This is a Word document that allows users to type into the spaces below. The comment may be single-spaced, but should be in at least 12-point type. The italicized instructions on this template may be deleted.

UNITED STATES COPYRIGHT OFFICE

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

Please submit a separate comment for each proposed class.

NOTE: This form must be used in all three rounds of comments by all commenters not submitting short-form comments directly through regulations.gov, whether the commenter is supporting, opposing, or merely providing pertinent information about a proposed exemption.

When commenting on a proposed expansion to an existing exemption, you should focus your comments only on those issues relevant to the proposed expansion.

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

Commenters can provide relevant multimedia evidence to support their arguments. Please note that such evidence must be separately submitted in conformity with the Office's instructions for submitting multimedia evidence, available on the Copyright Office website at https://www.copyright.gov/1201/2018.

ITEM A. COMMENTER INFORMATION

Harman International ("Harman") submits this comment in opposition to the adoption of the proposed exemption for Class 7. Harman is a global leader in connected car technology, lifestyle audio innovations, design and analytics, and cloud services. Harman designs and engineers connected products and solutions for automakers, consumers, and enterprises worldwide, including connected car systems, audio and visual products, enterprise automation solutions, and services supporting the Internet of Things. In March 2017, Harman became a wholly-owned subsidiary of Samsung Electronics Co., Ltd. The views expressed herein are Harman's own.

Harman is represented in this proceeding by Mayer Brown LLP. Contact information for Harman is as below:

Tom Mooney
Director, Public Affairs
Hung Chang
Director, IP & Open Source Counsel
Harman International
400 Atlantic Street
Stamford, CT 06901
Thomas.mooney@harman.com

Linda L. Rhodes
A. John P. Mancini
Xiyin Tang
Mayer Brown LLP
1999 K Street NW
Washington, DC 20006
lrhodes@mayerbrown.com
jmancini@mayerbrown.com

Hung.chang@harman.com

This comment is joined by Panasonic Corporation of North America ("Panasonic").

Panasonic is a leading technology partner and integrator to businesses, government agencies and consumers across the region. The company is the principal North American subsidiary of Osaka, Japan-based Panasonic Corporation. Panasonic Automotive Systems Company of America is a division company of Panasonic Corporation of North America and is the top supplier of automotive infotainment systems globally, according to IHS. Panasonic Automotive Systems Company of America is headquartered in Peachtree City, Georgia, with sales, marketing and engineering operations in Farmington Hills, Michigan. Contact information for Panasonic is as below:

Paul Schomburg
Director, Government & Public Affairs
Panasonic Corporation of North America
1130 Connecticut Ave, NW – STE 1100
Washington, D.C. 20036
Email: paul.schomburg@us.panasonic.com

Laurence (Larry) S. Roach
General Counsel
Panasonic Automotive Systems Company of America, Division of Panasonic Corporation of North America
776 Highway 74 South
Peachtree City, GA 30269
E-mail: Larry.Roach@us.panasonic.com

ITEM B. PROPOSED CLASS ADDRESSED

Proposed Class 7: Computer Programs – Repair

ITEM C. OVERVIEW

Harman respectfully requests that the United States Copyright Office ("Office") refrain from creating any exemption that permits circumvention of computer programs primarily designed for the control of telematics or entertainment systems. Accordingly, Harman respectfully submits that the Auto Care Association and Consumer Technology Association (collectively, "CTA")'s petition (the "Petition[1]") to remove the limitation in the current exemption for "telematics or entertainment systems" is overbroad and myopic. Telematics and entertainment systems, such as those developed and implemented by Harman and its automotive industry peers, are not merely aftermarket devices attached or installed on a vehicle to satisfy the needs or whims of an individual consumer, but are rather complex systems that are highly sophisticated, painstakingly designed and engineered, and thoughtfully integrated into land vehicles at the request of original equipment manufacturers. They often enable, support, and/or access critical vehicle safety functionality, in addition to managing, processing, and protecting sensitive proprietary software, licensed content, and consumer data. Circumventing certain

[1] Petition for New Exemption Under 17 U.S.C. § 1201 (Sept. 13, 2017), https://www.copyright.gov/1201/2018/petitions-091317/class7/class-07-newpetition-aca-cta.pdf.

controls on these systems have broader, potentially grim implications for consumers and manufacturers that reach far beyond servicing and research needs.

For example, permitting an exemption for telematics or entertainment systems would enable rampant piracy of copyrighted works like music and films—the very core of protected copyrighted works that Section 1201 intended to protect. Further, the many unknowns attendant in circumvention could result in significant risk or danger to consumer safety, elevating the potential for vehicular accidents. In addition, the proposed exemptions are so broad that they also impermissibly enable the broad theft of valuable intellectual property, including valuable source code. Finally, circumvention is fundamentally at odds with federal regulations, such as F.C.C rules, mandating the lockdown of various parameters controlling radio frequency devices contained in electronic-electrical products that are capable of emitting radio frequency energy, as discussed further below.

1. The Register Rightfully Concluded in the Last Triennial Rulemaking That Nothing in the Record Supports Extending an Exemption for Diagnosis or Repair to Telematic/Entertainment Systems, And No New Evidence Supports Such an Exemption Now

As the Office rightfully noted in its Notice of Proposed Rulemaking[2], during the 2015 triennial rulemaking, the Register had concluded that the record did not support extending the exemption for the diagnosis, repair, or lawful modification of motorized land vehicles to electronic control units ("ECUs") primarily designed for the control of telematics or entertainment systems. In the CTA's Petition, they do not present any new evidence for why the exemption should be extended to telematics or entertainment systems, other than a conclusory statement that "telematics systems increasingly are being designed by vehicle manufacturers as the means to access the embedded software that controls the parts and operation of the vehicle." But they do not cite to any examples of how, if at all, the same considerations that lead the Register to conclude that the record did not support an exemption for telematics or entertainment systems have changed in the past three years.

Finally, the CTA's own Petition makes the point that telematics systems control access to embedded software that controls the *operation of the vehicle*—software that, if improperly tampered with, could result in severe safety hazards, as discussed in detail immediately below.

2. Permitting an Exemption for Telematics Systems Poses Grave Consumer Privacy and Safety Concerns

Indeed, telematics systems are often gateways into vehicle ECUs that control critical safety functions of the vehicle, such as throttle, braking, and steering. A potential cybersecurity breach could expose an individual make/model vehicle *or an entire fleet of vehicles* utilizing certain Harman products and services to cyberhackers, who could in turn create life-threatening risks for consumers. For example, the recent Jeep hacking incident, in which hackers updated the ECU's firmware to adjust cruise control settings or activate parking brakes, illustrates the

[2] Notice of Proposed Rulemaking, 82 Fed. Reg. 49,550 (Oct. 26, 2017), *available at* https://www.gpo.gov/fdsys/pkg/FR-2017-10-26/pdf/2017-23038.pdf.

dangers attendant with permitting *any* type of circumvention of a vehicle's TPM. *See* Ex. A. Further, infotainment platform software is also responsible for implementing the National Highway Traffic Safety Administration's Federal Motor Vehicle Safety Standards-111 for rearview mirrors. For some of Harman's customers, this would mean an Automotive Safety Integrity Level (ASIL) A certification requirement, a mandate that may likely be abandoned by circumvention from aftermarket repair shops.

Permitting the circumvention of technical protection mechanisms ("TPMs") for telematics systems could result in serious privacy concerns for the owner of the vehicle. Information typically controlled by telematics systems, such as a customer's geolocation data, could be considered extremely sensitive personally-identifiable information ("PII"). Unauthorized access to such PII may give rise to consumer notification requirements under state breach notification laws.

The CTA also seeks the exemption not just for owners of motorized land vehicles, but also in circumstances where "circumvention is…at the request of the owner of the vehicle." Researcher and repair shops legally able to circumvent telematics services could lead to exposure of critical intellectual property, such as the source code for Harman's proprietary telematics systems, such that unauthorized individuals could either replicate the telematics systems or sell the source code on the dark web to potential third party counterfeiters. The overbroad proposal that circumvention is permitted so long as it is "at the request of the owner" could mean that hackers may circumvent the system so long as an owner so requested.

3. Permitting Circumvention of Infotainment Systems is Fundamentally At Odds With Controlling Federal Regulation

Under F.C.C. regulations concerning radio frequency ("RF") devices contained in electronic-electrical products that are capable of emitting radio frequency energy, Harman is *required* to lock down the various parameters controlling maximum-emitted RF power in wireless radios. Therefore, circumvention would fundamentally be at odds with controlling federal regulations that prohibit modifications to the software that could, for example, disable dynamic frequency selection (technology necessary for preventing interference to radars), enable tuning to unauthorized frequencies, increase power above authorized levels, etc.

4. Permitting an Exemption for Infotainment Systems Will Result in Unauthorized Piracy of Copyrighted Works

Contrary to the CTA's one-sentence statement that telematics systems consist of non-copyrightable data and entertainment systems are comprised of "storage capacity,"[3] infotainment systems provide access to a host of copyrighted content—such as film, television, music, geographic databases, and maps—that are protected by copyright law. For example, Sirius XM, a key component of many in-car entertainment systems, is a subscription-only service that contains countless copyrighted works of music, comedy, and premium talk content. Circumvention of

[3] Long Comment Regarding a Proposed Exemption Under 17 U.S.C. § 1201 at 6 (Dec. 18, 2017), https://www.copyright.gov/1201/2018/comments-121817/class7/class-07-initialcomments-cta.pdf.

these entertainment systems could result in unauthorized piracy of copyrighted works, as TPMs operate to protect the content of copyright holders. Just as with the Register's recommendation in the 2015 triennial rulemaking, proponents for the exemption for diagnosis, repair, and modification of computer programs are chiefly focused on the computer programs on ECUs that control the vehicle's mechanical operation, not entertainment systems used to consume copyrighted content.[4] The CTA has not put forth any evidence "to support a need for circumvention of the TPMs on these ECUs, especially when balanced against concerns about unauthorized access to the services and content they protect."[5]

The CTA's sole argument in support of circumvention of entertainment systems is that the present exclusion of entertainment systems cannot be justified by copyright law precedent. In support of this argument, the CTA presents a single case—the 1984 Supreme Court decision in *Sony Corp. of America v. Universal City Studios, Inc.* But *Sony* was not a Section 1201 case, and, in any event, *Sony* held no such thing. Rather, *Sony* focused on whether the use of tape recorders to archive copyrighted material was a "fair use." The Supreme Court held that it was, because the Betamax VHS player's "time-shifting" capabilities was fair use. The CTA notably does not state how circumvention, in and of itself, is equally transformative, thereby qualifying for a fair use exception.

Further, the CTA's argument, that "it has been the law that providing the ability to receive copied content…is not itself an infringement of copyright" makes no sense when read in connection with the *plain language* of 17 U.S.C. § 1201, which statute provides that no person shall circumvent a technological measure that controls access to a copyrighted work, *absent* exemptions set by the triennial rulemaking. Nor can the CTA justify this position, because there is no such precedent—whether statutory or common law—holding that circumventing an entertainment system in order to access copyrighted films, music, or television shows constitutes fair use. If anything, there is precedent to the contrary. *See Universal Studios v. Corley*, 273 F.3d 429, 459 (2d Cir. 2001) (holding that appellant provides no support for the premise that fair use of DVDs are constitutionally required to be made by copying the original work in its original format).

As will be discussed in Section E, below, it cannot possibly be argued that users are likely to make noninfringing uses of a copyrighted work in connection with circumvention of car entertainment systems—such as for purposes of nonprofit archival, preservation, or educational uses. On the other hand, however, companies like Harman may very well have content agreements in place with certain providers of copyrighted content, such as Sirius XM, that strictly guard how Sirius's content can be used. Permitting the type of circumvention that the CTA advances here risks not only the intellectual property rights of Harman, but also of third party entertainment providers, such as Sirius XM, that enable their copyrighted content to be played on Harman entertainment systems pursuant to end-user license agreements and restrict access by means of anti-circumvention measures.

---

[4] Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, at 246 (Oct. 2015) ("2015 Recommendation"), https://www.copyright.gov/1201/2015/registers-recommendation.pdf.

[5] *Id.*

E. Permitting an Exemption for Infotainment Systems Will Negatively Impact the U.S. Market

Permitting the circumvention of TPMs for entertainment and telematics systems will permit competitors, including foreign ones, to engage in theft of valuable intellectual property owned by leaders in the field, like Harman, who spend tremendous resources in developing the software needed for such telematics/entertainment systems. U.S. companies like Harman not only spend millions of dollars a year investing in intellectual property, but they also contribute significantly to domestic job creation and growth—jobs that would be damaged by foreign theft of Harman's IP. Further, permitting circumvention will *dramatically* affect the market for, and value of, copyrighted works in in-car entertainment and telematics systems, because users will be able to "hack" their systems in order to, for example, receive free satellite radio, or other free access to copyrighted content that users would otherwise have to pay for. Therefore, petitioner's position in advocating for unfettered circumvention rights runs counter to the United States' commitment to improving protection of U.S. IP on a global scale, and permitting an exemption would harm the global competitiveness of U.S. IP rights.

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

Harman's systems are locked down via the use of secure bootloaders that rely on signed certificates derived from a trust anchor (root certificate) installed in the head unit. All updatable platform/OS software must be signed binaries, or else they cannot be installed. Even third-party installable software, whether it be sideloaded from a memory stick or downloaded over the air, must be signed.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

As the Register rightfully noted in her Notice of Inquiry, when considering whether noninfringing uses are being adversely impacted by the prohibition on circumvention, the rulemaking focuses on "distinct, verifiable, and measurable impacts" compared to "*de minimis* impacts."[6]

The CTA's Petition does not set forth any adverse effects on the prohibition on circumvention of entertainment and telematics systems that are real, tangible, or concrete. Rather, the Petition spends little time discussing why it believes the present exclusion of telematics and entertainment systems from the current exemption should not hold, hinging their argument on two grounds: (1) that prohibiting circumvention contravenes the case law as established in *Sony*; and (2) that "[w]ithout the ability to access the telematics system, it may not be feasible for independent repair businesses to repair motorized vehicles and, thereby, to fulfill the purposes of the exemption for the vehicle owner."[7] For the reasons discussed below, both of these justifications do not rise above the speculative or *de minimis* into the realm of the distinct and verifiable.

---

[6] Notice of Proposed Rulemaking, 82 Fed. Reg. 49,550, 49,552 (Oct. 26, 2017), *available at* https://www.gpo.gov/fdsys/pkg/FR-2017-10-26/pdf/2017-23038.pdf.

[7] Petition for New Exemption Under 17 U.S.C. § 1201 at 4 (Sep. 13, 2017), https://www.copyright.gov/1201/2018/petitions-091317/class7/class-07-newpetition-aca-cta.pdf.

1. There Are No Compelling Noninfringing or Fair Uses To Be Made of Copyrighted Content Controlled by TPMs for Entertainment/Telematic Systems

Telematics and, in particular, entertainment systems in automobiles, contain many works protected by copyright, such as music, film, television, and software. For example, an entertainment system in a vehicle may contain access to satellite radio, which provides a user access to copyright music and premium talk content. Circumvention may result in the unauthorized performance, for example, of copyrighted music—a use that is undoubtedly infringing if unauthorized by the copyright holder.

It is difficult to conceive of a non-infringing use that a user may want to make of the vast majority of copyrighted content controlled by TPMs for entertainment and telematics systems, which consists mostly of in-car entertainment**.** In other words, unlike in a situation where a teacher may need access to the copyrighted content in a DVD protected by digital rights management for teaching purposes, there is no such justification for why a teacher would similarly need access to the same film content protected by TPMs in a vehicle's entertainment system for teaching purposes. Indeed, a vehicle's in-car entertainment, most of which are copyrighted works, are not subject to such fair uses as nonprofit archival, nonprofit preservation, educational purposes, criticism, comment, news reporting, teaching, scholarship, or research—at least, there is no reason why a researcher or commenter would need access to the copyrighted content *as specifically made available in an in-car entertainment system*, rather than, say, a DVD, an e-book, or otherwise. As the Register noted in her Recommendation in connection with the 2012 rulemaking cycle, "the mere fact that a particular medium or technology may be more convenient to use for noninfringing purposes than other formats is generally insufficient to support an exemption….If sufficient alternatives exist to permit the noninfringing use, there is no substantial adverse impact. Proponents of an exemption must show sufficient harm to warrant the exemption from the default rule established by Congress, the prohibition on circumvention."[8] *See also Universal Studios*, 273 F.3d at 459 (finding "no support for the[] premise that fair use" dictates "copying the original work in its original format").

With regard to the two arguments proponents advance in favor of the exemptions, proponents do not explain how the act of circumvention to *receive* copyrighted content is a fair use. As discussed in detail *supra*, pp. 5, the Betamax player at issue in *Sony* was found to constitute fair use because it had significant "time-shifting" capabilities. Proponents make no argument here that the act of circumvention for purposes of receiving copyrighted content, in and of itself, is somehow also significant or transformative for purposes of the fair use exception.

Second, the argument that repair "may not be feasible" without the ability to access the telematics system is the epitome of a hypothetical, theoretical, and speculative statement that the Office has admonished petitioners to avoid. As discussed above, there are no real, tangible adverse effects associated with a prohibition on circumvention of TPMs for entertainment and

[8] Section 1201 Rulemaking: Fifth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, at 8 (Oct. 2012), https://www.copyright.gov/1201/2012/Section_1201_Rulemaking_2012_Recommendation.pdf.

telematic systems. Nor is "tinkering with" the telematics system a fair use, as it is resolutely not transformative. As the Copyright Office has made clear, adapting firmware for diagnostic, repair, or modification purposes does not "add something new, with a further purpose of different character, altering the [original firmware] with new expression, meaning, or message."[9] While most courts have held that the first factor, and specifically, transformative use, is by far the most important factor in any fair use analysis, *see, e.g.*, *Cariou v. Prince*, 714 F.3d 694, 706 (2d Cir. 2013), some courts have also emphasized the primacy of the fourth factor, or the effect on the market of the copyrighted work. *See Kienitz v. Sconnie Nation LLC*, 766 F.3d 756, 759 (7th Cir. 2014). Under this factor, permitting the circumvention of TPMs for entertainment and telematics systems will *dramatically* affect the market for, and value of, copyrighted works in in-car entertainment and telematics systems, because users will be able to "hack" their systems in order to, for example, receive free satellite radio, or other free access to copyrighted content that users would otherwise have to pay for. Further, permitting circumvention of TPMs will permit competitors to engage in theft of valuable intellectual property owned by leaders in the field, like Harman, who spend tremendous resources in developing the software needed for such telematics/entertainment systems. Indeed, in her 2015 recommendations, the Register found that "circumvention of access controls on entertainment and telematics ECUs could result in a diminution in the value of copyrighted works if those systems could no longer reliably protect the content made available through them."[10]

Therefore, because the heart of the fair use analysis (the first and fourth factors) strongly militate against circumvention of infotainment systems as fair use, proponents have no credible argument that circumvention constitutes fair use under Section 107 of the Copyright Act.

2. Weighing Section 1201(a)(1)(C)'s Statutory Factors Confirms That Harm to the Market for Copyrighted Works in In-Car Entertainment Systems Vastly Outweighs Any Potential Fair Uses of Those Works

Specifically, in considering Section 1201(a)(1)(C)'s statutory factors, prohibiting circumvention of TPMs for entertainment and telematics systems: (i) does not decrease the availability for use of copyrighted works, as those works are available in numerous other formats other than in-car entertainment; (ii) does not decrease the availability for use of works for nonprofit archival, preservation, and educational purposes, for the same reason as stated in (i); and (iii) does not impact any use of copyrighted works for criticism, comment, news reporting, teaching, scholarship, or research, for the same reasons as described in (i). On the other hand, *permitting* the circumvention of TPMs for entertainment and telematics systems will *dramatically* affect the market for, and value of, copyrighted works in in-car entertainment and telematics systems, because users will be able to "hack" their systems in order to, for example, receive free satellite radio, or other free access to copyrighted content that users would otherwise

[9] 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, 94-95 (June 11, 2010) (quoting *Campbell v. Acuff-Rose*, 510 U.S. 569, 579 (1994)); https://www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf.

[10] 2015 Recommendation at 241.

have to pay for. Further, permitting circumvention of TPMs will permit competitors to engage in theft of valuable intellectual property owned by leaders in the field, like Harman, who spend tremendous resources in developing the software needed for such telematics/entertainment systems.

These considerations outweigh any purported need to circumvent entertainment/telematics systems to research the copyrighted underlying software that operates these systems, which is the only conceivable "research" purpose, for the only conceivable class of copyrighted work, contemplated by Section 1201(a)(1)(C)'s statutory factors. However, the software that operates these systems comprises but a small portion of all the copyrighted works protected by TPMs for entertainment and telematics systems. Further, Harman is unaware of any possible definition of "research" that would be narrow enough to preclude the type of malicious IP theft that could occur upon circumvention. Exposure of intellectual property developed at great expense by industry leaders, such as Harman, to unauthorized individuals could result in the unauthorized copying and selling of that intellectual property in nefarious markets such as the dark web. "White hat" researchers who are purportedly circumventing a telematic or entertainment system for "safety research" can easily turn into "black hat" hackers at their discretion.

* * *

In declining to provide an exemption for entertainment and telematics services, the Register's finding in the last triennial rulemaking, that there is no evidence "to support a need for circumvention of the TPMs on these ECUs, especially when balanced against concerns about unauthorized access to the services and content they protect", [11] should hold with equal force in this triennial rulemaking.

DOCUMENTARY EVIDENCE

Exhibit A: *Jeep Hackers At It Again, This Time Taking Control of Steering and Braking Systems*, https://www.theverge.com/2016/8/2/12353186/car-hack-jeep-cherokee-vulnerability-miller-valasek

[11] *Id.*

EXHIBIT A

Jeep hackers at it again, this time taking control of steering and braking systems

By Jordan Golson | @jlgolson | Aug 2, 2016, 1:45pm EDT

SHARE

Jeep

A pair of hackers have compromised their Jeep Cherokee, fooling the car into doing dangerous things like turning the steering wheel or activating the parking brake at highway speeds. It's the same pair that hacked their Jeep remotely last year. But, because this version of the hack requires physical access to the car — in this case, through a laptop connected to the OBD II engine diagnostic port — it may not be quite as scary, except for the fact that they're controlling way more vehicle systems.

A year ago, the two cybersecurity researchers, Charlie Miller and Chris Valasek, remotely compromised a Jeep Cherokee. They were able to disable the car's transmission and brakes, and, while the vehicle was in reverse, take over the steering wheel. These were all possible by abusing existing functionality in the car like the self-parallel parking feature, and commanding the vehicle to do things within the vehicle's limitations.

For example, the steering wheel could only be controlled while the car was going in reverse below a certain speed. That's because the car's central computer had checks to ensure that the car would only steer itself when it was in the auto-park mode. Chrysler later issued a patch to fix the vulnerability.

After last year's hack, Valasek and Miller went to work at Uber's Advanced Technology Center in Pittsburgh.

The new hack, while being more difficult to execute — the hackers were physically in the car at the time — nonetheless illustrates the dangers of connected cars. They were able to update the electronic control unit's (ECU) firmware to disable those checks and balances, allowing them to take control of the steering at any time, not just when the car was going in reverse. They could turn the steering wheel at any speed, activate the parking brake, or adjust the cruise control settings. Theoretically, that sort of manipulation could cause someone to veer off the road or rear-end someone.

"It's not like I can take control of the car and drive you to my house and you can't stop me," said Miller to *Wired*. "But if you're not paying attention, it's definitely dangerous."

What's even more concerning is that, while the hack in this case required the researchers to be physically in the car, it could be possible for other OBD II-connected dongles like those from Automatic, the Verizon Hum, or the sensors issued by some insurance companies to be compromised in a similar manner.

Miller and his partner Chris Valasek will present their findings at the Black Hat security conference later this week. For its part, Fiat Chrysler (FCA) issued a statement to *Wired* saying, "While we admire their creativity, it appears that the researchers have not identified any new remote way to compromise a 2014 Jeep Cherokee or other FCA US vehicles." FCA also pointed out that the hack was performed on a vehicle with an older version of its software, something that Valasek and Miller confirmed.

Regardless, the more connected — and autonomous — our cars get, the more on guard we will need to be.

MERCEDES' DRIVERLESS CAR OF THE FUTURE