U.S. COPYRIGHT OFFICE, LIBRARY OF CONGRESS

In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201

Docket No. 2014-07

Comment of Electronic Frontier Foundation

1. Commenter Information:

Kit Walsh
Corynne McSherry
Mitchell Stoltz
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
rulemaking-2015@eff.org

Counsel for EFF:
Marcia Hofmann
Law Office of Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
(415) 830-6664

The EFF is a member-supported, nonprofit public interest organization devoted to maintaining the traditional balance that copyright law strikes between the interests of copyright owners and the interests of the public. Founded in 1990, EFF represents thousands of dues-paying members, including consumers, hobbyists, computer programmers, entrepreneurs, students, teachers, and researchers, who are united in their reliance on a balanced copyright system that ensures adequate protection for copyright owners while facilitating innovation and broad access to information in the digital age.

2. Proposed Class Addressed

Proposed Class 22: Vehicle Software —Security and Safety Research

This proposed class would allow circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicle, [including programs that modify the code or data stored in such a vehicle and including compilations of data used in controlling or analyzing the functioning of such a vehicle,] for the purpose of researching the security or safety of such vehicles. Under the exemption as proposed, circumvention would be allowed when undertaken by or on behalf of the lawful owner of the vehicle[or computer to which the computer program or data compilation relates]. (brackets denote edits proposed by EFF)

In addition to computer programs actually embedded or designed to be embedded in a motorized land vehicle, the exemption as proposed by EFF includes computer programs designed to modify the memory of embedded hardware. Such software, such as updates and proprietary tools, raises the same security and safety concerns[1] and is often encrypted (requiring circumvention), and analyzing an update is often necessary to gain access to already-embedded software.[2] This

[1] Appendix D, Statement of Chris Valasek at ¶ 7 ("Valasek Statement").
[2] Appendix B, Statement of Charlie Miller at ¶ 6 ("Miller Statement").

comment uses the terms "vehicle firmware" or "vehicle software" interchangeably to refer to all the works falling within the proposed class.

3. Overview

Modern vehicles are equipped with a system of computers that monitor and control many of the vehicle's functions.[3] Ignition, braking, and engine power are among the many functions controlled in part by computers, often called Electronic Control Units (ECUs).[4] For vehicles to remain safe and secure, it is essential that users be able to study the software that controls vehicular computers.[5] Independent researchers can discover programming errors that endanger passengers, such as an unintended acceleration defect that caused a fatal accident, as a jury determined in 2013.[6] Independent researchers have also found errors that would allow a remote attacker to take control of a vehicle's functions,[7] and have written a patch to resolve the vulnerability.[8] This research is of such crucial importance that experts have received funding from multiple government agencies to support it, including the NSF, DARPA, and the Air Force Office of Scientific Research.[9]

The anti-circumvention provisions of the DMCA, however, chill such research. Vehicle software is increasingly subject to technical restrictions that must be circumvented in order to review the software running in a vehicle. This reduces the ability of independent experts to identify flaws in critical code on which hundreds of millions of Americans depend in their travels

As with any complex system of computers, programming errors and oversights are inevitable. One DARPA-funded researcher reported that "every system I have looked at *has been vulnerable to*

---

[3] *See* Graham Pitcher, *Growing Number of ECUs Forces New Approach to Cars Electrical Architecture*, NEW ELECTRONICS (Sept. 25, 2012), http://www.newelectronics.co.uk/electronics-technology/growing-number-of-ecus-forces-new-approach-to-car-electrical-architecture/45039/;
Ben Wojdyla, *How it Works: The Computer Inside Your Car*, POPULAR MECHANICS (Feb. 21, 2012), http://www.popularmechanics.com/cars/how-to/repair/how-it-works-the-computer-inside-your-car.

[4] Karl Koscher, et al., *Experimental Security Analysis of a Modern Automobile*, CENTER FOR AUTOMOTIVE EMBEDDED SYSTEMS 2010 IEEE Symposium on Security and Privacy 5 (May 16, 2010), http://www.autosec.org/pubs/cars-oakland2010.pdf.

[5] Stephen Checkoway, et al., *Comprehensive Experimental Analysis of Automotive Attack Surfaces*, USENIX Security (August 10 –12, 2011), http://www.autosec.org/pubs/cars-usenixsec2011.pdf; Miller Statement at ¶ 3.

[6] Baker, Phil (2013-11-04). "Software bugs found to be cause of Toyota acceleration death". San Diego Source. Retrieved 2014-01-24; Yoshida, Junko (2013-10-23). "Acceleration Case: Jury Finds Toyota Liable". EE Times. Retrieved 2014-01-24.

[7] Darlene Storm, *Untraceable $20 Device Can Allow Hacker to Control a Car 'From Miles Away'*, COMPUTERWORLD (Mar. 31, 2014, 5:57PM), http://www.computerworld.com/article/2476039/cybercrime-hacking/untraceable--20-device-can-allow-hacker-to-control-a-car--from-miles-away-.html; Martyn Williams, *BMW Cars Found Vulnerable in 'Connected Drive' Hack*, PCWORLD (Jan. 30, 2015) http://www.pcworld.com/article/2878437/bmw-cars-found-vulnerable-in-connected-drive-hack.html; Valasek Statement at ¶ 5.

[8] Jim Finkle, *Hacking Experts Build Device to Protect Cars from Cyber Attacks*, REUTERS (July 22, 2012, 5:15PM), http://www.reuters.com/article/2014/07/22/cybersecurity-autos-idUSL2N0PX2FH20140722; Miller Statement at ¶ 7.

[9] Koscher et al., *supra* note 3, at 15; *see also* Andy Greenberg, *DARPA-Funded Researchers Help You Learn to Hack A Car for A Tenth The Price*, FORBES, http://www.forbes.com/sites/andygreenberg/2014/04/08/darpa-funded-researchers-help-you-learn-to-hack-a-car-for-a-tenth-the-price/

some type of serious attack."[10] These errors are particularly persistent when they reside in software that is hidden from independent researchers.[11] One unfortunate side effect of Section 1201 is to exacerbate this problem by casting a legal cloud over otherwise-lawful security and safety research that could surface and resolve the threats posed by errors and vulnerability in vehicle software.[12]

The same lack of access to vehicle software also deprives consumers of information about programming choices being made by manufacturers.[13] These choices affect the privacy and safety of vehicle owners, who deserve access to information about how their vehicles are going to treat them and the opportunity to safeguard themselves against software flaws. If the veil of secrecy can be lifted, it will be pointless for a manufacturer to deny that a software error exists, and there will be all the more motivation for them to carefully audit software before it is deployed to the field.

Courts have long recognized that copyright law permits research into the way a piece of software functions, and there is no reason to deviate from that rule when the software relates to a vehicle. Security and safety researchers are interested in functional, noncopyrightable aspects of vehicle software and copyright simply has no business getting in the way of this kind of functional research. Accordingly, the Librarian should grant an exemption for the proposed class.

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

There are at least three technologies that restrict access to ECU firmware. The first includes "challenge-response mechanisms," involving access codes, passwords, keys, or digital signatures.[14] The second is encryption, which is used to restrict access both to firmware contained in certain vehicle ECUs and to firmware update files.[15] The third involves the disabling of access ports, such as "JTAG pins," on the circuitry itself.[16]

---

[10] Miller Statement at ¶ 4 (emphasis in original).
[11] Bruce Schneier, SECRETS AND *Lies*: DIGITAL SECURITY IN A NETWORKED WORLD 344 (2000) ("The only way to have any confidence in the security of a system is over time, through expert evaluation. And the only way to get that expert evaluation is if the details of a system are public.")
[12] Miller Statement at ¶ 9.
[13] Valasek Statement at ¶ 4.
[14] *See, e.g.*, Volha Bordyk, *Analysis of Software and Hardware Configuration Management for Pre-Production Vehicles*, 35 (Chalmers University of Technology 35 (Jan. 2012), http://publications.lib.chalmers.se/records/fulltext/156295.pdf; Charlie Miller & Chris Valasek, *Adventures in Automotive Networks and Control Units* 15, http://illmatics.com/car_hacking.pdf (last visited Feb. 4, 2015); *Factory Locked ECUs*, REVO, http://www.revotechnik.com/support/technical/factory-locked-ecus (last visited Feb. 4, 2015).
[15] Bordyk, *supra* note 13, at 21 (noting that software updates for some Volvo vehicles are encrypted); Rory Jurnecka, *Cobb Tuning Cracks Nissan GT-R 's Encrypted ECU*, MOTOR TREND (Apr. 09, 2008), http://wot.motortrend.com/cobb-tuning-cracks-nissan-gtrs-encrypted-ecu-308.html; Damon Lavrinc, *The Dinan S1 M5 is How an Obsessed Tuner Builds a Better BMW*, JALOPNIK (Oct. 09, 2014), http://jalopnik.com/the-dinan-s1-m5-is-how-an-obsessed-tuner-builds-a-bette-1643950782.
[16] Craig Smith, *Car Hackers' Handbook*, http://opengarages.org/handbook/2014_car_hackers_handbook_compressed.pdf , at pp. *56-60*.

A. Challenge-response Mechanisms and Methods of Circumvention

Many vehicles provide a physical interface to connect to the vehicle's internal network of ECUs. ECUs constantly communicate with one another over this internal network, and a computer plugged into the network can send and receive data as well.[17] Some ECUs are configured to refuse commands (such as the command to supply a copy of their firmware, or to update their firmware) unless a challenge-response condition is met.[18] When a challenge-response mechanism is in place, a user must answer an ECU's "challenge" with the correct 16-32 bit "response" in order to view and manipulate ECU firmware.[19] In most vehicles, the correct responds depends upon the Vehicle Identification Number (VIN) of a car and the hardware parts number associated with a given ECU. The response is therefore unique to each vehicle and each ECU. This category also includes secure boot loader mechanisms that disable an ECU unless a key is supplied.[20]

Solving the challenge-response mechanism by brute force analysis is mathematically possible (requiring a little over a week for a 16-bit key).[21] More commonly, researchers solve such challenges by extracting the necessary keys from official ECU software updates or diagnostic tools,[22] or from related firmware.[23] (Obtaining these keys may itself require circumvention of encryption, as discussed below). At least one court has held that applying a key to a TPM may qualify as circumvention if the key was obtained without authorization of the rightsholder.[24]

B. Encryption and Methods of Circumvention

Increasingly, manufacturers are encrypting the firmware that resides on ECUs as the hardware becomes capable of handling larger encryption keys. For example, many BMW ECUs use RSA encryption,[25] as does the Bosch Electronic Diesel Control EDC 16.[26] Encryption is also used to restrict access to data compilations containing vehicle-related data.[27] In addition, files containing official updates to ECU firmware can be encrypted, as part of a mechanism in which update files

[17] Koscher et al., *supra* note 3, at 5-6.
[18] *Id*.
[19] *Id*. at 6.
[20] Appendix C, Statement of Craig Smith at ¶ 6 ("Smith Statement").
[21] Koscher et al., *supra* note 3, at 7; Smith Statement at ¶ 8.
[22] *Id*.; Miller Statement at ¶ 6; Valasek Statement at ¶ 3.
[23] Valasek Statement at ¶ 4.
[24] *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004).
[25] *Real BMW S55, N63, N63TU, S63TU Tuning Coming – F-Series Infineon Tricore ECU's Cracked,* BOOSTADDICT (Dec. 11, 2014, 5:33PM), http://www.bimmerboost.com/content.php?5514-Real-BMW-S55-N63-N63TU-S63TU-tuning-coming-F-Series-Infineon-TriCore-ECU-s-cracked; *Mini Cooper S Ecu Upgrade Nm Engineering R55 R56 R57 R58 R59*, MINIMANIA, http://new.minimania.com/part/G2NME4300-P/Mini-Cooper-S-Ecu-Upgrade-Nm-Engineering-R55-R56-R57-R58-R59 (last visited Feb. 4, 2015).
[26] *Factory Locked ECUs*, REVO, http://www.revotechnik.com/support/technical/factory-locked-ecus; (last visited Feb. 4, 2015); Alberto Illera & Javier Vidal, *Dude, WTF in my Car?* at slide 18 and 27, available at https://media.defcon.org/DEF%20CON%2021/DEF%20CON%2021%20presentations/Albert%20Garcia%20Illera%20and%20Javier%20Vazquez%20Vidal-Updated/DEFCON-21-Illera-Vidal-Dude-WTF-in-My-Car-Updated.pdf (last visited Feb. 4, 2015).
[27] Complaint, *Ford Motor Co. v. Autel Inc.*, No. 14-13760 (E.D. Mich. filed Sept. 29, 2014), available at https://www.eff.org/files/2015/01/05/ford_v_autel_complaint.pdf.

must prove their authenticity before the ECU will accept the update.[28] This works by using a pair of related but different encryption keys, one public and one private. The public key, which can decrypt data encrypted by the private key, is stored within the ECU, whereas the private key is only given to authorized entities.[29] Operators wishing to update firmware encrypt the update files using the private key. If the ECU can decrypt the files with its matching public key, it knows the files are from an authorized party and then installs the update.[30] This is a recent phenomenon: it would have been impossible to rely on advanced encryption with previous technology due to the lack of processing power in ECUs.[31]

As with challenge-response mechanisms, encryption can be overcome by brute force[32] by acquiring the key from locations such as online message boards, or by deriving it from the diagnostic tools provided to authorized dealers. However, unlike challenge-response protection, security experts cannot currently break the encryption on vehicles that use 1024-bit keys[33] using brute force methods without specialized computing equipment, though they estimate this will be technically feasible within the next five years.[34] Instead, individuals would need to use other methods like finding errors in the encryption algorithm that inadvertently reveal the key, such as reusing the same number in place of what should be a randomly generated number.[35]

C. Disabled Access Ports and Methods of Circumvention

In some vehicles, it is possible to access firmware by dismantling the vehicle and gaining physical access to the memory on which the firmware is stored, bypassing the normal communications interface wired up within the vehicle. By connecting a voltmeter to data pins on the physical hardware, it is sometimes possible to extract information from memory, including firmware or keys that can be used to overcome a challenge-response mechanism or encryption.[36] However, some manufacturers intentionally disable these access ports (for example, the JTAG port).[37] One means of disabling access entails setting a control bit to prevent extraction of firmware unless

---

[28] *See* Eduardo Ciniglio et al., *RSA Authentication for Secure Flashing of Automotive ECUs* at 2-3 (French Institute for Research in Computer Science and Automation, Nov. 17, 2010), available at http://www-sop.inria.fr/members/Emilio.Mancini/papers/rsa-auth.pdf; Bordyk, *supra.* at 21; *see also* Koscher et al., *supra* note 3, at 14 (describing cryptographically signed firmware updates as a "simple security mechanism").

[29] Koscher et al., *supra* note 3,, at 4-5.

[30] Keith@APR, Comment on *New to Audi tuning – Why no handheld-flashing ecu upgrades?*, AUDIZINE FORUMS (Jan. 7, 2011, 12:05 PM).

[31] *See id.* ("The only reason it never happened before is because you would be pissed if it took 3 seconds for all of the controllers to calculate all of the RSA's before the car was allowed to start every time you turn the key on."); *see also* Koscher et al., *supra* note 3. at 3 ("It is common belief that the processing power and memory space available in a ECU do not lend themselves to the use of the time- and space-expensive public key cryptographic algorithms.")

[32] *See, e.g.*, Thorsten Kleinjung et al., "*Factorization of a 768-bit RSA modulus*,", CRYPTOLOGY EPRINT ARCHIVE (June 2010), available at http://eprint.iacr.org/2010/006.pdf (last accessed Feb. 4, 2015)

[33] Keith@APR, *supra* note 29.

[34] Kleinjung et al, *supra* note 31, at 1.

[35] This was an attack method used to find the private key for Sony's Playstation 3. *See* Jonathan Fildes, "*iPhone Hacker Publishes Secret Sony Playstation 3 key*, " BBC NEWS (Jan. 6, 2011), http://www.bbc.co.uk/news/technology-12116051 (last visited Feb. 4, 2015) (describing how Sony made a "critical mistake" in their security algorithm).

[36] Smith, *supra* note 15, at 56-57.

[37] *Id*. at 57; *see also* Appendix A, Statement of David Blundell at ¶ 7 ("Blundell Statement").

certain signals are received during runtime.[38] In such cases, clock or power glitching (also known as "fault injection") can be used to control the relevant bit and enable access to firmware.[39] Another means is to semi-permanently disable extraction of firmware by setting a type of permanent memory called a fuse (such as a JTAG fuse).[40] When this has been done, voltage or optical glitching is necessary in order to overcome the obstacle presented by the fuse.[41]

5. Asserted Noninfringing Use(s)

Security and safety research that requires copying of vehicle software or otherwise implicates the exclusive rights of the copyright owner is authorized by fair use law and by 17 U.S.C. § 117.

The simplest example of a use of vehicle software within the proposed class is copying software into a format that enables analysis.[42] For example, a researcher may hook up a general-purpose computer to a vehicle's internal network and instruct an ECU to upload a copy of its memory.[43] The researcher can then review the code using third-party software.[44]

A researcher may also prepare modified code based on vehicle software and write this new code into an ECU in order to test security vulnerabilities or fixes.[45] For example, a team funded by the NSF and the Air Force tested a vulnerability that allowed them to bridge otherwise separate networks within the car, demonstrating that safety-critical systems could be compromised via vulnerabilities in other, less-defended systems (for example, the Bluetooth interface with a driver's smartphone). The researchers needed to overcome a challenge-response mechanism to instruct ECUs to provide a copy of their code, then reverse engineered the code with third-party debugging software called "IDA Pro" in order to "explicitly understand how certain hardware features were controlled."[46] This vulnerability could only be explored through such debugging.[47] The research team noted that the vulnerability "is particularly concerning given the abundance of potential aftermarket add-ons available" with access to part of the vehicle's internal network.[48] In another test, they deployed code that forced the windshield fluid pump and wipers to activate when the car reached a certain speed, then to reboot and erase the evidence of the modification.[49]

Another research team, funded by DARPA, explored the security of dozens of other vehicle ECUs, using similar methods. One additional technique used by this team was the extraction of keys from official software updates.[50] Since a software update needs to be able to modify the code on an ECU, it must contain an authentication mechanism if there is a TPM restricting write access to the ECU program memory.[51] The same mechanism can be used to obtain read access – that is,

---

[38] Smith, *supra* note 15, at 57-60; *see also* Blundell Statement at ¶ 7.
[39] Smith, *supra* note 15, at 57-60; *see also* Blundell Statement at ¶ 7.
[40] Smith, *supra* note 15, at 57-60; *see also* Blundell Statement at ¶ 7.
[41] Smith, *supra* note 15, at 57-60; *see also* Blundell Statement at ¶ 7.
[42] Koscher et al., *supra* note 3, at 9; *see also* Smith, *supra* note 15, at 28-33.
[43] Koscher et al., *supra* note 3, at 9; *see also* Smith, *supra* note 15, at 28-33.
[44] Koscher et al., *supra* note 3, at 9; *see also* Smith, *supra* note 15, at 28-33.
[45] Koscher et al., *supra* note 3, at 12-13; *see also* Smith, *supra* note 15, at 41-44.
[46] *Id*. at 9.
[47] *Id*.
[48] *Id*. at 12-13.
[49] *Id*. at 13.
[50] Miller & Valasek, *supra* note 8, at 15; Miller Statement at ¶¶ 6,7.
[51] Miller & Valasek, *supra* note 8, at 15; Miller Statement at ¶¶ 6,7.

to copy the pre-existing code out of the vehicle ECU.[52] Alternatively, if only write access can be obtained, it is sometimes possible to use write access to alter the behavior of the ECU so that its software can then be extracted.[53]

This team also emphasized the importance of understanding the functionality of proprietary information within diagnostic tools, one of them explaining that "diagnostic tools are integral to understanding the functionality and security of every vehicle on the road…. Researchers need to understand these tools and their underlying protocols to properly assess a vehicle from a security perspective."[54] Circumventing encryption or other access controls on such a tool (which may include software and data compilations) is thus another exemplary, lawful use of a work falling within the proposed class.

A. Fair Use

The requested exemption is necessary to enable research and scholarship into vehicle security and safety. This research is an archetypical fair use codified in Section 107, undertaken to enhance public knowledge about the functioning of vehicles to which hundreds of millions of Americans trust their lives.

In the course of engaging in security and safety research, an individual may copy the code (typically onto a general-purpose computer for analysis), modify the code (for example, to detect or patch a security vulnerability or safety issue), and distribute the code as part of scholarly discourse. Such discourse could include criticism of the code's flaws, positive scholarship regarding its approach to security or safety, or reporting on matters of public interest, including vulnerabilities and bugs. These acts potentially implicate the exclusive rights granted to copyright owners, but are lawful as fair uses.

1. Purpose and Character of the Use

The "central purpose" of the first factor is to determine whether or not the use in question "merely supersedes the objects of the original creation" or is transformative.[55] Research and scholarship are purposes that are explicitly called out in Section 107 as supporting a finding of fair use.

Over the years, a robust body of caselaw has developed recognizing uses of copyrighted work that enable greater access to information as fair uses. Some of these cases deal specifically with research into functional aspects of software and have informed the Register's prior decisions to recommend exemptions for video game security research, jailbreaking, and other software-related exemptions.

In *Sega v. Accolade*, the Ninth Circuit explained that research into the functional aspects of Sega's video game software was a legitimate purpose, even for a competitor seeking to develop

[52] Miller & Valasek, *supra* note 8, at 15; Miller Statement at ¶¶ 6,7.
[53] *See* Miller & Valasek, *supra* note 8, at 41-44.
[54] Valasek Statement at ¶ 7.
[55] *Campbell v. Acuff Rose Music, Inc.*, 510 U.S. 569, 579 (1994) (internal quotations omitted).

competing games.[56] The court emphasized that the functional aspects of Sega's software were not copyrightable, and recognized that copying the entire software program, including any copyrightable elements, was necessary for analysis.[57] The court later reaffirmed this reasoning in *Sony v. Connectix*, explaining that it was legitimate for Connectix to copy Sony's Playstation BIOS in order to understand its functional parameters and allow it to create a competing means of playing games designed for the Playstation console.[58]

Additional cases have reaffirmed that increasing public access to information is a legitimate and important purpose that supports a finding of fair use, including book search and image search functions.[59]

In light of such cases, the Register recommended a comparable exemption allowing "good faith testing for, investigating, or correcting security flaws or vulnerabilities" in video games in the 2010 Rulemaking.[60] The Register found that "such good faith research constitutes fair use," noting the "socially productive purpose of investigating computer security and informing the public."[61]

Just like the functional research of Accolade and Connectix, security and safety research involving vehicle software has a legitimate purpose that falls well within the scope of fair use.[62] As Chris Valasek, one of the DARPA-funded researchers put it, "Dr. Miller and I pursue our research to educate the public and automotive industry about these risks and how to mitigate them. Our goal is to advance the state of knowledge in this field in hopes of making it harder for malicious actors to attack vehicles in the future."[63]

The security and proper functioning of vehicle computers are at least as important as the security of personal computers running video game software, an interest the Register recognized in the 2010 Rulemaking. After all, there are very immediate risks of personal harm if a vehicle malfunctions.[64]

Copyrightable elements of vehicle software are incidental to researchers' purpose in understanding and critiquing the code's functionality, which is where vulnerabilities and errors lie. Researchers examining vehicle software are interested in functional properties of the software.[65] Are security and safety measures correctly implemented, or are there conditions in which they will fail? How does the code safeguard against electrical glitches? Is the computing environment as stable as an it

---

[56] *See Sega Enterprises Ltd. v. Accolade, Inc.,* 977 F.2d 1510, 1522-23 (9th Cir. 1992) (holding that using copyrighted material to study functional requirements was fair use).
[57] *Id.*
[58] 203 F.3d 569, 608. (9th Cir. 2000).
[59] *See Perfect 10, Inc. v. Amazon.com, Inc*., 508 F.3d 1146 (9th Cir. 2007); *Kelly v. Arriba Soft Corp*., 336 F.3d 811 (9th Cir 2002), *Authors Guild, Inc. v. Google, Inc*., 954 F.Supp.2d 282 (S.D.N.Y. 2013).
[60] Final Rule in RM 2008-8, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (July 27, 2010) ("2010 Rule") 75 Fed.Reg. 43825, 43833-34, *available at* http://www.copyright.gov/fedreg/2010/75fr43825.pdf (to be codified at 37 C.F.R. pt. 201).
[61] *See id*. at 43834.
[62] *See* Miller Statement at ¶¶ 2, 3.
[63] Valasek Statement at ¶ 8.
[64] Miller Statement at ¶ 3.
[65] Miller Statement at ¶¶ 5, 7; Valasek Statement at ¶¶ 3, 4, 7.

needs to be when lives depend upon it? What is the scope of a vulnerability? Does a given vulnerability affect the entire network in a vehicle, or just one ECU? Copyright should not prohibit vehicle owners from answering these questions for themselves.

The Copyright Office inquired as to whether permitting research on vehicle software might have a negative impact on security or safety. It is well-recognized in the security community that security can only be reliably obtained when a system is subject to widespread testing.[66] The National Institute of Standards and Technology itself warns that "System security should not depend on the secrecy of the implementation or its components" and recommends "open design."[67]

As computer security guru Bruce Schneier has said, "whenever an IT system is designed and used in secret … the results are pretty awful. …'obscurity means insecurity.'"[68] He explains, "[s]ecurity is a process. For software, that process is iterative. It involves defenders trying to build a secure system, attackers -- criminals, hackers, and researchers -- defeating the security, and defenders improving their system. This is how all mass-market software improves its security. It's the best system we have. And for systems that are kept out of the hands of the public, that process stalls."[69] "Before software bugs were routinely published, software companies denied their existence and wouldn't bother fixing them, believing in the security of secrecy. And because customers didn't know any better, they bought these systems, believing them to be secure. If we return to a practice of keeping software bugs secret, we'll have vulnerabilities known to a few in the security community and to much of the hacker underground."[70]

Schneier's prediction that obscurity means poor security has borne out for vehicle software, in which one researcher reported that "every system I have looked at *has been vulnerable to some type of serious attack*."[71] His research partner explained that they had "shown that given proper time, skill, and budget, an attacker can take control of critical attributes of a vehicle, such as steering, braking, and acceleration."[72] And when researchers told Texas Instruments that they had reverse engineered a "secret algorithm" in a vehicle immobilizer and found it vulnerable, the company released a new, proprietary program with no transparency into whether they had solved the underlying issue or simply bought a little time by increasing the key size.[73]

In addition, public scrutiny increases manufacturers' incentives to program vehicles carefully and to provide patches to fix known bugs and vulnerabilities. In discussing adverse effects, below, petitioners identify issues with vehicle software that have been or could have been detected through independent research. In some cases this could have saved lives.

---

[66] Bruce Schneier, *The Insecurity of Secret IT Systems*, SCHNEIER ON SECURITY (Feb. 14, 2014), https://www.schneier.com/blog/archives/2014/02/the_insecurity_2.html; Miller Statement at ¶¶ 4, 8; Valasek Statement at ¶¶ 2, 3.
[67] Karen Scarfone et al., *Guide to Central Server Security*, http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf (last visited Feb. 4, 2015).
[68] *Schneier*, *supra* note 65.
[69] *Id*.
[70] *Schneier*, *supra* note 65.
[71] Miller Statement at ¶ 4 (emphasis in original).
[72] Valasek Statement at ¶ 5.
[73] Smith Statement at ¶ 4.

The transformative, socially beneficial purpose of security and safety research on vehicle software weighs heavily in favor of fair use.

2. Nature of the Copyrighted Work

The nature of vehicle firmware weighs heavily in favor of fair use under the second statutory factor because it contains "unprotected aspects that cannot be examined without copying."[74] In *Sega*, the Ninth Circuit found the second factor to weigh in favor of fair use where copying for reverse engineering purposes was necessary to understand software's functional parameters – in that case, interoperability requirements.[75] The court explained that permitting the disassembly of copyrighted code is necessary to prevent copyright owners from gaining a "de facto monopoly" over non-copyrightable, functional components of copyrighted works.[76] It reiterated this concern in *Connectix*, explaining that "[i]f Sony wishes to obtain a lawful monopoly on the functional concepts in its software, it must satisfy the more stringent standards of the patent laws."[77]

Any creative, copyrightable aspects of vehicle firmware that may exist are minimal.[78] Where TPMs are deployed, vehicle owners cannot even look at the code to appreciate any such elements. The primary significance, and nature, of vehicle firmware is functional, strongly favoring fair use.

3. Amount and Substantiality of the Portion Used

The third fair use factor examines the amount of the copyrighted work used to determine whether the "quantity and value of the materials used are reasonable in relation to the purpose of the copying."[79] The amount taken need only be "reasonable" and for a legitimate purpose.

In *Connectix* and *Sega*, the Ninth Circuit found that copying the entirety of a software program in order to understand its functional components was necessary and therefore fair in each case. And in *HathiTrust*, *Kelly*, and *Perfect 10,* the respective courts emphasized that copying anything less than the entire work would be insufficient in order to allow enable the transformative purpose of enhancing access to knowledge.[80]

Vehicle security and safety research necessarily requires the use of the entire work, since vulnerabilities may be found anywhere in the code.[81] "Without a full copy of the firmware, it's virtually impossible to properly understand the behavior of an ECU well enough to get predictable results from modifying parameters."[82] Additionally, the technological process of reading the

---

[74] *CorpConnectix,* 203 F.3d at 603.
[75] 977 F.2d at 1526.
[76] *Id.*
[77] 203 F.3d at 605.
[78] Miller Statement at ¶ 7.
[79] *Campbell*, 510 U.S. at 586-87.
[80] *Authors Guild, Inc. v. HathiTrust,* 755 F.3d 87, 98 (2d Cir. 2014) ("For some purposes, it may be necessary to copy the entire copyrighted work, in which case Factor Three does not weigh against a finding of fair use."); *Kelly*, 336 F.3d at 820-21 (holding that third fair use factor did not weigh against copier when entire-work copying was reasonably necessary); *Perfect 10*, 508 F.3d 1146.
[81] Miller Statement at ¶¶ 7, 8.
[82] Blundell Statement at ¶ 5.

firmware off of the ECUs or decrypting an update typically provides the entire program.[83] For each of these reasons, the use of the entire work is fair in light of the legitimate purposes of security and safety research.

4. Market for the Copyrighted Work

The fourth factor looks to direct harms to the market for the copyrighted work.[84] This factor is concerned with the harm of market substitution, not any harm caused by substantive criticism of the copyrighted work.[85] Further, "a use that has no demonstrable effect upon the potential market for, or the value of, the copyrighted work need not be prohibited in order to protect the author's incentive to create."[86]

In the case of vehicle firmware, the copyrighted work is generally sold to end-users along with an entire vehicle. The proposed exemption only allows those who already own a vehicle or device, or those working on the owner's behalf, to circumvent in order to access the related software or data. The owner has already paid for the vehicle or device, including the software. It does not harm any copyright interest of the manufacturer for the owner to analyze the system to understand how it works and evaluate whether it is secure and safe.

For these reasons, as with the video game exemption granted in the 2010 Rulemaking, copying and distribution of vehicle-related software in the course of legitimate research is "unlikely to have an adverse effect on the market for or value of the copyrighted work itself."[87]

5. Other Factors

Manufacturers have not put firmware restrictions on vehicles in order to protect a market for copies of the firmware. Rather, the restrictions exist to control the ways in which vehicle hardware can be used and restrict access to information about vehicular functionality. As the Register stated in 2010, "while a copyright owner might try to restrict the programs that can be run on a particular operating system, copyright law is not the vehicle for imposition of such restrictions, and other areas of the law, such as antitrust, might apply. It does not and should not infringe any of the exclusive rights of the copyright owner to run an application program on a computer over the objections of the owner of the copyright in the computer's operating system." [88]

The same analysis supports the granting of an exemption allowing independent researchers to access vehicle software. Whether or not manufacturers have adopted business models that benefit from restricting access to knowledge about how vehicles function, copyright is not a valid tool to enforce that ignorance.

---

[83] Smith, *supra* note 15, at 60.
[84] *Campbell*, 510 U.S. at 590.
[85] *See id*. at 591-92.
[86] *Sony Corp. of Am. v. Universal City Studios, Inc*., 464 U.S. 417, 450 (1984).
[87] 2010 Rule, 75 Fed.Reg. at 43834.
[88] 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, 96-97 (June 11, 2010)), *available at* www.copyright.gov/1201/2010/initialed-registers-recommendation-june-11-2010.pdf.

B. The Proposed Classes are Non-Infringing Uses As A Matter of Law Under 17 U.S.C. § 117

When vehicle owners purchase their vehicles, they are entitled to access, copy, and modify the vehicle firmware under Section 117 of the Copyright Act.

1. Threshold Issue: Ownership of Copies of Computer Programs in Vehicles

Section 117(a) applies to "the owner of a copy of a computer program." While the caselaw interpreting Section 117 is murky, the best interpretation is that the owner of a vehicle is protected by Section 117 when extracting the firmware embodied in its ECU for analysis.

The Second Circuit has held that a person can own a copy of a computer program even where they don't have formal title in the copy.[89] The court determined that title is not an "absolute prerequisite" to Section 117(a) protection. Rather, a party who exercises "sufficient incidents of ownership" over a copy of the program can be "sensibly" considered the owner of it.[90]

In *Krause*, the plaintiff copyright owner sued his former employer for continuing to use copies of a program he wrote on the employer's network. Despite the absence of a formal transfer of ownership of the copy, the court determined that the employer's uses were noninfringing under Section 117 because it owned the copies in question, and thus was able to legally modify them. The court noted that the programs were developed for the employer's sole benefit, that they were stored on the employer's servers, that the plaintiff had not reserved the right to repossess them, and that the employer had the right to continue to possess and use the programs forever, or to discard or destroy the copies if it so desired.[91]

Critically, the court also held that Section 117 allowed individuals to customize and improve functionality of their copies of software programs, rather than merely adapt them to facilitate interoperability or repairs.[92] Looking to Section 117 's legislative history, the court found that Congress had envisioned that owners of copies should be permitted to "[add] features so that a program better serves the needs of the customer for which it was created."[93]

As a counterpoint to the informal title transfer in *Krause*, the Ninth Circuit considered how Section 117 applies in the context of purchasing a software program pursuant to a licensing agreement in *Vernor v. Autodesk, Inc.*[94] *Vernor* held that when an individual receives a copy of a copyrighted work pursuant to a written agreement, ownership is determined by considering both formal and informal factors, such as whether the agreement was formally labeled a license; whether the copyright owner retained title to the copy; whether the copyright owner required the copy's return or destruction; whether the copyright owner forbade duplication of the copy; and

[89] *Krause v. Titleserv, Inc*., 402 F.3d 119, 123 (2d Cir. 2005).
[90] *Id.* at 124.
[91] *Id*.
[92] *Id.* at 126.
[93] *Id*. at 128.
[94] 621 F.3d 1102 (9th Cir. 2010).

whether the copyright owner required the transferee to maintain possession of the copy throughout the duration of the agreement.[95]

Our investigation has revealed that some vehicle ECUs are transferred with the vehicle with no explicit agreements governing title to the copies of the ECU firmware. For instance, Tesla's Vehicle Purchase Agreement includes no mention of licensing software.[96] This scenario is analogous to *Krause*: while vehicle owners do not have explicit title in the ECU firmware, they do have indicia of ownership. When purchasing the vehicle, they possess a copy of the software inside, and they retain the ability to transfer and dispose of the software freely along with the vehicle. The manufacturer does not retain rights to repossess the copy.

On the other hand, our research shows that some copyright holders transfer specific ECUs within their vehicles accompanied by end user license agreements. For example:

- The OnStar car safety and navigation system is governed by a license agreement that provides:

  "You may only use the Application and Data as authorized in this EULA. Any use of the Application or Data in any manner not authorized under this EULA is prohibited. Prohibited use of the Application or Data includes, but is not limited to, the following: resale, transfer, modification or distribution of the Application or Data or copying or distribution of text, pictures, hyperlinks, displays and other content. You may not … (c) access the Application or Data or any Company proprietary information except through means authorized herein; (d) copy, reproduce, distribute, or in any manner duplicate the Application or Data, in whole or in part; … (f) modify, port, translate, or create derivative works if the Application; (g) decompile, disassemble, reverse engineer or otherwise attempt to derive, reconstruct, identify or discovery any source code, underlying ideas, or algorithms, of the Application by any means; …. You also agree to abide by and will not circumvent any security means or access control technology included in or with the Application. Further you may not use the Application or Data in a manner that … (c) attempts to introduce viruses or any other malicious computer code that interrupts, destroys or limits the functionality of any computer Application, hardware or telecommunications equipment[.]"[97]

- The license agreement for the Pioneer in-vehicle media software includes the following provision: "RESTRICTIONS ON USE. You may not, directly or

[95] *Id.* at 1108. *Krause* is consistent with judicial interpretations of Section 109, which has similar language to Section 117. In the context of Section 109, courts consistently look beyond the face of a formal agreement to its underlying characteristics to determine whether it is truly a license or a sale of a copy. See *UMG Recordings, Inc. v. Augusto*, 628 F.3d 1175, 1180 (9th Cir. 2011) (noting that Section 109 cases recognize that the "mere labeling of an arrangement as a license rather than a sale, although it was a factor to be considered, was not by itself dispositive" of ownership).

[96] *See* Motor Vehicle Purchase Agreement Terms & Conditions, Tesla (Oct. 4, 2013), *available at* https://my.teslamotors.com/order/download-order-agreement?country=US

[97] *OnStar End User License Agreement* (last accessed Feb. 5, 2015), *available at* https://www2.onstar.com/web/portal/eula?g=1.

indirectly: copy the Software, sub-license lend, lease or otherwise make the Software available to any third party (on the Internet or tangible media, by broadcast or in any other manner), use the Software commercially, modify, adapt or translate any part of the Software, reverse engineer, decompile or disassemble the Software or otherwise attempt to obtain its source code, bypass, modify, defeat, tamper with or circumvent any of the securities features of the Software, including altering any digital rights management functionality of the Software[.]"[98]

- The Ford Sync license agreement, which covers the media software, voice command system, and navigation system, says "You may not reverse engineer, decompile, or disassemble nor permit others to reverse engineer, decompile or disassemble the SOFTWARE, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation." The license agreement also applies to software updates.[99]

- The Toyota Safety Connect Terms and Conditions does not characterize itself as a license. However, the document says that a vehicle purchaser agrees "not to resell, copy, store, reproduce, distribute, modify, display, publish, transmit, broadcast, or create derivative works from any content you receive through your Service."[100]

- The Mercedes-Benz mbrace System is an Internet-enabled in-vehicle telematics, safety and personal assistance technology. The system has a Terms of Service providing, "[W]e own . . . [the] software and you do not acquire any rights in such software, including any right to use or modify the software other than the ordinary course of your receipt and use of the service."[101]

Despite the existence of these written terms, *Vernor* is distinguishable. The AutoCAD software in *Vernor* was highly transferrable and valuable to any architect, while ECU firmware is part and parcel of a vehicle has no use or utility other than for the purpose of operating the car. The car owner pays a hefty one-time fee for its use along with the vehicle, much like a sale of goods.

Moreover, the circumstances underlying a vehicle purchase are important. In a car-buying scenario, it may be impractical, if not impossible, to sit at the dealership and carefully review each document presented before signing a purchase agreement, and it is unclear whether car owners may return their vehicles for a full refund once they are actually able to understand the conditions

---

[98] PIONEER CORPORATION APPRADIOLIVE APPLICATION END-USER LICENSE AGREEMENT, (last accessed Feb. 5, 2015), *available at* http://www.pioneerappradiolive.com/eula/

[99] *Ford Sync End User License Agreement* (last accessed Feb 5, 2015), *available at* https://www.ford.com.au/servlet/Satellite?c=DFYArticle&cid=1249080829442&pagename=wrapper&site=FOA.

[100] *Terms and Conditions of Your Safety Connect Telematics Service*, Toyota, 4 (Oct. 20, 2010), *available at* http://www.toyota.com/safety-connect/img/safetyconnect-terms.pdf.

[101] *Mercedes-Benz mbrace Terms of Service* Mercedes Benz (May 3, 2012), *available at* http://mbrace.mbusa.com/static/pdf/mbrace_Terms_of_Service.pdf.

of their use.[102] The purchaser of a used vehicle may also not be presented with all of the documentation, including license terms, that were given to the original purchaser.

The totality of the circumstances surrounding the transfer of ECU firmware and "shrinkwrap" nature of the agreement make the transaction more like a sale of goods than a license.[103] The car owner manifests sufficient indicia of owning the firmware copy rather than merely licensing it, even if the EULAs at issue were held to be enforceable contracts.

2. Section 117(a)(1) Authorizes Users to Copy Vehicle Software for Use with Analytical Tools

Section 117(a)(1) grants the owner of a copy the right to make a copy or adapt a copy of a computer program provided "that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine, and that it is used in no other manner."

In *Vault*, the defendant designed software aimed at overcoming a protective measure in the original program; the court held that Section 117 protects the copying of the software expressly made for the purpose of defeating it, because the copy is created as an essential step to accomplishing that end.[104]

Making copies of vehicle firmware is an essential step in the process of reflashing or otherwise modifying ECUs. Although such a use is not essential to using the vehicle software for routine driving purposes, it is necessary for use in conjunction with a machine such as a commercial reflash tool or general-purpose computer on which the code will be analyzed for potential security and safety vulnerabilities.

Under *Krause*, a copy made for the express purpose of adding new features and capabilities that do not implicate a copyright holder's rights qualifies as an essential step for the purposes of Section 117 protection.[105]. The court approved the modifications and deemed them essential "not because they were necessary to make the software *work*, but because they were necessary to make the software *helpful* or worth using."[106]

3. Section 117(a)(2) Authorizes Users to Copy Vehicle Software for Archival Purposes

Section 117(a)(2) grants the owner of a copy the right to make a copy or adapt a copy of a computer program where "such a new copy or adaptation is for archival purposes only" and "all

---

[102] *See, e.g., ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1452-53 (7th Cir. 1996) (licensee was aware of the terms, and had the opportunity to read the license at his leisure); *Blizzard*, 629 F.3d at 935 ("WoW players "must read and accept Blizzard's EULA and Terms of Use on multiple occasions" and that "players who do not accept both the EULA and the ToU may return the game client for a refund.").
[103] *SoftMan Products Co., LLC v. Adobe Sys., Inc.*, 171 F. Supp. 2d 1075, 1085 (C.D. Cal. 2001).
[104] *Vault Corp. v. Quaid Software, Ltd.*, 847 F.2d 255, 261 (5th Cir. 1988).
[105] *See Krause v. Titleserv, Inc.,* 402 F.3d 119, 127 (2d Cir. 2005).
[106] *Softech Worldwide, LLC v. Internet Tech. Broad. Corp.,* 761 F. Supp. 2d 367, 373 & n.2 (E.D. Va. 2011) (emphasis in original) (describing *Krause*).

archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful."

This provision allows owners of copies of computer programs to authorize the creation of copies or adaptations on their behalf by third parties. The archival exception has been only rarely litigated, but according to one court, independent service organizations are entitled to make copies and adaptations on behalf of their customers, the owners of copies of the program.[107] This is an important consideration for car hobbyists who do not have the expertise to engage in firmware modification on their own, but still want to reap its benefits by customizing their vehicles.

Section 117(a)(2) also protects some of the research done by those engaging in copying or adaptation to test the security of vehicle firmware. The provision allows for the making of archival copies, provided that such copies are destroyed if their possession ceases to be rightful. Backup copies are important to establish a baseline if modifications are to be made, and to ensure that an ECU can be restored to its original state if it is compromised by experimentation.

Individuals may only avail themselves of this protection when they purchase a "destructible" or "damageable" copy of software that features a risk of damage beyond the dangers that would also apply to physical copies, such as "accidental shredding."[108] In practice, this has allowed for the making of copies to guard both against physical destruction, such as by mechanical or electric failure, as well as human mishap.[109] This provision could permit owners to back up copies of firmware before receiving a factory update, for instance, to review the changes made to the code and roll back to a prior version if desired.

6. Asserted Adverse Effects

A. The Ban on Circumvention Increases the Risk of Vehicle-Related Injury and Theft and Deprives Vehicle Purchasers of Crucial Information

The research contemplated in the proposed class provides a critical public service by identifying potential programming errors that compromise the security and safety of motor vehicles. This research improves user safety and provides essential information for vehicle purchasers to make informed decisions and hold manufacturers accountable, which is impossible without access to the software that runs the vehicle.[110] Researchers have demonstrated shortcomings in car networks' security,[111] prompting improvements by manufacturers.[112] But manufacturers do not always

[107] *Telecomm Tech. Servs., Inc. v. Siemens Rolm Comms., Inc.,* 66 F. Supp. 2d 1306, 1325 (N.D. Ga. 1998).
[108] *Micro-Sparc, Inc. v. Amtype Corp.,* 592 F. Supp. 33, 35 (D. Mass. 1984).
[109] *See Vault Corp. v. Quaid Software, Ltd.,* 847 F.2d 255, 261 (5th Cir. 1988), 847 F.2d at 264-66.
[110] Miller Statement at ¶ 3; Valasek Statement at ¶¶ 4, 7.
[111] Andy Greenberg, *Hackers Reveal Nasty New Car Attacks —With Me Behind The Wheel*, FORBES (Aug. 12, 2013, 9:00AM), *available at* http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video; *TODAY: Two experts demonstrate carjacking gone digital* (NBC television broadcast July 29, 2013) http://www.today.com/video/today/52609500#52609500; Jeremy Wagstaff, *Access to Tesla Cars Only a Password Away, Researcher Says* (Mar. 28, 2014), http://www.reuters.com/article/2014/03/28/tesla-motors-cybersecurity-idUSL1N0MP1OR20140328; Miller Statement at ¶ 4.

address proven vulnerabilities. In a pointed letter, United States Senator Ed Markey criticized Toyota and Ford for dismissing vulnerabilities found by DARPA-funded researchers rather than acting to fix them.[113]

In some cases, independent researchers have and developed technology to protect drivers from flaws left open by manufacturers.[114] Researchers also investigate ECU firmware for bugs that impact the safety of vehicles on the road, bugs that can affect airbags, lights, brakes, acceleration, and other critical vehicle functions.[115] Software flaws are common:[116] many high-profile recalls across a number of makes and models have been prompted by software issues[117], including an error in the software that controlled the anti-lock braking system of the 2010 Toyota Prius.[118] Enthusiasts discovered problems in a number of Toyota and Subaru cars that caused shuddering and stalling, after which the manufacturers developed an update.[119] On numerous other occasions, manufacturers have been required to issue recalls or software updates as a result of dangerous software errors, affecting millions of vehicles – in many cases prompted by reports from users.[120]

---

[112] Michael Leibel & Jim Finkle, *Chrysler, Nissan Looking Into Claims Their Cars 'Most Hackable,'* REUTERS (Aug. 5, 2014, 9:27PM), http://www.reuters.com/article/2014/08/06/us-cybersecurity-hackers-cars-idUSKBN0G603220140806.

[113] Edward J. Markey, *Letters to Automobile Manufacturers on Computer Security* (Dec. 2, 2013)*, representative letter available at* http://www.markey.senate.gov/documents/2013-12-2_GM.pdf.

[114] Jim Finkle, *Hacking Experts Build Device to Protect Cars from Cyber Attacks*, REUTERS (July 22, 2012, 5:15PM), http://www.reuters.com/article/2014/07/22/cybersecurity-autos-idUSL2N0PX2FH20140722.

[115] Michael Barr, *Bookout v. Toyota: 2005 Camry L4 Software Analysis,* 5 (last visited Feb. 5, 2015), http://www.sddt.com/files/BARR-SLIDES.pdf.

[116] *See Software Glitches in the Auto Industry and What that Means for You*, PSC PROSERVICES, http://proservicescorp.com/auto-industry-software-glitches (last visited Feb. 4, 2015).

[117] *See, e.g.,* Tom Robjornsen, *2012-2013 Mitsubishi Outlander Sport To Get Fix for Faulty ECU*, THE CAR CONNECTION (June 10, 2014), http://www.thecarconnection.com/news/1092546_2012-2013-mitsubishi-outlander-sport-to-get-fix-for-faulty-ecu; Vlad Savov, *Toyota Recalls Millions of Prius Hybrids to Fix Software Glitch*, THE VERGE (Feb. 12, 2014), http://www.theverge.com/2014/2/12/5403908/toyota-recalls-millions-of-prius-hybrids-to-fix-a-software-glitch; Brandon Turkus, *Mazda Recalling 88k Vehicles for ECU Glitch*, AUTOBLOG (Apr. 4, 2014), http://www.autoblog.com/2014/04/04/mazda-recalling-88k-vehicles-for-ecu-glitch; Jonathan Welsh, *Honda Recalls Nearly 260,000 Vehicles to Fix Electronics*, THE WALL STREET JOURNAL (Mar. 22, 2013, 1:20PM), http://blogs.wsj.com/drivers-seat/2013/03/22/honda-recalls-nearly-260000-vehicles-to-fix-electronics; *Jaguar Recalls 17,500 Cars Due to Software Glitch*, INFORMATION AGE (Oct. 25, 2011), http://www.information-age.com/technology/applications-and-development/1663983/jaguar-recalls-17500-cars-due-to-software-glitch.

[118] *Toyota Announces Voluntary Recall on 2010 Model-Year Prius and 2010 Lexus HS 250h Vehicles to Update ABS Software*, TOYOTA PRESSROOM (Feb. 08, 2010), http://pressroom.toyota.com/article_display.cfm?article_id=1868.

[119] Travis Okuliski, *Here's How To Fix The Scion FR-S and Subaru BRZ Engine's Idle Problem*, JALOPNIK (Oct. 2012), http://jalopnik.com/5948647/heres-how-to-fix-the-scion-fr-s-and-subaru-brz-engines-idle-problem.

[120] *See* Smith Statement at ¶ 8; Tom Robjornsen, *2012-2013 Mitsubishi Outlander Sport To Get Fix for Faulty ECU*, THE CAR CONNECTION (June 10, 2014), http://www.thecarconnection.com/news/1092546_2012-2013-mitsubishi-outlander-sport-to-get-fix-for-faulty-ecu; Vlad Savov *supra* n.116; Brandon Turkus, AUTOBLOG *supra* n.116; Jonathan Welsh, *supra* n.116*;* TOYOTA PRESSROOM *supra* n.117; Richard Read, *2014 Infinity Q50, Q70 Recalled for Software Glitch,* THE CAR CONNECTION (Nov. 4, 2014), http://www.thecarconnection.com/news/1095273_2014-infinity-q50-q70-recalled-for-software-glitch; *Jaguar Recalls 17,500 Cars Due to Software Glitch*, *supra* n.116; Richard Read, *2015 Volkswagen Jetta Recalled To Fix Headlight Software Glitch*, THE CAR CONNECTION (Dec. 30, 2014), http://www.thecarconnection.com/news/1096082_2015-volkswagen-jetta-recalled-to-fix-headlight-software-glitch; Ryan Beene, *Audi Recalls 102,000 A4 Cars in the U.S. Over Airbag Glitchglitch*, AUTOMOTIVE NEWS (Oct. 23, 2014), http://www.autonews.com/article/20141023/COPY01/310239941/audi-recalls-102000-a4-cars-in-u.s.-over-airbag-

In at least one case, a vehicle manufacturer was found liable for the death of a driver as a result of a software error. Toyota initially denied that there was a programming error, and only after independent researchers analyzed the software did they discover the programming oversights and flaws that made it possible for the vehicle to accelerate out of control.[121]

The increasing adoption of remote, wireless control systems also introduces new vulnerabilities.[122] An independent research and hobby group discovered a vulnerability in BMW's "Connected Drive" feature that allows an attacker to wirelessly unlock a car's doors.[123] The connection evidently was not using HTTPS encryption to secure the channel by which instructions could be issued, a serious oversight that was fixed when the independent researchers alerted BMW.[124] The independent researchers were located in Germany, and when their counterpart in the United States was interviewed for the story, he explicitly mentioned that "Because of laws like the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act, some researchers are hesitant to come forward with vulnerabilities lest they be accused of hacking and prosecuted."[125]

Despite the importance of public security and safety auditing, vehicle manufacturers have generally not made car firmware publicly available. Independent vehicle security and safety research has been limited by the practical effect of TPMs. For example, out of twenty-seven locked ECUs examined by experts Miller and Valasek, they could only successfully inspect the firmware on two.[126] The legal cloud hanging over vehicle security research has also chilled research and publication of research results.[127]

The net effects of the ban on circumvention are that fewer people are able to engage in essential research involving vehicle safety and security and publishing is chilled. Rather than robust systems tested and improved by interested parties, vehicle software is obscure and the public must rely on manufacturers for information about defects.[128] Manufacturers cannot be relied upon for information that they may have a litigation incentive to conceal in order to avoid liability, nor can they be relied upon to inform the public of software decisions that compromise user privacy and choice in favor of manufacturers' business models. Analysis by independent researchers would

---

glitch; Peter Valdes-Dapena, *Honda recalling 1.5 million cars*, CNN MONEY (Aug. 5,August 2011), http://money.cnn.com/2011/08/05/autos/honda_recall/; Colin Lecher, *GM Recalls Almost 34,000 Cars Because of Faulty Software*, POPULAR SCIENCE (Mar. 20,March 2013), http://www.popsci.com/cars/article/2013-03/gm-recalls-33700-cars-because-faulty-software.

[121] Michael Dunn, "Toyota's killer firmware: Bad design and its consequences," (October 28, 2013), *available at* http://www.edn.com/design/automotive/4423428/2/Toyota-s-killer-firmware--Bad-design-and-its-consequences; Barr, supra note 115.

[122] Valasek Statement at ¶ 6.

[123] *See* Martyn Williams, *BMW Cars Found Vulnerable in 'Connected Drive' Hack*, PCWORLD (Jan. 30, 2015) http://www.pcworld.com/article/2878437/bmw-cars-found-vulnerable-in-connected-drive-hack.html.

[124] *Id.*

[125] *Id.*

[126] *See* Charlie Miller and Chris Valasek, *Adventures in Automotive Networks and Control Units*, http://illmatics.com/car_hacking.pdf.

[127] *See* Miller Statement at ¶ 9; Smith Statement at ¶ 9; Ishtiaq Rouf et al., *Security and Privacy Vulnerabilities of InCar Wireless Networks: A Tire Pressure Monitoring System Case Study*, USENIX SECURITY 2010 12, http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf.

[128] Miller Statement at ¶ 3.

reveal bugs sooner, and the knowledge that vehicle code will be scrutinized will create a further incentive toward good practices on the part of manufacturers. The ban on circumvention should not stand in the way of research that could save lives.

B. The DMCA's Statutory Exemptions Are Too Narrow and Uncertain to Mitigate the Adverse Effects of the Ban on Circumvention

The adverse effects of 1201(a)(1) on vehicle security and safety research are not addressed by the statutory exemptions. The existing statutory exemptions to the circumvention ban are likely to apply only in a narrow subset of scenarios, as detailed below.

1. Section 1201(f) – Reverse Engineering

Section 1201(f)(1) provides a statutory exemption permitting circumvention when (1) one has lawfully obtained the right to use a copy of a computer program; (2) one acts "for the sole purpose" of identifying and analyzing elements necessary to achieve interoperability of an independently created computer program with other programs; (3) the elements of the program the user seeks to identify and analyze have not been readily available before; and (4) the acts of identification and analysis do not constitute infringement under copyright law.

Researchers who circumvent technological measures protecting their vehicle's firmware for purposes of studying the safety or security of the vehicle are acting within the bounds of interoperability because they are utilizing "the ability of computer programs to exchange information and of such programs mutually to use the information which has been exchanged." Section 1201(f)(4). This use would seem at first blush to fit within Section 1201(f).

However, researchers do not perform these activities for the sole purpose of interoperability, but also for the larger purpose of better understanding and enhancing public knowledge about the safety of vehicles. Under *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 320 (S.D.N.Y. 2000), such a use may not qualify for the reverse engineering exception. In that case, the court found that an individual's "sole" purpose in circumventing an access control was not to ensure interoperability when that individual was part of a group that viewed circumvention "as an end in itself and a means of demonstrating [the individual's] talent."

Moreover, a security researcher studying a vehicle may build on scholarship done by other researchers before them. Such activity would fail to satisfy the requirement that the elements the researcher is analyzing have not been analyzed before.

The questionable applicability of Section 1201(f) is further demonstrated by the history of this rulemaking. For instance, the Librarian determined in 2010 that cell phone owners jailbreaking technological measures protecting the firmware in their phones did not "fall within the four corners" of the Section 1201(f) statutory exemption.[129] However, the Librarian's decision folded the interoperability test into a fair use analysis, finding that the use was noninfringing because it

[129] Final Rule in RM 2008-8, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (July 27, 2010) ("2010 Rule") at 43829, available at http://www.copyright.gov/fedreg/2010/75fr43825.pdf.

allowed firmware compatibility with specifically created applications. But ruling on an identical petition less than three years later in the 2012 rulemaking, the Librarian said that it was "unclear, at best," whether Section 1201(f) applied.[130] When even the Copyright Office is unsure whether individuals can avail themselves of the Section 1201(f) statutory exemption, class members cannot conclude with any certainty that their activities are protected. This uncertainty adversely affects lawful and important research.

2. Section 1201(g) – Encryption Research

Section 1201(g)(2) permits the circumvention of a technological measure "as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research," where an individual satisfies four conditions: 1) the copy must have been lawfully obtained, 2) the act must be necessary to conduct such encryption research, 3) the person must make a good faith effort to obtain authorization before the circumvention, and 4) the act underlying the research must not constitute copyright infringement or a violation of other applicable law.

As an initial matter, the encryption research statutory exemption is too narrow to reach the full range of technological measures that may control access to ECU software. To be sure, one possible technological measure is encryption, which is used to restrict access to vehicle software and data compilations. However, security researchers are also likely to encounter challenge-response mechanisms and access ports on circuitry that don't involve encryption technology.[131] The encryption research exemption would not reach those technologies.

Moreover, a researcher may circumvent encryption in the course of bona fide security research without intending to perform encryption research *per se*. "Encryption research" is narrowly defined to mean "activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products." 17 U.S.C. § 1201(g)(1)(A). A researcher studying the overall security of ECUs may not examine encryption technologies at all.[132]

Furthermore, the encryption research exemption can apply only where a researcher makes "a good faith effort to obtain authorization before circumvention." 17 U.S.C. §1201(g)(1)(B). Even good-faith researchers rarely seek permission, for several reasons. The limited utility and complexity of this exception have contributed to a lack of awareness about its existence. Without specific knowledge of the law and detailed advice of counsel, a researcher who thinks permission is unlikely to be granted has every incentive not to ask for permission. Doing so increases the potential scrutiny they face from a rightsholder who may not be eager to see vulnerabilities

[130] Final Rule in RM 20011-7, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (October 26, 2012) ("2012 Rule") at 65264, *available at* http://copyright.gov/fedreg/2012/77fr65260.pdf.http://copyright.gov/fedreg/2012/77fr65260.pdf.

[131] The statutory exemption specifically defines "encryption technology" as "the scrambling and descrambling of information using mathematical formulas or algorithms." Section 1201(g)(1)(B).

[132] Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World* 102 (2000) ("Cryptography is a branch of mathematics. Mathematics is theoretical; mathematics is logical . . . . Security is rooted in the physical world.").

exposed. Given the counter-intuitive and complex landmine of Section 1201, researchers are often hesitant to invite hostile scrutiny. It is also inconsistent with the culture of academic freedom and consumer protection to ask permission before studying a product that is already operating in the real world; it may never occur to researchers that they should ask, especially if they intend to proceed even if permission is denied. Finally, researchers may find that their access to a manufacturer's products is diminished if they explain that their goal is to find flaws in them.

In scenarios where the encryption research exemption may plausibly come into play, the statute provides a list of factors for courts to weigh in considering whether the exemption should apply. The first factor is whether the information learned from the research is disseminated, and if so, whether it is disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, or in a manner that facilitates infringement or violation of applicable law. 17 U.S.C. §1201(g)(3)(A). The second factor looks to the person undertaking the encryption research and asks whether they are engaged in a legitimate course of study, are employed, or are trained or experienced in the field. 17 U.S.C. §1201(g)(3)(B). The third factor considers whether the researcher provides the copyright owner with notice of the findings and documentation of the research and the timeliness of any notice. 17 U.S.C. §1201(g)(3)(C).

The researchers who seek to use the proposed class are accessing ECUs for the purpose of determining whether flaws make the computers work in unanticipated ways or render them vulnerable to attack. These researchers tend to widely disseminate their results by publishing them and speaking at conferences. The researchers are often trained, experienced, and well respected in the field, or aspire to become so. They may or may not provide the copyright owner with notice of their findings, depending on whether they think the copyright owner will react receptively or negatively. Thus, these factors may not produce a clear, decisive result.

Without the proposed exemption, the legal cloud of 1201 will continue to limit the public benefits that could be gained through more effective encryption research.

3. Section 1201(j) – Security Testing

Section 1201(j) provides a statutory exemption for "security testing," which is defined as "accessing a computer, computer system, or computer network solely for the purpose of good faith testing, investigating, or correcting a security flaw of vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network." Section 1201(j)(1). Like the other exemptions, the conduct must not constitute copyright infringement or a violation of other applicable law.

Like Section 1201(g), Section 1201(j) lists factors that should be considered when determining whether one qualifies for the exception. First, it asks whether the information learned from the security testing is "used solely to promote the security of the owner or operator of the computer, system, or network, or whether it is shared directly with the developer." 17 U.S.C. §1201(j)(3)(A). Second, it asks whether the information learned from the testing is "used or maintained in a manner that does not facilitate infringement or a violation of applicable law, including a violation of privacy or breach of security." 17 U.S.C. §1201(j)(3)(B).

Because technological measures other than encryption protect vehicle firmware and update files, individuals seeking to circumvent those measures for the purpose of security research would likely have to avail themselves of the security testing exception to ensure that their conduct is protected.

However, the information derived from the testing is often published to advance the state of knowledge for all, not used solely to promote the security of the owner or operator of the vehicle. Further, independent security researchers sometimes locate vulnerabilities that involve not just the computer system on the vehicle, but a broader network,[133] which may call into question whether the vehicle owner's permission is sufficient for such research to fall within the scope of the statutory exemption.

Over the past decade of rulemaking proceedings, the Librarian has recognized the lack of clarity around 1201(j). In 2006, the Librarian granted a security testing exemption for research on DRM software on CDs;[134] in 2010, an essentially identical exemption was granted allowing for security testing of video games.[135] In the process of granting these exemptions, the Librarian acknowledged that the applicability of Section 1201(j) was an open question. In 2006, the Librarian wrote that the exception "*may* permit circumvention [but] . . . it is not clear whether that provision extends to such conduct."[136] In 2010, the Librarian wrote "it is unclear whether Section 1201(j) applies in cases where the person engaging in security testing is not seeking to gain access to, in the words of Section 1201(j), 'a computer, computer system, or computer network.'"[137]

This uncertainty extends to vehicle researchers, and discourages independent research, especially among individuals without the resources and institutional support to face a circumvention lawsuit. This is a substantial adverse impact that necessitates an exemption.

Congress, acting in 1998, did not foresee the ways in which important security research that does not fit within the narrow confines of the statutory exemptions would be stymied by Section 1201(a) over the past sixteen years. It was for precisely this reason that Congress empowered the Librarian to grant additional exemptions.

7. Statutory Factors

A. The Availability For Use of Copyrighted Works

Availability of copyrighted works will be improved by the proposed exemption. As described above, technical measures currently restrict the availability of vehicle firmware for a variety of lawful uses. There will be no adverse effect on the availability of copyrighted works, since code is

[133] *See,* E.g., Martyn Williams, *BMW Cars Found Vulnerable in 'Connected Drive' Hack*, PCWORLD (Jan. 30, 2015) http://www.pcworld.com/article/2878437/bmw-cars-found-vulnerable-in-connected-drive-hack.html.
[134] Final Rule in RM 2005-11, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Nov. 27, 2006) ("2006 Rule") at 68477, *available at* http://www.copyright.gov/fedreg/2006/71fr68472.pdf.
[135] Final Rule in RM 2008-8, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (July 27, 2010) ("2010 Rule") at 43832, *available at* http://www.copyright.gov/fedreg/2010/75fr43825.pdf.
[136] 2006 Rule at 68477.
[137] 2010 Rule at 43833.

necessary for vehicles to function and is produced for non-copyright-related reasons, and because no market harm cognizable by copyright law will result from the proposed exemption. To the contrary, additional copyrighted works will be made available that rely on the non-copyrightable information made accessible via the proposed exemption. Craig Smith, author of the *2014 Car Hacker's Handbook*, reported that the *Handbook* was downloaded 300,000 times in the first two weeks it was available.[138] Software patches also depend on access, including patches to fix serious vulnerabilities.[139] Numerous tools designed to analyze and manipulate firmware also depend on the ability to access software and reverse engineer it.[140] The availability of copyrighted works will be promoted by the proposed exemption. Moreover, there is no reasonable alternative to the circumvention that is necessary to investigate and improve the security of many vehicles.

B. The Availability For Use of Works for Nonprofit Archival, Preservation, and Educational Purposes

Education about vehicle security and safety will benefit from increased knowledge of vehicle firmware to use as real-world examples in teaching.[141] In addition, it will be possible to archive and preserve firmware on general-purpose storage media, without expensive and unreliable storage of ECU hardware removed from a vehicle.

C. The Impact That the Prohibition on the Circumvention of Technological Measures Applied to Copyrighted Works Has on Criticism, Comment, News Reporting, Teaching, Scholarship, or Research

As discussed above, the prohibition on circumvention curtails speech in all of the categories identified in the third statutory factor. The legal cloud resulting from the prohibition on circumvention reduces participation in research, scholarship and teaching on vehicle security and safety, as well as critiquing, commenting, and reporting on vulnerabilities and safety issues.

D. The Effect of Circumvention of Technological Measures on the Market for or Value of Copyrighted Works

As discussed above, the market for vehicle firmware will not suffer any harm cognizable under copyright law.

E. Other Factors That May Be Appropriate for the Librarian to Consider in Evaluating the Proposed Exemption

1. *With respect to the proposed uses, (a) the extent to which any of the asserted noninfringing activities merely requires examination or changing of variables or codes relied upon by the vehicle software, or instead requires copying or rewriting of the vehicle software, and (b) whether vehicle owners can properly be considered "owners" of the vehicle software.*

[138] Smith Statement at ¶ 3.
[139] Miller Statement at ¶ 7.
[140] Blundell Statement at ¶ 5.
[141] Miller Statement at ¶¶ 2, 6; Smith Statement at ¶ 9; Valasek Statement at ¶¶ 2, 7, 8.

With respect to part (a), it is impossible to tell merely from variables or codes (such as diagnostic codes) whether security or safety vulnerabilities exist in a vehicle's firmware.[142] Errors can arise at multiple layers in the ECU system, specifically a bug in the software, a gap in the safety features, or a design that does not adequately protect against routine glitches in the electronics.[143] As for part (b), the answer depends on the vehicle manufacturer and the ECU in question, as discussed above in the context of Section 117. The Librarian should grant an exemption that does not depend on a vehicle owner's status as owner or licensee of the firmware running on the vehicle.

2. Whether granting the exemption could have negative repercussions with respect to the safety or security of vehicles, for example, by making it easier for wrongdoers to access a vehicle's software.

As discussed above in the context of the first fair use factor, the consensus among security researchers and the advice of the government agency responsible for security standards is that security comes from visibility and widespread testing and challenging of systems, not from concealing vulnerabilities or preventing widespread access.[144] Perpetuating the legal uncertainty that overhangs security research will only deter researchers with legitimate interests in studying and improving vehicle safety, prolonging the period in which "every system" researchers evaluate contains massive security vulnerabilities.[145] Secrecy creates unnecessary risk, because "the actors willing to pay for cracking an algorithm are not always academic or public-minded, and may be unlikely to share their findings with the consumer."[146] Bad actors seeking to harm persons or property in violation of criminal law are unlikely to be deterred by the legal ban on circumvention.

3. The applicability (or not) of the statutory exemptions for reverse engineering in 17 U.S.C. 1201(f) and encryption research in 17 U.S.C. 1201(g) to the proposed uses.

This question is addressed at length above, under Item 6.

4. Whether a third party – rather than the owner of the vehicle – may lawfully offer or engage in the proposed circumvention activities with respect to that vehicle pursuant to an exemption granted under 17 U.S.C. 1201(a)(1).

Yes, the exemption should permit circumvention done with the permission of the owner of a vehicle by a third party. Many individuals do not possess the resources to circumvent on their own, and the rulemaking cannot authorize the distribution of the means of circumvention, so third parties must be able to circumvent with permission of vehicle owners for the exemption to reach the majority of its beneficiaries.

To the extent the Register is concerned that such activities would be barred by Section 1201(a)(2), the answer is that vehicle security and safety research will be lawful under that section because

[142] *See* Illera & Vidall *supra* at 74-80; Miller Statement at ¶ 8; Valasek Statement at ¶ 3.
[143] *See* Barr, *supra* note115.
[144] Valasek Statement at ¶ 2.
[145] Miller Statement at ¶ 4; *see* Koscher et al., *supra* note 3.
[146] Smith Statement at ¶ 8.

they do not fall under any of the three categories of forbidden conduct identified in 1201(a)(2)(A) through (C).

If an expert asks to borrow your vehicle to analyze it for security and safety vulnerabilities, for example, they are not offering a service barred by 1201(a)(2), even if they engage in circumvention as part of their research. To the extent this constitutes offering a service at all, it bears no resemblance to the "black boxes that are expressly intended to facilitate circumvention" Congress sought to outlaw, nor does it fall within the language of the statutory prohibition.

Security and safety research is not "primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access" to a copyrighted work. 17 U.S.C. § 1201(a)(2)(A). Rather, it is conducted for a variety of socially beneficial purposes identified above. Such research also does not have "only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access" to a copyrighted work. 17 U.S.C. § 1201(a)(2)(B). This provision presupposes that the service or device at issue has commercial significance for circumvention, and seems not to contemplate the intrinsic or public-minded motivations of researchers. Finally, such research is not "marketed . . . for use in circumventing a technological measure that effectively controls access" to a copyrighted work. 17 U.S.C. § 1201(a)(2)(C). Again, the statutory language is clearly a poor fit for the research inquiry at issue in the proposed class, the objective of which is to add to collective knowledge about vehicular function and improve the safety and security of those who rely upon vehicles.

Extending an exemption for use by third parties with the permission of the vehicle owner would be consistent with Congress's directive in the Unlocking Consumer Choice and Wireless Competition Act. With respect to the unlocking of mobile computing devices, Congress recognized that to be most effective in alleviating negative effects of Section 1201(a), permission to circumvent should be granted to "another person at the direction of the owner, or by a provider [of cellular service] at the direction of such owner or other person."[147] The same considerations apply to vehicle security.

[147] S. 117 113th Cong, (2014) (as enacted).

Appendix A

Statement of David Blundell
Automotive Enthusiast

February 6, 2015

1. My name is David Blundell. I do tech support, teach classes and design new products for a small company that makes devices for reprograming factory engine computers, mostly those made prior to 1996.[1] I started and ran one of the first open-source, community oriented internet sites focused on reverse-engineering vehicle firmware for the purpose of enabling enthusiasts to modify their vehicles, pgmfi.org. I've also been active with the OpenGarages project since its start. I calibrate vehicles as part of my occupation and I also teach classes to help people learn how to modify their car's engine computer systems for performance modifications. Through my work and teaching, I help hundreds (if not thousands) of enthusiasts a month find the tools they need to control the digital side of their vehicles and learn how to effectively modify their engine controllers.

2. In past years, I've developed commercial hardware and software to work with OEM engine computers, which make it possible for people to adjust their computer's operation to suit modifications to the car. I have also used many tools developed by others for calibrating original equipment manufacturer engine computers. Having done the ground-level reverse engineering work myself in the past, I know how much reverse engineering went into these tools.

3. I have been modifying cars for approximately 14 years. About 12 years ago, I took my first step into the field of ECU modification when I reverse engineered my car's engine computer firmware while adding a turbocharger and changing fuel injectors to make the car go faster. Had I not reverse engineered the firmware running my vehicle's engine computer, those modifications would not have been possible.

4. Here are a few other examples of modifications I've made to cars that required me to reprogram a factory engine computer:

- 2008 Chevy Silverado. After I installed a different rear axle gear in this truck to improve its ability to tow heavy loads, the computers needed to be modified to accommodate the new part. The speedometer was off by the change in gear ratio, the transmission was shifting at inappropriate times (too late), and the anti-lock braking system was inoperable. The engine computer needed to be reprogrammed to make the speedometer read correctly, and the transmission controller needed to be reprogrammed to make the truck shift appropriately. After proper calibration, the speedometer worked properly, the transmission shifted at appropriate times, and the anti-lock brakes functioned again.

[1] I am making this statement in my personal capacity, not on behalf of my employer.

- 1996 Nissan 240. I reprogrammed the factory computer to match a newly installed engine and transmission. Before the reprogramming, the car needed to be towed because it barely ran. After reprogramming to match the new engine, the car ran as though it had originally come from the factory with the new part.

- 1995 Honda Civic. As an alternative to junking this car, I reprogrammed the factory computer to allow a 2000 CRV engine and transmission to replace the blown-up original engine. This vehicle has driven almost 60,000 miles since the motor was replaced instead of ending up in a junkyard.

- 2005 Chevrolet Avalanche. I reprogrammed the factory computer for better fuel mileage by adjusting when the transmission shifted and basic engine operation in terms of fuel and spark. These changes improved fuel economy from 15.4 mpg to 18.5 mpg average while maintaining Louisiana emissions testing compliance.

- 2005 Ford F350. When switching from summer to winter tires, I reprogrammed the engine and transmission computers to account for the change in tire size to ensure speedometer accuracy and appropriate transmission gear shifting.

- I reprogrammed computers from several modern cars allowing complete modern drivetrains to be used in older vehicles such as a 1929 Ford, 1954 Ford, and 1954 Chevy. In each case, the factory engine computers were reprogrammed to behave without many of the sensors and systems originally present in the donor vehicle.

5. Before any of the modifications I have described could be performed, the firmware of each of these controllers had to be read in its entirety and meticulously analyzed. Each firmware image was disassembled and then analyzed to discern the logic used and parameters available to change. Without a full copy of the firmware, it's virtually impossible to properly understand the behavior of an ECU well enough to get predictable results from modifying parameters. In each of the examples above, the tools created as a result of this firmware analysis were used to interface with the engine controller by sending commands that the engine firmware will recognize and respond to in order to achieve the desired result. This would not have been possible without first reverse engineering the firmware in order to understand how to make tools to interact with it.

6. Moreover, to replace any modern vehicle computer that fails, it is necessary to reprogram (or disable) the anti-theft system. This process requires an understanding of how the anti-theft system works on a digital level, something only likely to have been done by reverse-engineering the factory firmware or paying for the information from the manufacturer. Installing a replacement engine in a vehicle typically requires tweaks to anti-theft system (and often additional measures if the new engine's computer is swapped along with the engine itself). Without being able to access the firmware and make these changes, consumers are limited to using engines that are exactly the same as the one they are replacing. It isn't possible to upgrade to newer, more fuel-efficient models or newer engines that have fewer miles but incompatible electronics.

7. In the course of my reverse-engineering work, I have encountered several access control mechanisms that needed to be side-stepped in order for me to access and modify ECU firmware. First, it is very common (almost universal) for microcontrollers to have security bits set that prevent readout using JTAG or other standardized programming methods. In every single case where it was critical to read internal MCU memory, I found that some glitching method (voltage manipulation, clock manipulation, startup state manipulation, manipulation of memory control pins) successfully revealed the code. Second, many ECUs employ a seed/key arrangement to prevent casual reprogramming. In many cases, these measures can be attacked by physically opening the case of the ECU, desoldering memory chips and reading them. Where there is a strong enough will to get access to firmware, there will be a way to do so. The only question is how much work will be involved and how expensive it will be to do so.

8. America loses racing, one of its great pastimes, if consumers aren't able to modify their vehicles because of limitations imposed by engine computers. For many vehicles, there is no option other than reprogramming the factory computers as no aftermarket computers are available which are compatible. I personally know dozens of people in the U.S. who make their living by reverse engineering car computer firmware. Hundreds if not thousands of workers are employed in the U.S. by companies that produce tools derived from reverse engineering car computers (SCT, Diablosport, Bullydog, and Hondata, to name a few). Thousands more make their living using tools derived from reverse engineering car computers to service the needs of consumers.[2] Thousands more are employed by companies whose products rely on tools for reprogramming vehicles.[3] These are all companies selling millions of dollars a year worth of products to the racing community.

9. Racing is a huge deal both economically and culturally. According to the Performance Racing Industry (PRI), which is owned by the Specialty Equipment Marketing Association (SEMA), around $19 billion is spent in the racing industry annually worldwide, and much of that spending is in the USA.[4] Moreover, "451,000 people compete each year in auto races held at

---

[2] For instance, Facebook has many groups and pages devoted to automotive modification. *See*, *e.g.*, Guild of EFI Tuners (464 members), https://www.facebook.com/groups/737420992943719; EFI Live Users (2,513 members), https://www.facebook.com/groups/291322157655351; EFI Live Diesel Tuning Support (4,150 likes), https://www.facebook.com/EFILiveDiesel; EFI University (3,460 likes), https://www.facebook.com/EFI101; COBB Tuning (company that makes tuning hardware) (205,217 likes), https://www.facebook.com/cobbtuning; Hondata (company that makes tuning hardware) (38.347 likes), https://www.facebook.com/pages/Hondata/108772022480315; SCT (company that makes tuning hardware) (53,181 likes), https://www.facebook.com/scttuning; DiabloSport (company that makes tuning hardware) (67,625 likes), https://www.facebook.com/DiabloSport (all pages last visited on Feb. 3, 2015).

[3] Companies you may have heard of even if you're not involved with racing are Ford Racing (www.fordracingparts.com), Edelbrock (www.edelbrock.com), GM Performance Parts (http://www.chevrolet.com/performance.html), Roush (www.roush.com), Procharger (www.procharger.com), Vortech (www.vortech.com), and Holley (www.holley.com).

[4] See Performance Racing Industry, *Market Demographics*, http://www.performanceracing.com/magazine/index/demographics.html (last visited Feb. 3, 2015).

over 1,300 race tracks across the United States," and about 48,000 professionals and 1,200 companies attended the annual PRI trade show organized by SEMA.[5] With cars becoming increasingly computerized, racing depends more and more on people having access to their cars' computers. Additionally, I hope the examples of some of the work I have done with engine computers illustrate that many outside the racing community rely on tools derived from reverse engineering car firmware to make vehicles operate properly after modifications as simple as tires and gears. A DMCA exemption would benefit countless individuals and companies by enabling cars to continue to be modified for racing and repair without fear of this law.

[5] Performance Racing Industry, *Company Profile*, http://www.performanceracing.com/tradeshow/about_us/company_profile.html (last visited Feb. 3, 2015).

Appendix B

Statement of Charlie Miller, PhD
Independent Security Researcher

February 6, 2015

1. My name is Charlie Miller.[1] I am currently a security engineer at Twitter. Previously, I was employed as a computer security consultant for seven years. Before that I worked for the National Security Agency as a computer security analyst for five years. I have a PhD from the University of Notre Dame and am a well-known computer security researcher, having spoken around the world at various information security conferences. In the past I have identified and reported vulnerabilities in many products such as mobile phones, web browsers, word processors, and even video games. I have also co-authored several books in the field of information security, including *Fuzzing for Software Security Testing and Quality Assurance*, *The iOS Hacker's Handbook*, and *The Mac Hacker's Handbook*.

2. For the past few years, along with my research associate Chris Valasek, I have been investigating the susceptibility of automobiles to be attacked by hackers. I have co-authored several papers about this topic[2] and reported my findings to automotive manufacturers, computer security conferences, as well as trade organizations such as the Society for Automotive Engineers.

3. I feel this research is especially important because vulnerabilities in the computer networks of vehicles can lead to physical harm to their users. Previous research has shown that it is possible to remotely compromise a vehicle over cellular or bluetooth communications and physically affect the vehicle such as locking up the brakes.[3] Chris and I showed that in some circumstances, it is possible on newer vehicles to not only control the brakes, but sometimes an attacker can take control over the steering and even the acceleration of some vehicles. These findings are all very scary and critically important, which is why I am currently performing research in this field.

---

[1] I am making this statement in my personal capacity, not on behalf of my employer.

[2] *See*, *e.g.*, Charlie Miller & Chris Valasek, *Adventures in Automotive Networks and Control Units*, http://illmatics.com/car_hacking.pdf (last visited Feb. 2, 2015); Charlie Miller & Chris Valasek, *A Survey of Remote Automotive Attack Surfaces,* http://illmatics.com/remote%20attack%20surfaces.pdf (last visited Feb. 2, 2015); Charlie Miller & Chris Valasek, *Car Hacking for Poories*, http://illmatics.com/car_hacking_poories.pdf (last visited Feb. 2, 2015).

[3] Karl Koscher et al., *Experimental Security Analysis of a Modern Automobile*, CENTER FOR AUTOMOTIVE EMBEDDED SYSTEMS Security (May 16, 2010), http://www.autosec.org/pubs/cars-oakland2010.pdf; Stephen Checkoway et al., *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, http://www.autosec.org/pubs/cars-usenixsec2011.pdf (last visited Feb. 2, 2015).

4. Car manufacturers reassure the public that they take these attacks on automotive systems very seriously and that their vehicles are safe.[4] Yet they do not specifically describe what protections they build in or how they address these threats. It is notable that every system I have looked at *has been vulnerable to some type of serious attack*. For this reason, it is critical that researchers and consumers be allowed to investigate and better understand the security of vehicles and their resilience to these types of attacks.

5. In order to perform automotive security research of this kind, it is necessary to extract and examine the code (firmware) that runs on the computers that control aspects of the vehicle. These small embedded systems are commonly referred to as electronic control units (ECUs).

6. In the past, we have extracted the firmware from ECUs in a few different ways. In one case, we physically attached a hardware debugger to a processor on the chip and downloaded it that way. In other cases, we've been able to remotely extract portions of the firmware over the CAN network, using diagnostic commands. This type of access is typically protected by a challenge-response mechanism (see below) that we needed to circumvent. In the past, we were able to circumvent this mechanism by reverse engineering the tools that automotive dealers use to repair vehicles. With the firmware, you could also extract the keys for the challenge response in order to test other features requiring authentication with the device. Another way to extract firmware, which is an approach we are taking in our most recent research, is to extract firmware from the USB updates provided to vehicle owners from manufacturers. The firmware on the USB can only be loaded onto the ECU if a cryptographic checksum is valid. In a talk I gave at Blackhat USA this year, I discussed in one case how to circumvent this checksum and install arbitrary firmware from a USB stick.

7. There are a few reasons that having the firmware is necessary for our analysis. First, the firmware details exactly how the ECU reacts to inputs and reveals any safety mechanisms in place in the ECUs. While we can often infer these properties by observing the ECU, the definitive source of information is the ECU itself. Another reason why having the firmware is necessary is that we are specifically looking for vulnerabilities in the firmware that would allow a remote attacker to take control of the ECU and make it affect the safety of the entire automotive system. The best way to do this is to statically analyze the firmware looking for coding flaws and vulnerabilities. Without the firmware, it is almost impossible to find vulnerabilities in the ECUs. The final reason why having the firmware is necessary is that a large part of our research centers around whether the firmware can be modified remotely by an attacker. Having the firmware allows us to not only know whether this is possible (through a vulnerability or intentional feature) but also illustrates on how to modify the firmware. Without knowing the details of how the firmware is constructed and how it is comprised, we would not be able to construct patches or modifications to make to the ECUs.

---

[4] *See*, *i.e.*, Andy Greenberg, *Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel*, FORBES (July 24, 2013), http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video ("A Ford spokesman says the company takes hackers 'very seriously,' but Toyota, for its part, says it isn't impressed by Miller and Valasek's [research] . . . 'We believe our systems are safe and secure.'")

8. As a security professional, I examine and test the security of the vehicle myself, responsibly report any issues identified, and verify fixes for the issues are delivered. This is not possible without having access to the code running on the computers in the vehicle.

9. I live in constant fear that the DMCA will be used as a tool by the manufacturers to stop this safety critical research from continuing. I worry that in an effort to stop bad publicity and prevent their customers from getting scared, they will leverage the DMCA against us and the effect will be that everyone's vehicle will be less safe.

Appendix C

Statement of Craig Smith
CEO of Theia Labs and Founder of Open Garages

February 6, 2015

1. My name is Craig Smith. I am CEO of Theia Labs, an information security research and consulting firm focusing on reverse engineering, product development, and design.[1]

2. I am also Founder of Open Garages, a network of hobbyists and mechanics across the country who research, modify (or "mod") and explore the increasingly complex systems inside modern cars. Open Garages provides access, documentation, and tools to help people better understand and customize their vehicles. My particular interest is reverse engineering to better understand the security implications of the computer systems inside cars. Others in the Open Garages community customize their cars for artistic, mechanical, or performance reasons.[2]

3. I am also the author of the *2014 Car Hacker's Handbook*, which is a manual that teaches people interested in automotive research about the complicated infrastructure under the hoods of their cars and how to analyze the computer systems inside their vehicles.[3] The handbook was downloaded from my website 300,000 times within the first two weeks after publication alone. A new, more detailed version is slated for release mid-year.

4. As long as automobiles have existed, there has been a long tradition in this country of car owners tinkering with their cars. In recent years, however, vehicles have become almost entirely controlled by electronic devices.

5. With the new electronics came proprietary codes and security access passwords. These barriers present a threat to reverse engineers.

6. In my research I have encountered secure boot loader mechanisms that prevent debugging and modification of code on the systems. When I encountered these types of protections, it was necessary for me to reverse-engineer the installation process to determine the methods used to lock out third-party modifications.

7. The International Organization for Standardization has published an open international standard for Unified Diagnostic Services (UDS), but unfortunately only a few of these signals

[1] Theia Labs, http://www.theialabs.com (last visited Jan. 7, 2015).
[2] Open Garages Wiki, http://opengarages.org/index.php/Main_Page (last modified July 15, 2014).
[3] See http://www.amazon.com/2014-Hackers-Manual-Craig-Smith-ebook/dp/B00LIAVJFG/ (last visited Jan. 7, 2015).

are public.[4] The rest are proprietary and used by the manufacturers and dealers. In order to determine what these proprietary signals are, the firmware of the ECU or other components would need to be reverse engineered.

8. Sometimes, bypassing these checks is not enough to access the code, and additional action would be necessary to access the signals. One example is the DST40 algorithm produced by Texas Instruments, which is used in immobilizer systems, among other applications. The DST40 was determined to be crackable after a research team deciphered their "secret" algorithm.[5] (The "40" in DST40 apparently stands for the 40-bit key size.) The solution from Texas Instruments was not to open the algorithm to peer review or to use a public-tested algorithm, but instead to create a new proprietary algorithm: DST80. (It is assumed that Texas Instruments simply increased the key size to 80 bits.) This is an unfortunate approach to security: it increases the time and cost necessary to do valid research. Moreover, the actors willing to pay for cracking an algorithm are not always academic or public-minded, and may be unlikely to share their findings with the consumer.

9. My goal is to build a robust community of researchers, hobbyists, and mechanics who are free to share expertise and information about the communication protocols used in vehicles and the diagnostic signals used by manufacturers for testing and wiring diagrams. However, I worry that somebody who makes a business of selling this information will use the DMCA in an attempt to prevent us from doing so, which will have a chilling effect on our community effort.

[4] ISO 14229-1:2013, http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=55283 (last visited Feb. 2, 2015).

[5] Stephen C. Bono et al., Security Analysis of a Cryptographically-Enabled RFID Device, 14th USENIX Security Symposium, https://www.usenix.org/legacy/events/sec05/tech/bono/bono.pdf (last visited Feb. 2, 2015).

Appendix D

Statement of Chris Valasek
Director of Vehicle Security Research, IOActive

February 6, 2015

1. My name is Chris Valasek, and I'm the Director of Vehicle Security Research at the information security firm IOActive (htttp://www.ioactive.com).[1] I've worked in the computer security field for several years and have spent most of my career studying reverse engineering and exploitation research.

2. Over the past three years, Dr. Charlie Miller and I have partnered to focus our research efforts on automotive cyber security. Our research has covered everything from vehicle network architecture, to control of cyber physical automotive systems, to reverse engineering of diagnostic software and vehicle computer controls. The results of our research have been made available to the public in attempt to raise awareness for vehicle cybersecurity in hopes that fellow colleagues would also pursue research in the automotive arena.[2]

3. In the course of our research Dr. Miller and I had to overcome several barriers to continue our research. Many times, individual vehicle computer controls needed to be put into a special mode before certain testing or firmware writing could occur. We were required to reverse engineering maintenance software in order to assess the security and physical abilities of individual computers within a vehicle. Many times, the process of putting the computer in a privileged mode was not enough and a standalone firmware update needed to be acquired from the manufacturer's website. We felt it vital to assess the maintenance and ECU firmware to assess the security of the vehicle because an attacker would need to perform the same functions in order to compromise your car.

4. During our research Dr. Miller and myself have found that several methods for analyzing a vehicle's functionality may depend on having the proper security access challenge/response keys. Sometimes the only option to validate the functionality was to identify the algorithms responsible for restricted access and active testing in the firmware.

5. Dr. Miller and I both believe independent researchers must be able to fully analyze threats to the modern computerized vehicle for safety reasons. Poor security in a car could result in bodily harm to the driver, passengers, or bystanders—and this danger is not hypothetical. We have shown that given proper time, skill, and budget, an attacker can take control of critical attributes of a vehicle, such as steering, braking, and acceleration.

---

[1] I am making this statement in my personal capacity, not on behalf of IOActive.
[2] See, for example, Charlie Miller and Chris Valasek, *Adventures in Automotive Networks and Control Units*, http://illmatics.com/car_hacking.pdf.

6. Additionally, the modern vehicle now contains an unprecedented amount of technology that communicates with the outside world, such as Bluetooth for your phone, cellular modems for telematics systems, and even in-car Wi-Fi. These technological features are a major factor in the purchase of a vehicle as consumers desire a more connected life. But additional contact with the outside world also comes with added attack surface. While physical control of the automobile depends on several different factors, any piece of technology that accepts input from the outside is a potential entry point for someone with malicious intent.

7. Using software to diagnose and interact with the vehicle is a major part of automotive research, since proprietary information is commonplace in the automotive space. These diagnostic tools are integral to understanding the functionality and security of every vehicle on the road. The tools are required to perform certain actions, such as vehicle computer reprogramming. Researchers need to understand these tools and their underlying protocols to properly assess a vehicle from a security perspective.

8. Consumers have a right to know exactly what potential risks are associated with the technology used in today's vehicle. Dr. Miller and I pursue our research to educate the public and automotive industry about these risks and how to mitigate them. Our goal is to advance the state of knowledge in this field in hopes of making it harder for malicious actors to attack vehicles in the future.