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 21: Vehicle Software—Diagnosis, Repair, or Modification

This proposed class would allow circumvention of TPMs protecting computer programs,[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,] that control the functioning of a motorized land vehicle, including personal automobiles, commercial motor vehicles, and agricultural machinery, for purposes of lawful diagnosis and repair, or aftermarket personalization, modification, or other improvement. 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 firmware updates and proprietary repair software, raises the same concerns,[1] is often encrypted (requiring circumvention), and analyzing an update is often necessary to gain access to already-embedded software.[2]

It has also come to EFF's attention that manufacturers are claiming copyright over compilations of non-copyrightable information (which could include parts specifications or diagnostic codes).[3] Ford recently sued an independent diagnostic company for violation of 1201(a)(1), alleging that defeating the encryption on such a compilation was unlawful circumvention.[4] Such data, including diagnostic codes, can be obtained by reverse-engineering vehicle software,[5] but direct decryption would be far more straightforward. Thus, compilations of data relating to parts specifications or diagnostic codes should be included in the proposed class. As discussed below, such compilations implicate many of the same concerns as embedded software, software updates, and software diagnostic tools, and are often a part of such diagnostic tools.

This comment uses the terms "vehicle firmware" or "vehicle software" interchangeably to refer to all the works falling within the proposed class. This comment also refers to diagnosis, repair, and modification collectively as "tinkering."

3. Overview

Modern vehicles are equipped with a system of computers that monitor and control many of the vehicle's functions.[6] Ignition, braking, and engine power are among the many functions controlled in part by computers, often called Electronic Control Units (ECUs).[7] As a result, a wide variety of customization, innovation, and repair activities that have traditionally been within reach of a vehicle owner now depend upon access and modification of this computer code.[8] Modifications and adjustments to car firmware allow car owners to fix malfunctioning software, install new parts, add new features, and customize the vehicle for their use. One community, known as "ecomodders" or "hypermilers," alters car firmware to improve gas mileage to save money and help the environment.[9] Cars may be built for fuel optimization at sea level and run inefficiently at high altitudes unless adjustments are made.[10] The increasing prevalence of inter-vehicle communication may necessitate modification for drivers to travel without being tracked

[1] Appendix D, Statement of Chris Valasek at ¶ 7 ("Valasek Statement").

[2] Appendix B, Statement of Charlie Miller at ¶ 6 ("Miller Statement").

[3] 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.

[4] *Id.*

[5] Appendix A, Statement of David Blundell at ¶ 7 ("Blundell Statement"); Miller Statement at ¶ 7.

[6] *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.

[7] 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.

[8] Appendix C, Statement of Craig Smith at ¶¶ 4, 5 ("Smith Statement").

[9] *See* James Foxall, *Can You Improve Economy by Chipping Your Car 's Engine?*, THE TELEGRAPH (Feb. 7, 2013), http://www.telegraph.co.uk/motoring/news/9826964/Can-you-improve-economy-by-chipping-your-cars-engine.html.

[10] *See, e.g.*, Marlan Davis, *Density Altitude-Tuning for the Weather*, HOT ROD MAGAZINE (Apr. 29, 2009), *available at* http://www.hotrod.com/techarticles/engine/hrdp_0406_density_altitude_tuning.

by their electronic signatures.[11] Certain repairs also necessitate firmware adjustments.[12] For example, without access to ECU firmware, it may be impossible to operate a car after replacing engine components, axles, or transmission systems.[13] Vehicle owners “rely on tools derived from reverse engineering car firmware to make vehicles operate properly after modifications as simple as tires and gears.”[14]

Vehicle owners who tinker with their vehicles are engaged in a decades-old tradition of mechanical curiosity and self-reliance, and they are numerous. When researcher Craig Smith published his *2014 Car Hacker’s Handbook*, it was downloaded 300,000 times in the first two weeks.[15] And automotive enthusiast Dave Blundell helps “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.”[16] The commercial automobile aftermarket is also remarkably robust, accounting for hundreds of billions of dollars in the United States alone.[17] Yet, because most automobile manufacturers deploy measures to prevent access to ECU firmware and software that modifies it, vehicle owners are unable to access the firmware on their own vehicles without incurring legal risk under Section 1201(a)(1).

The tinkering contemplated by the proposed exemption is authorized by fair use and by Section 117. Copyright law permits users to employ copyrighted works in the course of reverse engineering the software and hardware associated with those works, and there is no reason to deviate from that principle for any aspect of vehicle tinkering. Accordingly, the Librarian should grant an exemption from Section 1201(a)(1) 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.[18] The second is encryption, which is used to restrict access both to firmware contained in certain vehicle ECUs and to firmware update files.[19] The third involves the disabling of access

[11] *See* “Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications,” 79 Fed. Reg. 49270 (Aug. 20, 2014) (describing vehicle-to-vehicle communications capabilities).

[12] Blundell Statement at ¶ 2.

[13] Blundell Statement at ¶¶ 3-5.

[14] Blundell Statement at ¶ 9.

[15] Smith Statement at ¶ 3.

[16] Blundell Statement at ¶ 1.

[17] *Who We Are*, AUTOCARE ASSOCIATION, http://www.autocare.org/who-we-are (last visited Feb. 5, 2015) (“The Auto Care Association is the voice of the $300 billion plus auto care industry.”).

[18] *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).

[19] Bordyk, *supra* note 19, 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.

ports, such as "JTAG pins," on the circuitry itself.[20]

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.[21] 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.[22] 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.[23] 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.[24]

Solving the challenge-response mechanism by brute force analysis is mathematically possible (requiring a little over a week for a 16-bit key).[25] More commonly, researchers solve such challenges by extracting the necessary keys from official ECU software updates or diagnostic tools,[26] or from related firmware.[27] (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.[28]

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,[29] as does the Bosch Electronic Diesel Control EDC 16.[30] Encryption is also used to

[20] Craig
Smith, *Car Hackers' Handbook*, http://opengarages.org/handbook/2014_car_hackers_handbook_compressed.pdf , at pp. *56-60*.

[21] Koscher et al., *supra* note 7, at 5-6.

[22] Id.

[23] Id. at 6.

[24] Smith Statement at ¶ 6.

[25] Koscher et al., *supra* note 7, at 7; Smith Statement at ¶ 8.

[26] Id.; Miller Statement at ¶ 6; Valasek Statement at ¶ 3.

[27] Valasek Statement at ¶ 4.

[28] 321 Studios v. Metro Goldwyn Mayer Studios, Inc., 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004).

[29] 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).

[30] 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).

restrict access to data compilations containing vehicle-related data.[31] In addition, files containing official updates to ECU firmware can be encrypted, as part of a mechanism in which update files must prove their authenticity before the ECU will accept the update.[32] 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.[33] 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.[34] 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.[35]

As with challenge-response mechanisms, encryption can be overcome by brute force[36] 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[37] using brute force methods without specialized computing equipment, though they estimate this will be technically feasible within the next five years.[38] 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.[39]

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.[40] However, some manufacturers intentionally disable these access ports (for example, the JTAG

[31] 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.

[32] 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* note 19; see also Koscher et al., *supra* note 7, at 14 (describing cryptographically signed firmware updates as a "simple security mechanism").

[33] Koscher et al., *supra* note 7, at 4-5.

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

[35] *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.")

[36] *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)

[37] Keith@APR, *supra* note 34.

[38] Kleinjung et al, *supra* note 36, at 1.

[39] 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).

[40] Smith, *supra* note 20, at 56-57.

port).[41] One means of disabling access entails setting a control bit to prevent extraction of firmware unless certain signals are received during runtime.[42] 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.[43] 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).[44] When this has been done, voltage or optical glitching is necessary in order to overcome the obstacle presented by the fuse.[45]

5. Asserted Noninfringing Use(s)

Copying and manipulating vehicle software in the course of diagnosis, repair, and modification is authorized by fair use (17 U.S.C. § 107) and by 17 U.S.C. § 117.

Vehicle owners have long tinkered with their cars, coming up with features the manufacturers never imagined, like plugging into the cigarette lighter for electricity.[46] This tradition continues in the age of computerized vehicles, albeit under a legal cloud. Modern tinkerers are adding vehicle features to the unused memory of their vehicles and fine-tuning the software to eke out better gas mileage or power.[47] They are modifying their vehicles to work better for the specialized purposes they need, such as operating at high altitude or racing on private courses.[48] They alter their vehicles' software to make sure the lights turn on when the windshield wipers activate, display miles-per-gallon in real time,[49] or to cap the speed when they lend the car to their teenage children[50] or to a valet.[51] These modifications rely upon the ability to access vehicle software.

In order to facilitate diagnosis and repair, users must sometimes modify vehicle software. One common example of this arises when a user is trying to understand what part of a complex system – their vehicle – is causing a particular malfunction.[52] In order to narrow down the possibilities, it is common to disable certain hardware components, such as sensors or fans.[53] Disabling these

[41] *Id*. at 57; *see also* Blundell Statement at ¶ 7.

[42] Smith, *supra* note 20, at 57-60; *see also* Blundell Statement at ¶ 7.

[43] Smith, *supra* note 20, at 57-60; *see also* Blundell Statement at ¶ 7.

[44] Smith, *supra* note 20, at 57-60; *see also* Blundell Statement at ¶ 7.

[45] Smith, *supra* note 20, at 57-60; *see also* Blundell Statement at ¶ 7.

[46] Jason Torchinsky, *A Tribute to the Cigarette Lighter Plug, The Original Car Hack,* Jalopnik (May 8, 2014), http://jalopnik.com/a-tribute-to-the-cigarette-lighter-plug-the-original-c-1573310295

[47] KJINTF, Comment to *GM Tech 2 Scanner*, iRV2.com (Dec. 18, 2014), http://www.irv2.com/forums/f22/gm-tech-2-scanner-229545.html ([C]hanging firmware is done "for many reasons including better mileage and or more power.").

[48] Blundell Statement at ¶¶ 3, 8, 9.

[49] *Trip computer: Upgrading and Calibrating?* Focus Fanatics (Aug. 8, 2013), http://www.focusfanatics.com/forum/showthread.php?t=323569.

[50] "Custom Hydra Calibrations" Product Page, Power Hungry Performance, available at http://store.gopowerhungry.com/3l-tuning/132-custom-hydra-calibrations.html (last accessed Feb. 4, 2015)

[51] *See* Forum discussion on *Valet Tune??? Prevent Strangers From Joyriding in My Car*" LS1TECH.com Forums (June 8, 2010), http://ls1tech.com/forums/pcm-diagnostics-tuning/1291328-valet-tune-prevent-strangers-joyriding-my-car.html. Valet mode restricts the vehicle to a present speed limit and RPM. *Custom Operating Systems*, EFILive (last accessed Feb. 5, 2015), http://www.efilive.com/product-info-custom-operating-systems.

[52] iFixit, Short Comment Regarding a Proposed Exemption under 17 U.S.C. 1201, Proposed Class 21 (February 6, 2015) (discussing attempt to repair vehicle used for agriculture).

[53] *Id.*

components requires access to and modification of vehicle firmware.[54] Without the ability to manipulate software in the course of diagnosis and repair, users are often forced to wait for technicians with proprietary systems to become available[55] or replace parts that may or may not be faulty, creating waste and unnecessary expense.

Additionally, it is common for repairs that replace hardware components to require modifications to firmware in order to calibrate the new part. If new gears have a different radius than old ones, the computer needs to know so that the speedometer will work correctly.[56] If engine components are replaced, they must be calibrated in concert with the computer and sometimes engine or computer replacements require the anti-theft system on another computer to be deactivated or reset.[57] In order to understand vehicle software and identify the appropriate changes to make in order to calibrate new parts, users require access to the software, and sometimes have to circumvent technological restrictions in order to get that access.[58] It may also be necessary to study locked-down software tools that are designed to modify the computer memory in the vehicle, such as software updates[59] and diagnostic tools.[60]

Access to vehicle software enables owners to understand how it works so that some modifications can later be made arguably without circumventing access controls at all. Some modifications can be made by satisfying a challenge-response mechanism that grants the ability to write data to a location on the ECU storage, but does not regurgitate the vehicle software.[61] Circumventing such technology, when it is not an access control, is not prohibited by Section 1201. The knowledge required to pinpoint which memory locations to modify for which purpose, and the means of satisfying the challenge-response mechanism, however, require a user to have accessed the entire software in the first place in order to understand which memory locations store variable values and how they are used by the software.[62] Analyzing the software is also a means of obtaining vehicle diagnostic codes, since the software is responsible for sending those codes out.[63] Thus access to diagnostic codes can be achieved by gaining access to vehicle software, as well as by gaining access to vehicle data compilations directly.

A. Fair Use

Fair use[64] is "a privilege in others than the owner of the copyright to use the copyrighted material in a reasonable manner without his consent."[65] In 2010 and 2012, the Register concluded correctly that modifying the firmware in one's device in order to run lawfully acquired software is a fair use, falling squarely within Congress's intent to promote software interoperability. Court

[54] *Id.*
[55] *Id.*
[56] Blundell Statement at ¶ 4.
[57] Blundell Statement at ¶¶ 4, 6.
[58] Blundell Statement at ¶¶ 2-7; Smith Statement at ¶ 5.
[59] Smith Statement at ¶ 5.
[60] Valasek Statement at ¶ 7.
[61] Koscher et al., *supra* note 7, at 6-12 (describing the "carshark" software written to send such commands to vehicle ECUs and the tests performed with such functionality, including "Self-Destruct Mode" involving locks, horns, radio, and engine control.)
[62] Blundell Statement at ¶ 5; Miller Statement at ¶ 7.
[63] Blundell Statement at ¶ 5; Miller Statement at ¶ 7.
[64] 17 U.S.C. § 107.
[65] *Harper & Row, Publrs. v. Nation Enters., Inc.*, 471 U.S. 539, 549 (1985) (internal quotations omitted).

decisions since 2012 give additional weight to that determination.

For similar reasons, vehicle owners who manipulate vehicle-related software for legitimate tinkering purposes are engaged in fair use.

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.[66]

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 analysis and modification of 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 competing games.[67] The court emphasized that the functional aspects of Sega's software were not copyrightable, and recognized that copying the entire software – including copyrightable elements – was necessary for analysis.[68] 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.[69] These cases both stand for the proposition that enabling interoperability and increasing the utility of hardware are fair uses.

Just like the interoperability research of Accolade and Connectix, research involving vehicle software for repair, modification, and diagnosis has legitimate purposes that fall well within the scope of fair use. Tinkering implicates the same software interoperability interests as those cornerstone fair use cases, and additionally implicates *hardware* interoperability, because of the embedded nature of vehicle software.[70] Copyright should not be a tool for manufacturers to create a monopoly in vehicle repair parts, which is the result when users are barred from making the necessary modifications to ECUs to calibrate replacement parts.

Tinkering involves a variety of transformative purposes. In the case of modification, users are literally adding new functions or modifying existing functions to suit different needs. In the case of all three categories of tinkering (diagnosis, repair, and modification), users are seeking to understand the functional aspects of the copyrighted work. The copyrightable elements of vehicle software are incidental to such users' purpose in understanding the code's functionality.[71] What functions exist that can be modified, or communicated with by other software and hardware? Will

[66] *Campbell v Acuff Rose Music, Inc.*, 510 U.S. 569, 579 (1994) (internal quotations omitted).

[67] *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).

[68] *Id.*

[69] *Sony Computer Entm't Inc. v. Connectix Corp.,* 203 F.3d 596, 608 (9th Cir. 2000).

[70] E.g., Blundell Statement at ¶¶ 2-7.

[71] Blundell Statement at ¶ 5.

errors arise elsewhere if something is changed? What values must be edited to calibrate a replacement part or fine-tune performance or gas mileage? Which memory locations are available for custom software? Which memory locations correspond to variables that may be altered without circumventing an access control? What conditions cause which diagnostic codes to be issued? What will the software do when it receives a standardized command from an outside repair interface? Copyright should not prohibit vehicle owners from answering these questions for themselves.

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."[72] 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.[73] 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. *Id.* 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."[74]

In the 2010 and 2012 rulemaking proceedings, relying in part on *Sega's* reasoning, the Register concluded that the second factor "decisively favors a finding of fair use."[75] Noting that the second factor is "perhaps more important than usual in cases involving the interoperability of computer programs," the Register noted that bootloaders and operating systems are largely functional works, and that "[a]s functional works, certain features are dictated by function and in order to interoperate with those works certain functional elements of those programs, elements that in and of themselves may or may not be copyrightable, must be modified."

The Federal Circuit's 2014 holding in *Oracle v. Google* regarding fair use of software interfaces is consistent with the Register's reasoning in the 2010 and 2012 rulemakings. The court noted that some elements of computer programs are "dictated by considerations of efficiency or other external factors" and held that "where the nature of the work is such that purely functional elements exist in the work and it is necessary to copy the expressive elements in order to perform those functions, consideration of this second factor arguably supports a finding that the use is fair."[76]

At least one court has found that where a portion of a software program functions as a "lockout code[]" that *must* be used to enable compatibility with independently created programs, the rightsholder's copyright interest in that portion of code is exceedingly slim. In *Static Control Components, Inc. v. Lexmark Intern., Inc.*, Static Control copied a small portion of code from Lexmark's laser printer firmware, acting on a reasonable belief that only by copying that code

[72] *Id.* at 603.

[73] *See* 977 F.2d at 1526.

[74] 203 F.3d at 605.

[75] 2010 Rec. at 96; 2012 Rec. at 73.

[76] *Oracle America, Inc. v. Google Inc.*, 750 F. 3d 1339, 1375 (Fed. Cir. 2014).

could Static Control build toner cartridge components that would interoperate with Lexmark printers.[77] The court held that software code used as a "lockout" bears only a thin copyright interest that is overcome by the need to use that code for interoperability.[78]

Any creative, copyrightable aspects of vehicle firmware that may exist are minimal.[79] 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 a finding of fair use. Further, the rights of a copyright owner in device firmware are not customarily understood to be infringed when the device owner runs other, independently created software without the manufacturer's consent.

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."[80] 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.[81]

Tinkerers' access and copying of the entire firmware within an ECU or an update is essential to understanding the functionality of a vehicle[82] and determining how much storage capacity is available in the hardware for additional functionality.[83] This process requires the use of the entire work, since functionality may be found anywhere in the code[84] and the technological process of reading the firmware off of the ECUs or decrypting an update typically provides the entire program.[85] As automotive enthusiast Dave Blundell explains, tinkerers regularly rely on the knowledge gleaned from reverse engineering vehicle software, and "[w]ithout 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."[86] For these reasons, the use of the entire work is fair in light of the legitimate purposes of the use.

[77] No. CIV.A. 02-571, 2007 WL 1485770, at *5 (E.D. Ky. Apr. 18, 2007) (on remand from *Lexmark Int 'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004)).

[78] *Id.* ("Regardless of whether Lexmark's [programs] were uncopyrightable lockout codes or not, SCC was reasonable in initially believing that they were.").

[79] Miller Statement at ¶ 7.

[80] *Campbell*, 510 U.S. at 586-87.

[81] *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 v. Arriba*, 336 F.3d 811, 820-21 (9th Cir. 2003) (holding that third fair use factor did not weigh against copier when entire-work copying was reasonably necessary); . [perfect 10 cite]

[82] *See Koscher supra* note 7, at 9.

[83] *See, e.g.,* Tephra, Forum post to *TephraMod V7*, EVOLUTIONM.NET (Oct. 10, 2009), http://www.evolutionm.net/forums/ecuflash/451836-tephramod-v7.html (last updated Apr. 10, 2011).

[84] Miller Statement at ¶¶ 7, 8.

[85] Smith, *supra* note 20, at 60.

[86] Blundell Statement at ¶ 5.

4. Market for the Copyrighted Work

The fourth factor looks to direct harms to the market for the copyrighted work.[87] This factor is concerned with the harm of market substitution, not any harm caused by substantive criticism of the copyrighted work.[88] 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."[89]

In the case of vehicle firmware, the copyrighted work is sold to end-users along with an entire vehicle. In addition, 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, and it does not harm any copyright interest of the manufacturer for the owner to learn how it works and engage in lawful modification and repair.

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."[90]

The same analysis supports the granting of an exemption allowing vehicle owners to tinker with the firmware that operates vehicles. 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 on the public. Nor is it a valid tool to deprive users of control over their own vehicles and the ability to repair them.

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.

[87] *Campbell*, 510 U.S. at 590.

[88] *See id*. at 591-92.

[89] *Sony Corp. of Am. v. Universal City Studios, Inc*., 464 U.S. 417, 450 (1984).

[90] 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.

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.[91] 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.[92]

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.[93]

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.[94] 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."[95]

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.*[96] *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 whether the copyright owner required the transferee to maintain possession of the copy throughout the duration of the agreement.[97]

[91] *Krause v. Titleserv, Inc.*, 402 F.3d 119, 123 (2d Cir. 2005).

[92] *Id.* at 124.

[93] *Id*. at 124.

[94] *Id.* at 126.

[95] *Id*. at 128.

[96] 621 F.3d 1102 (9th Cir. 2010).

[97] *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).

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.[98] 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[.]"[99]

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

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

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

including altering any digital rights management functionality of the Software[.]"[100]

- 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.[101]

- 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."[102]

- 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."[103]

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 of their use.[104] 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.

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

[101] *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.

[102] *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.

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

[104] *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.").

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.[105] 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) Authorizes Users to Copy Vehicle Software for Use with Tinkering 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.[106]

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 in order to understand its functionality.

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.[107]. 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."[108]

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 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.[109] This

[105] *SoftMan Products Co., LLC v. Adobe Sys., Inc.*, 171 F. Supp. 2d 1075, 1085 (C.D. Cal. 2001).

[106] *Vault Corp. v. Quaid Software, Ltd.*, 847 F.2d 255, 261 (5th Cir. 1988).

[107] *See Krause v. Titleserv, Inc.,* 402 F.3d 119, 127 (2d Cir. 2005).

[108] *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*).

[109] *Telecomm Tech. Servs., Inc. v. Siemens Rolm Comms., Inc.,* 66 F. Supp. 2d 1306, 1325 (N.D. Ga. 1998).

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 analyze 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."[110] 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.[111] 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 Curtails User-Driven Innovation, Endangers Users, Restricts User Choice, and Harms Independent Repair Providers

Vehicle owners expect to have the freedom to repair and tinker with their vehicles, as they have done for decades. A booming aftermarket industry has grown up in reliance on owners' having the freedom to tinker with their cars and bring them to repair facilities of their choice.[112] But TPMs on ECU firmware block such legitimate activities,[113] forcing vehicle owners to choose between incurring legal risk or losing the self-reliance that has been a hallmark of vehicle ownership in the United States. Car repair, diagnosis, and modification increasingly depend on access to the software that controls a vehicle's functions and proprietary codes, information that is increasingly locked down with access controls.[114]

Vehicle manufacturers are introducing more and more computer-controlled features as demonstrated at the 2015 Consumer Electronics Show, including self-driving cars.[115] Additionally, cars are increasingly communicating wirelessly, providing new avenues for hackers and leaking information about drivers.[116] The increasing computerization of vehicles means that a

[110] *Micro-Sparc, Inc. v. Amtype Corp.,* 592 F. Supp. 33, 35 (D. Mass. 1984).

[111] See *Vault Corp. v. Quaid Software, Ltd.,* 847 F.2d 255, 261 (5th Cir. 1988), 847 F.2d at 264-66.

[112] *About SEMA*, SEMA, http://www.sema.org/about-sema (last visited Feb. 5, 2014).

[113]*Calibrating Automotive Electronics*, ETAS, http://www.etas.com/en/products/solutions_calibrating_automotive_electronics.php (last visited Oct. 28. 2014).

[114] Smith Statement at ¶ 5.

[115] Will Oremus, *The Year of the Car*, SLATE (Jan. 9, 2015), http://www.slate.com/articles/technology/technology/2015/01/ces_2015_in_car_tech_year_of_the_car_at_the_consumer_electronics_show.html.

[116] *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;.

driver who wishes to make something new, to repair their own vehicle, or to make their own choices about their security and privacy must contend with the legal cloud of Section 1201 to turn those preferences into practice. There is no copyright-based reason to prevent users from exercising those freedoms.

1. *The Prohibition on Circumvention Reduces User Choice and Reduces Competition in the Vehicle Repair Industry*

TPMs on vehicles restrict vehicle owners' choice of their preferred method of vehicle repair. When only manufacturers are able to effectuate repairs, users can no longer do it themselves or use an independent service provider of their choice. This results in higher prices, longer trips for repair, fewer options, and all the other ills of reduced competition.

AutoMD, an auto-repair information site, conducted a study that shows that consumers can cut their repair bills by an average of about $300 a year, or 25%, by going independent.[117] In 2011, 70% of car owners went to an independent repair shop for aftermarket care while the cars were still under warranty.[118] However, in newer model cars needing complex repairs, dealers will sometimes have diagnostic equipment not available to independents.[119]

The prevalence of proprietary computer systems in cars has reduced the effectiveness of independent repair shops significantly: according to one 2005 study, 67% of independent repair shops had to send vehicles to a franchise dealer to complete the repairs, in part because 59% of the independent technicians had problems accessing the technical information necessary to complete the repair.[120] Since the 2009 recession caused consumers to search for cost-effective measure to repair their cars, "[manufacturers] have become very aggressive in the aftermarket and they are using technology as one means to do that."[121] The presence of TPMs on software in vehicles makes it even harder for consumers to tinker with their own vehicles or to turn to independent repair shops of their choosing.

Motorcycle owners have documented issues with proprietary computer systems that restrict their ability to repair and even to re-key their own vehicles. Because of restricted access to motorcycle ECUs, owners of Ducati motorcycles who misplace the "red key," a physical key given to

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; Valasek Statement at ¶ 6.

[117] Jonathan Welsh, *Is the Dealer Better Than an Independent Mechanic?*, THE WALL STREET JOURNAL (May 2010), http://blogs.wsj.com/drivers-seat/2010/05/17/is-the-dealer-better-than-an-independent-mechanic/; *see also Where to Repair? Dealer or Independent*, CAR TALK, http://www.cartalk.com/content/where-repair-dealer-or-independent (finding that dealers charged 15% more than independent repair shops for the same repairs).

[118] Alina Tugend, *Who's Best for Your Car, Dealer or Independent?*, THE NEW YORK TIMES (Feb. 2011), http://www.nytimes.com/2011/02/26/your-money/26shortcuts.html?pagewanted=all.

[119] *Id.*

[120] Jennifer Saranow, *Where to Get Your Car Fixed*, THE WALL STREET JOURNAL (Sept. 2005), http://www.wsj.com/articles/SB112795765902455411.

[121] *Dealership or Independent Repair Facility? It's complicated*, INFOMEDIA (June 2014), http://www.superservice.com/us/blog/counterview/50-dealership-or-independent-repair-facility-it-s-complicated.

purchasers of new motorcycles, are unable to reprogram their ECUs for any purpose.[122] This means that software errors, such as unintended activation of the immobilizer system, cannot be addressed by users.[123] When contacting Ducati for assistance in these situations, Ducati North America representatives have reportedly told owners that they must replace the dash, lockset, and ECU—at a cost of approximately $3000.[124] Owners are faced with a choice between wasteful, time-consuming, and expensive replacement of hardware, and potentially exposing themselves to legal risk via circumvention.

This is not the only obstacle faced by owners of Ducati Motorcycles seeking to do their own repairs. At certain intervals, a red "Oil Service" light turns on to remind the owner to perform routine maintenance. Owners who choose to perform the service themselves, to either avoid paying hundreds of dollars for a glorified oil change or simply to ensure that the highest quality components are used, however, are unable to subsequently reset the light – it remains lit indefinitely. [125] Not only does this render the light inoperable as a signal, but it can also distract the rider, as the light is attention-grabbing by design.[126] Owners report that a dealership may refuse to turn off the light at all if they were not hired to do the maintenance work, or may charge up to $100 to plug in a computer that can turn off the light.[127] They went on to lament the lack of a non-proprietary tool.[128] There is no copyright-based reason to prevent vehicle owners from performing this kind of maintenance and turning off their own service lights.

According to one account, a vehicle owner had to travel 6 hours in Maine to reach a dealership that was able to reboot the car's computer to shut off the "low tire pressure" light, because the nearby independent repair shop that replaced the tire was not given the computer code by the manufacturer for the low-tire-pressure sensor.[129] This is a case where access to diagnostic codes – which can be acquired by circumventing TPMs on vehicle software or on vehicle data compilations – is necessary to protect robust competition that gives users choice and reduces the prevalence of vehicle service monopolies. Similarly, there are third-party tools that would give individuals or independent repair shops the ability to modify ECU memory and effectuate certain repairs arguably without circumventing, but creating those tools requires that someone was able to access and reverse engineer the vehicle software, an activity that must take place under the legal cloud of Section 1201 absent an exemption.[130]

[122] Brett Foster, *Ducati Motorcycles & The Dreaded Red Key*, HubPages (Nov. 21 2012), http://kurant82.hubpages.com/hub/DUCATI-MOTORCYCLES-THE-DREADED-RED-KEY-DILLEMA-WHAT-DUCATI-OWNERS-SHOULD-KNOW

[123] Forum discussion on *Immobilizer Crapped; New ECU or Ignition?* (2012), http://www.ducati-superbikes.com/index.php/topic/22508-immobilizer-crapped-new-ecu-or-ignition/.

[124] Forum discussion on *Ducati Key/Code Card Nightmare*, PWNRIDERS.COM (2013), http://pnwriders.com/motorcycle-talk/180615-ducati-key-code-card-nightmare.html - post2909878.

[125] Forum discussion on *Oil Service Light*, DIAVEL-FORUM.COM (2011), http://www.diavel-forum.com/index.php?/topic/665-oil-service-light/page__p__60920.

[126] *Id.*

[127] *Id.;* Forum discussion on *Ducati Dealer Refused to Turn Off Service Light*, Ducati.ms (2012), http://www.ducati.ms/forums/44-multistrada/139726-ducati-dealer-refused-turn-off-service-light.html.

[128] *See* Forum discussion on *Oil Service Light*, *supra* note 125.

[129] Tom Bell, *Long Drive for Car Repair Sparks Call For Legislation*, PORLAND PRESS HERALD (Feb. 2013), http://www.pressherald.com/2013/02/04/long-drive-for-car-repair-sparks-call-for-legislation_2013-02-04/.

[130] Blundell Statement at ¶ 5.

Similar concerns about proprietary technical information have fueled the battle to pass right-to-repair laws. In the European Union, as part of antitrust regulation, the European Commission requires car manufacturers to provide independent repair shops with access to technical information on the same terms as authorized dealers. This ruling is based on findings that "carmakers seem to have withheld certain technical information from independent repairers and have provided the rest in a way that does not meet their needs. These apparent inadequacies could force independent repairers from the markets, resulting in considerable consumer harm."[131] Independent repair shops lower the price of repairs, which make up almost half the total cost of owning a car. Since technical information (which is very broadly defined) is becoming an increasingly important part of car repairs, accessing it is crucial for independent manufacturers to stay afloat and provide competition to authorized dealerships.[132] This regulation is partially based on a decision by the European Commission against DaimlerChrysler, Toyota, General Motors and Fiat, which concerned these manufacturers' restricting independent mechanics' access to technical information.[133]

2. *The Prohibition on Circumvention Makes Automobiles Less Safe*

When vehicle repairs are more expensive and less convenient due to lack of competition, vehicles will receive less rigorous and frequent maintenance. This endangers drivers, bystanders, and property.

But additional hazards exist as a direct result of the way technological restrictions on vehicles are being deployed. In EFF's petition regarding Proposed Class 22, relating to vehicle security and safety, EFF explains how essential independent research is to the integrity and safe functioning of vehicles. Simply discovering vulnerabilities and malfunctions is valuable, and is all the more valuable if users are empowered to patch those errors and protect themselves.

Manufacturers are also using TPMs to enforce new business models that render vehicles useless if the purchaser misses a payment. The New York Times has reported that some automobile sales are accompanied by "starter interrupter" devices that can shut down a purchaser's car if they are a few days late with a loan payment or drive out of a designated area.[134] Drivers were suddenly prevented from driving their children to the doctor, stranded when they tried to escape domestic abuse, and in some cases had their cars deactivated while they were on the road. These extreme consequences came without judicial process, and often without notice. Similarly, the French automobile company Renault offers an electric car that comes with a "rented" battery. The manufacturer can shut off the battery remotely and uses the battery computer to collect data about the car.[135] Renault ostensibly included this feature to guarantee regular payments from the

[131] *Antitrust: Commission adopts revised competition rules for motor vehicle distribution and repair*, EUROPEAN COMMISSION (May 2010), http://europa.eu/rapid/press-release_IP-10-619_en.htm.
[132] *Id.*
[133] *Id.*
[134] Michael Corkery & Jessica Silver-Greenberg, *Miss a Payment? Good Luck Moving That Car* (Sept. 24, 2014), http://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/.
[135] *See* gerloff, *Renault Will Remotely Lock Down Electric Cars* (Oct. 31, 2013), https://blogs.fsfe.org/gerloff/2013/10/31/renault-will-remotely-lock-down-electric-cars/; Ryan W. Neal, *Renault Zoe: Why DRM Software in Vehicles Is A Bad* Idea, INTERNATIONAL BUSINESS TIMES (Nov. 2013), http://www.ibtimes.com/renault-zoe-why-drm-software-vehicles-bad-idea-1470872.

purchasers of its vehicles.[136] Concerned consumers immediately noted the potentially dangerous repercussions of this feature, which could allow the car to be remotely deactivated by the manufacturer, the government, or malicious hackers and leaks sensitive information about the driver.[137] However, the inclusion of TPMs prevented the car owners from acting on their concerns without incurring legal risk.

Finally, manufacturers are designing other systems that enable remote override of user control, introducing additional vulnerabilities and points of failure. The issue is illustrated by a recent security vulnerability discovered by independent researchers. The vulnerability, residing in BMW's "Connected Drive" wireless feature, allows an attacker to wirelessly instruct the car to unlock itself.[138] If the original manufacturer disappoints them, drivers will wish to go to the competitive marketplace for alternatives – provided the marketplace is not preempted by TPMs.

3. The Prohibition on Circumvention Curtails Innovation by Drivers and Third Parties

The freedom to reverse engineer vehicle software is essential to the livelihood of thousands of Americans.[139] These thousands of persons, and their customers, will be adversely affected if the legal cloud surrounding access to vehicle software is allowed to persist in light of the increasing application of TPMs to vehicle software. This group includes engineers, users of tools that were created using information gained from vehicle software or data compilations, and the employees of companies for whom this is a booming business, including Hondata, Diablosport, COBB Tuning, Ford Racing, Edelbrock, GM Performance Parts, Roush, Procharger, Vortech, and Holley.[140]

In the BMW aftermarket, the presence of TPMs forced tuning company Dinan to create their own replacement ECU hardware, which could be installed at great expense to control the systems of BMWs in lieu of the original ECU devices and software.[141] For an individual vehicle owner, it would be very difficult to design and manufacture custom ECU hardware and software in order to regain control of one's vehicle in the face of TPMs. However, if the TPM could be circumvented, the driver could perform the necessary modifications at the software level, and competitors in the aftermarket could provide their own ECU software for users to flash into their vehicles, avoiding the waste of perfectly good stock ECUs.

There are also thriving communities dedicated to improving their vehicles. One such community, known as "ecomodders" or "hypermilers," alters car firmware to improve gas mileage to save money and help the environment.[142] Another group addresses the fact that cars leave the factory optimized for fuel consumption at sea level and run inefficiently at high altitudes unless

[136] *Id.*

[137] Glyn Moody, *Renault Introduces DRM For Cars*, TECHDIRT (Nov. 2013), https://www.techdirt.com/articles/20131108/09350825182/renault-introduces-drm-cars.shtml.

[138] *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.

[139] Blundell Statement at ¶ 8.

[140] Blundell Statement at ¶ 8.

[141] *See* Lavrinc, *supra* note 19.

[142] *See* James Foxall, *Can You Improve Economy by Chipping Your Car 's Engine?*, THE TELEGRAPH (Feb. 7, 2013), http://www.telegraph.co.uk/motoring/news/9826964/Can-you-improve-economy-by-chipping-your-cars-engine.html.

adjustments are made.[143] They alter their vehicles' software to make sure the lights turn on when the windshield wipers activate, display miles-per-gallon in real time, [144] or to cap the speed when they lend the car to their teenage children[145] or to a valet. [146] Vehicles are frequently called upon to perform in conditions the manufacturers did not foresee, and one size does not fit all when it comes to owner's preferences for how their vehicle will operate. Yet these users' needs may never be addressed by a manufacturer if doing so would not be profitable. Ford's Venkatesh Prasad recognized the value that users provide when they tinker and share their knowledge[147] and also recognized that user innovation outpaces centralized innovation by manufacturers when allowed to thrive.[148] There is no copyright-based reason to prevent owners from accessing the software and data compilations they need to understand in order to modify their property to suit their preferences and needs.

4. The Prohibition on Circumvention Compromises the Privacy of Drivers

Consumers also expressed concern over the privacy implications of the Renault battery computer sharing driver data with the manufacturer. [149] Similarly, Tesla has been criticized for remotely activating GPS tracking in a user's vehicle and collecting reams of data on how a vehicle is being used by a purchaser.[150] Other manufacturers have also been criticized for their weak privacy practices. The Government Accountability Office found in December 2013 that companies' disclosures to consumers were unclear, customers could not request that companies delete retained data about them, consumers were at risk of being identified based on supposedly "de-identified" location data, and no public information was available on how auto makers held employees accountable for violations of user privacy.[151] Senator Markey pointed out that the privacy principles "fall short in two key areas: choice and transparency." [152] Consumer Watchdog explained that automakers' privacy principles "sound good, but the rest of the document that explains how they will be implemented reads like it was written by lawyers paid by the word to

[143] *See, e.g.*, Marlan Davis, *Density Altitude-Tuning for the Weather*, HOT ROD MAGAZINE (Apr. 29, 2009), *available at* http://www.hotrod.com/techarticles/engine/hrdp_0406_density_altitude_tuning.

[144] *Trip computer: Upgrading and Calibrating?* Focus Fanatics (Aug. 8, 2013), http://www.focusfanatics.com/forum/showthread.php?t=323569.

[145] "Custom Hydra Calibrations" Product Page, Power Hungry Performance, available at http://store.gopowerhungry.com/3l-tuning/132-custom-hydra-calibrations.html (last accessed Feb. 4, 2015)

[146] *See* Forum discussion on *Valet Tune??? Prevent Strangers From Joyriding in My Car*" LS1TECH.com Forums (June 8, 2010), http://ls1tech.com/forums/pcm-diagnostics-tuning/1291328-valet-tune-prevent-strangers-joyriding-my-car.html. Valet mode restricts the vehicle to a present speed limit and RPM. *Custom Operating Systems*, EFILive (last accessed Feb. 5, 2015), http://www.efilive.com/product-info-custom-operating-systems.

[147] Ventkatesh Prasad, *User Innovation on the Internet of Things on Wheels*, 8 (May 22, 2014), *available at* http://cdn.oreillystatic.com/en/assets/1/event/111/User Innovation on the Internet of Things on Wheels Presentation.pptx.

[148] *Id.* at 9.

[149] *See* gerloff, *supra* note 135; Ryan W. Neal, *supra* note 135.

[150] Kashmir Hill, *Should Companies be Able to Monitor Our Use of Their Products for Our Own Good?* Forbes (Mar. 1, 2012), http://www.forbes.com/sites/kashmirhill/2012/03/01/should-companies-be-able-to-monitor-our-use-of-their-products-for-our-own-good/.

[151] United States Government Accountability Office, "In-Car Location-Based Services" (December 2013), *available at* http://www.gao.gov/assets/660/659509.pdf

[152] Markey Statement on Automaker Privacy Pledge (November 13, 2014), available at http://www.markey.senate.gov/news/press-releases/markey-statement-on-automaker-privacy-pledge

obfuscate the issues, rather than make them clear."[153] This trend continues, with new Vehicle-to-Vehicle communication standards that fail to address basic privacy concerns.[154] Without the ability to circumvent TPMs, users have no way to act on their concerns about how their property is programmed to serve the interest of the manufacturer over their own interests.

B. The DMCA's Statutory Exemption for Reverse Engineering Is Too Narrow and Uncertain to the Mitigate the Adverse Effects of the Ban on Circumvention

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.

Hobbyists who modify their vehicles' firmware to make it compatible with aftermarket parts 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."[155] To the extent the software in a vehicle needs to be repaired or modified to allow it to communicate with the software in a new engine, fuel system, or other parts, the use would seem at first blush to fit within Section 1201(f).

However, an owner may not modify a vehicle for the sole purpose of interoperability, but to tailor the vehicle to best meet the owner's needs or preferences and to educate others. Many hobbyists access and modify vehicle firmware for fun or to test and improve their own hacking skills in addition to enabling interoperability. *Reimerdes* held that such a use did not qualify for the reverse engineering exception.[156] 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 hobbyist making a modification or repair to a vehicle may well follow a set of instructions shared by other hobbyists, such as the Car Hacker's Handbook. Such activity would fail to satisfy the requirement that the elements the hobbyist 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

[153] Consumer Watchdog, "Automakers' Privacy Principles Offer Little Real Protection, Consumer Watchdog Says," *available at* http://www.consumerwatchdog.org/newsrelease/automakers%E2%80%99-privacy-principles-offer-little-real-protection-consumer-watchdog-says.

[154] Professor Dorothy Glancy and EFF, Comments Re: NHTSA V2V ANPRM (Docket No. NHTSA–2014–0022), (October 20, 2014), available at ; "Comments of the Electronic Privacy Information Center to the National Highway Traffic Safety Administration, Federal Motor Vehicle Safety Standards: 'Vehicle-to-Vehicle (V2V) Communications,'" (October 20, 2014), available at https://epic.org/privacy/edrs/EPIC-NHTSA-V2V-Cmts.pdf.

[155] 17 U.S.C. § 1201(f)(4).

[156] *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 320 (S.D.N.Y. 2000).

technological measures protecting the firmware in their phones did not "fall within the four corners" of the Section 1201(f) statutory exemption.[157] However, the Librarian's decision folded the interoperability test into a fair use analysis, finding that the use was noninfringing because it 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.[158] 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 modification, repair, and diagnosis involving vehicle software.

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 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.[159] Software patches also depend on access, including patches to fix serious vulnerabilities.[160] Numerous tools designed to analyze and manipulate firmware also depend on the ability to access software and reverse engineer it.[161] The availability of copyrighted works will be promoted by the proposed exemption.

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

Education about vehicle engineering and tinkering will benefit from increased knowledge of vehicle firmware to use as real-world examples in teaching and the increased ability of individuals to explore the technology for themselves.[162] In addition, it will be possible to archive and preserve firmware on general-purpose storage media, without expensive and unreliable storage of ECU hardware. Furthermore, tinkering is itself educational and is a common path for young people to become interested in studying science and engineering.[163] Copyright law should

[157] 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.

[158] 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.

[159] Smith Statement at ¶ 3.

[160] Miller Statement at ¶ 7.

[161] Blundell Statement at ¶ 5.

[162] Miller Statement at ¶¶ 2, 6; Smith Statement at ¶¶ 3, 9; Valasek Statement at ¶¶ 2, 7, 8.

[163] *See, e.g.*, Steve Song, "In Praise of Taking Things Apart," *available at* https://manypossibilities.net/2008/03/in-praise-of-taking-things-apart/ (quoting an interview with John Seely-Brown in which he said "A huge amount of the

not discourage this important activity, but should permit works to be used for the educational purpose of hands-on learning.

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 functionality, repair, and modification, as well as critiquing, commenting, and reporting on the functionality of manufacturer software and potential alternatives.

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

As discussed above, the relevant markets 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 each of the proposed uses—diagnosis, repair, and modification—(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.

With respect to part (a), as discussed above, a wide variety of activities in each proposed use category require access to vehicle software itself.[164] In addition, access to variable descriptions, function documentation, diagnostic codes, and parts specifications are themselves restricted by manufacturers' claims of copyright on compilations of such non-copyrightable information and such data compilations should be included in the proposed class. Even if they are not included in the proposed class, the restricted access to these works and the resulting adverse effects are partially mitigated by an exemption covering vehicle software, since such data can be reverse engineered by someone with access to the software itself.[165] As for part (b), the answer depends on the vehicle manufacturer, 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. The applicability (or not) of the statutory exemption for reverse engineering in 17 U.S.C. 1201(f) to the proposed uses.

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

learning that a lot of us do, that formed the foundations of all the formal education that we got afterwards, could be called 'tinkering.' Because of changes in electronics and cars, a whole generation couldn't tinker.")

[164] *See* Blundell Statement at ¶¶ 2-7; Miller Statement at ¶ 8; Smith Statement at ¶¶ 4-9; Valasek Statement at ¶ 3.

[165] Miller Statement at ¶ 7.

3. *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 permission of the owner of a vehicle by a third party. Many individuals do no 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 offer circumvention services for the exemption to reach the majority of its beneficiaries.

To the extent the Register is concerned that such services would be barred by Section 1201(a)(2), the response is that many such services do not fall under any of the three categories of forbidden conduct identified in 1201(a)(2)(A) through (C).

General purpose vehicle repair services do not constitute a service barred by 1201(a)(2), even if they engage in circumvention as part of offering their services. Vehicle tinkering services are 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, repair and diagnosis services are primarily oriented towards repairing vehicles by definition, and typically repair shops do not give customers themselves access to vehicle software. Modification services also include a wide array of services not prohibited by this section and pursue purposes such as improved performance and additional of new features, catalogued above in the discussion of adverse effects. Vehicle tinkering services also do 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). Vehicle tinkering is itself highly commercially significant, as described above, and circumvention is incidental to this activity. The commercial value of tinkering has nothing to do with copyright infringement. Finally, vehicle tinkering is typically not "marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access" to a copyrighted work. While a service could theoretically be marketed "for use in circumventing," 17 U.S.C. § 1201(a)(2)(C) such as a remote-processing service marketed for a user to crack vehicle encryption keys, this is not part of typical tinkering services. The fact that a repair shop circumvents in the course of some repairs, and may in some cases advertise its ability to perform repairs requiring circumvention, does not transform repair services into services marketed "for use in circumventing" technological measures.

Extending an exemption for use by third parties with the permission of the vehicle or device 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."[166] The same considerations apply to vehicle tinkering.

[166] 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/737420992943 719; EFI Live Users (2,513 members), https://www.facebook.com/groups/291322157655351; E FI 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 make s tuning hardware) (205,217 likes), https://www.facebook.com/cobbtuning; Hondata (company t hat makes tuning hardware) (38.347 likes), https://www.facebook.com/pages/Hondata/10877202 2480315; 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://w ww.chevrolet.com/performance.html), Roush (www.roush.com), Procharger (www.procharger.c om), 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.