good faith testing, investigation and/or correction of a security flaw or vulnerability," immunizing research carried out for purposes that require disseminating sensitive security information to third parties would create unnecessary risks that bad actors will gain access to security vulnerabilities. As discussed in more detail below in the section on the Use Limitation, encouraging researchers to follow responsible disclosure practices is a positive feature, not a malign bug, of the existing exemption.

Moreover, elimination of the Good Faith Limitation would open the door, not only to these seemingly benign "broader aims," but also to a host of other purposes, including

---

petition for renewal of the existing exemption in July 2017 and the opportunity to petition for expansion of the existing exemption in December 2017. To the considerable extent that some proponents rely upon the record in the study that produced the Copyright Office's 1201 Report, that proceeding also provided multiple opportunities to produce any such evidence. If proponents use the reply round in this proceeding to bring forward any such evidence, Auto Alliance and Global Automakers urge the Office to disallow it. Acceptance of new evidence on this point in the reply round would raise serious questions regarding the fairness of this proceeding because opponents would not have an opportunity to adequately respond.

[41] *See* 1201 Report at 28 ("[l]ikely adverse impacts must be more than speculative or theoretical harms").

[42] As noted above, if the Office decides to recommend relaxation or removal of this limitation with regard to other devices, automobiles should be specifically excluded from such changes, since there is no evidence in the record to support such a modification with regard to automobiles.

[43] As noted in n. 40, *supra*, proponents have had ample opportunity build the factual record on this point. It is now too late in the proceeding to permit them to cure their failure to do so.

[44] *See* FH Comment at 24.

commercial motivations, all of which would need to be analyzed under the fair use four factor test or pursuant to any other applicable exception to exclusive rights. Furthermore, removing the term "solely" from the existing exemption as proponents suggest would allow researchers to justify doing almost anything with the research information, regardless of its relationship to good-faith security research. These are among the reasons why Congress included this same limitation in the section 1201(j) permanent exception. While FH deprecate the Office's effort to conform the existing exemption to the contours of the statutory exemption in section 1201(j) (including through the limitation to circumvention carried out "solely for the purposes of good faith security research"), FH provide no persuasive reason to reject this approach in favor of a wide open immunization of circumvention carried out for any purpose so long as security research is somewhere in the mix.[45]

FH's suggestion that the Copyright Office must expand the exemption to "avoid unconstitutionally limiting post-circumvention First-Amendment-protected speech"[46] is unfounded and misplaced. In crafting the existing exemption, the Copyright Office did take into account relevant First Amendment concerns.[47] Furthermore, FH's attempt to leverage into this proceeding a complaint filed by the Electronic Frontier Foundation (EFF) challenging the constitutionality of this process should be rejected. Citing the complaint, FH suggest that the Copyright Office would be acting unconstitutionally if it fails to grant their proposed modifications.[48] To the extent the constitutional issues raised in the EFF complaint have any merit, those issues will be decided by the courts. The Copyright Office should not take the allegations asserted in the EFF complaint into account in making its recommendation regarding whether to amend the existing exemption.[49]

C. Illegality Limitation

Proponents have provided no evidence that prohibiting researchers from violating applicable law when circumventing access controls in any way inhibits or impedes security research on motor vehicle software. [50] FH and CDT argue that the Illegality Limitation chills research because it creates legal uncertainty and risk regarding other laws, such as the Computer Fraud and Abuse Act (CFAA).[51] But, to the extent that there is legal uncertainty, that legal uncertainty lies with those other laws themselves, not with the Illegality Limitation. Accordingly, the uncertainty would still exist even if the Illegality Limitation were eliminated because researchers must still comply with the law. Moreover, enforcement actions under the CFAA are much more common than are enforcement actions pursuant to the DMCA. And the former is a criminal statute, while the latter's criminal prohibitions are largely limited to commercial

[45] The Copyright Office modeled the existing exemption on section 1201(j) "in the interest of adhering to Congress's basic purpose" of facilitating good-faith security research. *See* 2015 Recommendation at 319.
[46] *See* FH Comment at 24.
[47] *See* 2015 Recommendation at 319.
[48] *See* FH Comment at 34.
[49] As noted above, if the Office decides to recommend relaxation or removal of this limitation with regard to other devices, automobiles should be specifically excluded from such changes, since there is no evidence in the record to support such a modification with regard to automobiles.
[50] As noted in n. 40, *supra*, proponents have had ample opportunity build the factual record on this point. It is now too late in the proceeding to permit them to cure their failure to do so.
[51] *See* FH Comment at 23-24; *see also* CDT Comment at 4.

activity.[52] Thus, to the extent there is any chilling effect on legitimate security research involving automobiles, researchers are far more likely to be inhibited in their research due to fear of civil action or potential prosecution under the CFAA than they would be due to the threat of enforcement under the DMCA. Proponents suggest this limitation could result in "potentially exporting" DMCA penalties into other legal regimes;[53] but, as proponents indicate, this outcome, and certainly any possible resulting harm, is purely theoretical and speculative, falling far short of proponents' statutory burden.[54] Proponents have not provided any evidence that the Illegality Limitation has had any incremental impact on security research beyond the impacts attributable to other laws such as the CFAA. Since this proceeding is solely concerned with adverse impacts arising "by virtue of [the] prohibition" contained in 17 USC § 1201(a)(1)(A), any impacts attributable to other laws are completely irrelevant.[55] Finally, it is significant that Congress included this limitation as part of the permanent exception for security research in section 1201(j), indicating that Congress understood the importance of ensuring circumvention for research purposes did not violate other laws. Therefore, proponents have not met their burden to demonstrate harm due to this limitation.[56]

D. Controlled Environment Limitation

The Copyright Office concluded in 2015 that, "In the context of a general security research exemption, there appeared to be universal agreement among proponents that testing in 'live' conditions – such as cars being driven on public roads – is wholly inappropriate."[57] One of the proponents, Consumers Union, supports maintaining this limitation, saying that it may be necessary for "ensuring safety and security."[58] Other proponents, however, now dissent from the "universal agreement" noted three years ago, and call for elimination of the common-sense requirement that good-faith security research on motor vehicles must take place in a controlled environment. Just as with the other limitations, proponents do not provide a single concrete example of this limitation having hampered legitimate security research on automobiles.[59] To the contrary, in each example cited by CDT, it appears the researcher was able to identify the flaw as part of security research done in a controlled environment.[60] FH's criticism of this limitation is

[52] *See* 17 U.S.C. § 1204 (requiring proof of "commercial advantage or private financial gain" for criminal liability for circumvention).
[53] *See* FH Comments at 23.
[54] *See* 1201 Report at 28 ("[l]ikely adverse impacts must be more than speculative or theoretical harms").
[55] *See* 17 U.S.C. § 1201(a)(1)(B); *see also* NPRM at 49551 (identifying one element of this proceeding's inquiry as whether "the statutory prohibition on circumventing access controls is the cause of the adverse effects") (emphasis added).
[56] As noted above, if the Office decides to recommend relaxation or removal of this limitation with regard to other devices, automobiles should be specifically excluded from such changes, since there is no evidence in the record to support such a modification with regard to automobiles.
[57] *See* 2015 Recommendation at 318.
[58] *See* Consumers Union, Class 10 Long Comment at 3 (Dec. 18, 2017).
[59] As noted in n. 40, *supra*, proponents have had ample opportunity build the factual record on this point. It is now too late in the proceeding to permit them to cure their failure to do so.
[60] The Wired article describing the issue with the Chrysler, Dodge, and Jeep vehicles does include a harrowing description of a demonstration in which the researchers apparently hacked the reporter's vehicle while the reporter was driving on a public highway, underscoring the need for this important limitation. *See* Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me In It*, WIRED, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Jul. 21, 2015). There is no indication, however, that such a dangerous stunt was required in order to identify or describe the security issue in the first place.

that its "contours" are ambiguous and that it is necessary for researchers to test their research outside of a controlled environment.[61] CDT similarly argues that the limitation should be removed "to reduce ambiguity for researchers."[62] Neither of these critiques persuasively applies to automobiles. The Controlled Environment Limitation very sensibly precludes real-time research on cars that are on public roads, where innocent third parties may be exposed to serious risks of damage, injury or death. Proponents profess to be confused about what constitutes the "controlled environment" within which research qualifying for the existing exemption must be confined. To the extent there may be ambiguity regarding other controls on this type of research that may be needed to avoid harm to individuals or the public, those limits can be determined through legal challenges if necessary, just as the metes and bounds of any administrative regulation may be determined. Removing or altering this limitation to permit research to be conducted on public roadways would come at a very high societal cost, and would endanger motorists, pedestrians, and the general public.

Without any evidence that the Controlled Environment Limitation impedes security research on automobiles, the Copyright Office must give substantially greater consideration to the obvious dangers of security researchers interfering with cars on public roads, endangering both the occupant of the car as well as other drivers and pedestrians. Proponents have not met their burden of demonstrating adverse impacts on security research on automobiles due to the Controlled Environment Limitation.[63]

E. Use Limitation

Proponents have not provided even a single example where security research involving automobiles has been inhibited, abandoned, impeded or curtailed because of the obligation under the existing exemption to refrain from carrying out research in a way that is primarily used to promote some goal other than safety or security, or that facilitates copyright infringement or otherwise harms the public.[64] FH and CDT appear to want an unlimited ability 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. FH argue the Use Limitation is ambiguous and, thus, researchers are not sure whether they are able to publish their results.[65] CDT argues that this limitation violates the First Amendment rights of researchers.[66] While it may be true that the Use Limitation is more ambiguous than definitive requirements for disclosing research results, in 2015, the Copyright Office declined to issue definitive disclosure requirements because the Office did not want to "implicate First Amendment concerns."[67] Instead, it opted for a standard that provides more leeway, but effectively rules out clearly impermissible bad-faith activities, including irresponsible disclosure of copyrighted information.

[61] *See* FH Comment at 21-23
[62] *See* CDT Comment at 4.
[63] As noted above, if the Office decides to recommend relaxation or removal of this limitation with regard to other devices, automobiles should be specifically excluded from such changes, since there is no evidence in the record to support such a modification with regard to automobiles.
[64] As noted in n. 40, *supra*, proponents have had ample opportunity build the factual record on this point. It is now too late in the proceeding to permit them to cure their failure to do so.
[65] *See* FH Comment at 25.
[66] *See* CDT Comment at 5.
[67] *See* 2015 Recommendation at 319.

To the extent that the Use Limitation requires clarification, as with any administrative rule, courts are available to make those determinations on the specific facts of an appropriate case.

Moreover, just because a rule provides flexibility is not a reason to get rid of it altogether, especially a rule that serves an important purpose. Removal of the Use Limitation 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 informing bad actors as well as the general public. Proponents are attempting to have it both ways, arguing that the existing exemption is both vague and that it violates the First Amendment because it is too restrictive. Their agenda is to be able to use the data however they see fit, while ignoring the risk of copyright infringement as well as risks to public safety and security. The Copyright Office struck the right balance in 2015 by granting some flexibility to beneficiaries of the existing exemption, but ensuring that researchers use research information to promote the security or safety of devices or users, and not to facilitate copyright infringement.

Under the existing legal framework, automobile manufacturers have increased collaboration with independent security researchers using responsible disclosure processes. For example, as noted above, GM engages with independent security researchers on the HackerOne platform, but that engagement is conducted pursuant to certain disclosure guidelines. These guidelines include that researchers cannot cause harm to GM customers or others, researchers cannot violate any laws, and researchers can "publicly disclose vulnerability details only after GM confirms completed remediation of the vulnerability and not publicly disclose vulnerability details if there is no completion date or completion cannot be ascertained."[68] Similarly, one of the purposes of the Auto-ISAC, as discussed above, is to provide manufacturers with the opportunity to address threats discovered by third party researchers before they are publicly revealed. Allowing the manufacturer the opportunity to remedy a vulnerability before publicly disclosing it is a common-sense requirement that is necessary to prevent this information from falling into the hands of bad actors, which would risk harm to public safety.

FH also incorrectly claims that the Use Exception may prevent a researcher from "using the information about a vulnerability to dissuade consumers from using a vulnerable device that cannot be made safe or secure because the vulnerability cannot be fixed, or because the device's vendor refuses to fix the vulnerability."[69] Once again, FH provide no concrete example, and the Office should be reluctant to follow them down a trail of speculation and hypothetical supposition, since in this proceeding, "[l]ikely adverse impacts must be more than speculative or theoretical harms."[70] If the Office did follow this trail, however, it would conclude that this circumstance would likely be permitted under the existing exemption, as long as the researcher takes care not to facilitate copyright infringement; because, as FH acknowledges, cautioning consumers about a vulnerable device that will never be made safe or secure would promote the safety or security of those who would otherwise use the device. Of course this premise involves a

[68] *See GM Policy*, HACKERONE, https://www.hackerone.com/gm (last updated May 6, 2016).
[69] *See* FH Comment at 25.
[70] *See* 1201 Report at 28.

number of determinations – including that the vulnerability exists, that it actually undermines the safety or security of the device, and that the device cannot be fixed or the device's seller refuses to fix it. In the evolving ecosystem of collaboration to identify and remedy security flaws or vulnerabilities affecting automobiles, as described above, it seems far-fetched at best to assume that the last of these determinations is valid; but in the hypothetical circumstance in which it were, it seems equally far-fetched to assert that warning consumers away would not qualify as seeking to promote driver or passenger security or safety.

Finally, contrary to FH and CDT arguments, it simply is not true that the Use Limitation conditions eligibility for the exemption on the behavior of third parties. The Use Limitation clearly applies to the beneficiary of the exemption (i.e. the researcher who circumvents access controls on the copyrighted work), and does not depend on independent actions of third parties. As long as the beneficiary of the exemption uses the research information derived from circumvention in accordance with the Use Limitation (i.e., to promote safety and security), then liability will not attach. If subsequent infringement occurs, that is in no way dispositive of whether the Use Limitation has been violated; the operative inquiry will be whether *the way that the researcher used or maintained the research results* facilitated the infringement in question.[71]

III. Removal of Limitations of the Existing Exemption Will Result in Substantial Harm to Safety and Security

In the 1201 Report, the Office declined to categorically exclude "non-copyright" concerns, but said it will "generally decline" to consider health, safety, and environmental concerns.[72] Auto Alliance and Global Automakers urge the Copyright Office not to exclude or to deprecate consideration of the risks to public safety and security that could flow from allowing unrestricted circumvention of access controls on vehicle firmware in order to carry out security research that exceeds the boundaries of the existing exemption. 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.

As the Copyright Office recognized in setting the ground rules for a previous rulemaking cycle of this proceeding in the 2011 Notice of Inquiry, "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."[73] The Auto Alliance and Global Automakers urge 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" of the existing exemption's limitations to the performance of legitimate security

[71] As noted above, if the Office decides to recommend relaxation or removal of this limitation with regard to other devices, automobiles should be specifically excluded from such changes, since there is no evidence in the record to support such a modification with regard to automobiles.
[72] *See* 1201 Report at 125-26.
[73] *See Exemption to the Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies; Notice of Inquiry and Request for Petitions*, 76 Fed. Reg. 60398, 60403 (Sept. 29, 2011).

research on automobiles is minimal, or even, on the current record, non-existent. But even if it were considerably greater, it would be outweighed by the harms that would result from granting the expanded 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. In the last rulemaking cycle, the Copyright Office wisely adopted many of these same limitations as part of the existing exception.

Clearly the proponents find the existing environment too constricting, and seek to persuade the Copyright Office that in order to carry out their activities, the existing exemption must be radically expanded to allow them to venture farther afield. Their goal appears to be unrestricted disclosure of security vulnerabilities on their own terms and timetable, regardless of the risks. As noted above, the limitations of the existing exemption, particularly the Controlled Environment Limitation and the Use Limitation, are critically important to protect public safety and security. In support of their comments, CDT provides examples of independent researchers who brought to light various flaws in automobile security under the even more restrictive legal landscape that existed prior to the enactment of the existing exemption. 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.

FH's charge that "developers and copyright holders attempt to leverage Section 1201 against researchers to *conceal* security vulnerabilities rather than fixing them"[74] is baseless, at least regarding the automobile industry. The reality, as summarized above, is that vehicle systems are being robustly tested (both by auto manufacturers themselves and by independent researchers) and vulnerabilities, once identified, are addressed. Cooperation between manufacturers and independent researchers has increased dramatically since the last rulemaking cycle. The record is devoid of any shred of evidence to the contrary, including any evidence that any researcher has been sued or threatened with suit under Section 1201(a) for carrying out activities within the scope of the current exemption.

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 above, or whether there is a need to radically broaden the existing exemption, with the foreseeable consequence of increasing the risk that such destructive exploitation of the vulnerabilities will occur. Auto Alliance and Global Automakers urge the Copyright Office to

[74] *See* FH Comment at 34-35 (emphasis in original).

take these risks fully into account in striking the balance of harms identified in the 2011 Notice of Inquiry.

IV. Conclusion

For the foregoing reasons, Auto Alliance and Global Automakers believe that proponents have failed to meet their burden of persuasion that the Copyright Office should remove important restrictions of the existing exemption that help ensure that security research on motor vehicle systems is responsible and does not endanger safety and security or facilitate copyright infringement. The role of independent security research into vehicle systems is best advanced through collaborative efforts under the current legal landscape, rather than exposing new vulnerabilities through an expanded exemption.

DOCUMENTARY EVIDENCE

Exhibit A:

Auto-ISAC Letter (February 9, 2018)

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Jessica L. Simmons
Assistant General Counsel
Alliance of Automobile Manufacturers
Washington, D.C.

February 9, 2018

Ms. Simmons,

In response to your request, please find below information regarding the Auto-ISAC and, in particular, collaboration activities involving Auto-ISAC and third party researchers.

The Auto-ISAC facilitates sharing of timely and actionable information pertaining to security threats impacting the automotive industry. Currently, Auto-ISAC members account for more than 99 percent of light-duty vehicles in North America, with over 30 global Original Equipment Manufacturer (OEM) and supplier members. Building upon the success of this collaboration, Auto-ISAC expanded membership to heavy trucking OEMs and their suppliers, as well as the commercial vehicle sector—including fleets and carriers. Auto-ISAC enhances the ability of the automobile industry to prepare for and respond to threats, deal with vulnerabilities and incidents and raise awareness across the community in order to reduce business risks.

The Auto-ISAC is member-driven and governed by a Board of Directors composed of leaders across the global automotive industry. Auto-ISAC's goals include:

- providing a forum for trusted and timely information regarding security threats;
- fostering cooperation and communication among members to their mutual benefit;
- researching and analyzing information received to validate accuracy and severity and to recommend actions;
- disseminating insights into threat and mitigation strategies using secure and effective methods;
- enabling development of professional and trusted relationships among peers and subject matter experts to protect the whole of the automotive industry; and
- providing best practices and educational awareness through exercise and key sharing events.

To further these goals, Auto-ISAC has developed relationships, both formal and informal, with numerous researchers from academia, government, and other research and non-profit organizations. These "collaborators" support the mission of the Auto-ISAC through sharing of their time, resources, information, education, promotional efforts, referrals, and introductions.

One such organization is HackerOne. Auto-ISAC has been working with HackerOne to facilitate coordination between the HackerOne hacker community and Auto-ISAC members, and to collaborate on implementation of vulnerability disclosure processes.

The following are examples of successful Auto-ISAC collaborations with independent security researchers:

- Through relationships with the security industry, Auto-ISAC learned that the Russian cybersecurity firm Kaspersky Lab was scheduled to give a presentation at the RSA Conference in February 2017 highlighting research indicating that some automakers' Android-based mobile apps may be hacked by exploiting vulnerabilities in the Android mobile operating system. Immediately after learning about the presentation, Auto-ISAC contacted Kaspersky Lab and facilitated confidential information sharing before the vulnerability could be publicly disclosed. In particular, Auto-ISAC alerted the members whose apps had been tested by Kaspersky, facilitated information sharing and organized meetings between member analysts and the Kaspersky researchers, and coordinated with federal regulators regarding the research. As a result, Auto-ISAC members investigated the issue and, when necessary, remediated any existing vulnerabilities related to the Kaspersky research before the issue was publicly disclosed.
- Based on information received from an OEM member in June 2017, Auto-ISAC reached out to researchers at McAfee who were investigating vulnerabilities in a component found in certain automobiles. This vulnerability also impacted other industries that use the same component. Auto-ISAC coordinated with McAfee and with the Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to gain the necessary information to address the vulnerability. Auto-ISAC members investigated and remediated any existing vulnerability related to McAfee's research before the issue was disclosed publicly.
- In September 2017, Auto-ISAC learned through public sources that Armis Security had identified vulnerabilities in the BlueTooth standard that impacted components deployed in automobiles. Auto-ISAC reached out to Armis Security and facilitated communication to exchange information on the vulnerabilities. As a result, Auto-ISAC members were able to take prompt action to understand how automobiles might be impacted by these wide-ranging vulnerabilities.
- In September 2017, an Auto-ISAC member alerted the Auto-ISAC about research into a vulnerability in an airbag electronic control unit (ECU) conducted by researcher Juergen Duerrwang at Karlsruhe Technical University in Germany. The information had been reported to the German government and industry organizations, but was not widely available to U.S.-based automotive teams. Auto-ISAC analysts communicated with Mr. Duerrwang about the issue. Mr. Juergen had prepared to share his research more broadly through a conference presentation, but decided not to do so because of the sensitivity of the issue and the fact that all key stakeholders were aware of the vulnerability through the Auto-ISAC. When the vulnerability ultimately did become public through publication of a paper in December 2017, Auto-ISAC members were already taking action to address the issue.

Please let us know if you have additional questions.

Sincerely,

Faye Francy

Faye Francy
Executive Director
Automotive ISAC

AUTO-ISAC
20 M STREET, SE, SUITE 9025
WASHINGTON, D.C. 20003