Before the

U.S. COPYRIGHT OFFICE, LIBRARY OF CONGRESS

In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

Docket No. 2014-07

Petition of Electronic Frontier Foundation

Submitted by:

Kit Walsh
Corynne McSherry
Mitch Stoltz
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
kit@eff.org

Of counsel:

Marcia Hofmann
25 Taylor Street
San Francisco, CA 94102
Telephone: (415) 830-6664
marcia@marciahofmann.com

Devon Edwards and Nicole Kramer, Student Attorneys
Jason Schultz, Professor of Clinical Law
NYU Technology Law & Policy Clinic
40 Washington Square South
New York, NY 10012-1099
SchultzJ@exchange.law.nyu.edu

The Electronic Frontier Foundation submits the following petition and respectfully asks the Librarian of Congress to exempt the following class of works from 17 U.S.C. § 1201(a)(1)'s prohibition on the circumvention of access control technologies for 2015-2018:

Proposed Class:[1] *Lawfully-obtained computer programs that control or are intended to control the functioning of a motorized land vehicle, including firmware and firmware updates, where circumvention is undertaken by or on behalf of the lawful owner of such a vehicle for the purpose of lawful aftermarket personalization, improvement, or repair.*

I. The Commenting Party

The Electronic Frontier Foundation (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.

In filing this petition, EFF represents the interests of the many individuals who have purchased vehicles that contain computer programs that control vehicle operation and either have or would like

[1] Petitioners expect to further develop the proposed exemption consistent with the principles identified in this petition and the record developed in the course of this proceeding.

to personalize, improve, or repair those vehicles.

II. Proposed Class: Circumvention Necessary for After Market Personalization, Improvement, or Repair in Vehicles with Internal Computer Systems

A. Overview

Modern vehicles are equipped with a system of computers that monitor and control many of the vehicle's functions. In cars, these computers are called Electronic Control Units, or ECUs. In any given car, there are scores of individual ECUs with unique functions working in synchronization to dictate vehicle performance.[2] For example, the Engine Control Module is the ECU that "determine[s] the amount of fuel, ignition timing, and other engine parameters" of a car.[3] The Electronic Brake Control Module is the ECU that "controls the [system that] prevent[s] brakes from locking up and skidding by regulating hydraulic pressure."[4]

The ECUs in a vehicle perform their designated functions because they have been programmed to do so. Given this, a wide variety of customization, innovation, and repair activities that have traditionally been within reach of a vehicle owner now require access and modification of this computer code, including ECU firmware. 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.[5] Cars may be built for fuel optimization at sea level and run inefficiently at high altitudes unless adjustments are made.[6] The increasing prevalence of inter-vehicle communication may necessitate modification for drivers to travel without being tracked by their electronic signatures.[7] Certain repairs also necessitate firmware adjustments. For example, without access to ECU firmware, it may be impossible to operate a car after replacing engine components.[8]

Vehicle owners who tinker with their vehicles are engaged in a decades-old tradition of mechanical curiosity and self-reliance. The automobile aftermarket is remarkably robust, accounting for hundreds of billions of dollars in the United States alone.[9] Yet, because most automobile manufacturers deploy

---

[2] *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.

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

[4] *Id.*

[5] *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.

[6] *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.

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

[8] *Overview*, OPENXC, http://openxcplatform.com/overview/index.html (last visited Oct. 17, 2014).

[9] *Who We Are*, AUTOCARE ASSOCIATION, http://www.autocare.org/who-we-are (last visited Oct. 13, 2014) ("The Auto Care Association is the voice of the $300 billion plus auto care industry.")

measures to prevent access to ECU firmware and updates, vehicle owners are unable to access the firmware on their own vehicles without incurring legal risk under Section 1201(a)(1).

B. Copyrighted Works Sought to be Accessed

This petition seeks a limited exemption for computer programs that control the functioning of a vehicle or are intended to do so, including firmware and firmware updates. Computer programs are considered "literary works" under 17 U.S.C. § 102.

C. Technological Protection Measures

There are at least three technologies that prevent access to most ECU firmware and create a vast array of challenges for vehicle owners and hobbyists who wish to improve or alter the performance of their vehicle. The first includes a set of challenge-response mechanisms, involving access codes, passwords, keys, or digital signatures.[10] The second is encryption, which is used to restrict access both to firmware contained in certain vehicle ECUs and to firmware update files.[11] The third involves the disabling of access ports, such as "JTAG pins," on the circuitry.[12]

D. Noninfringing Uses

1. Fair Use

Vehicle owners who copy and modify vehicle-related software for legitimate purposes and distribute their findings are engaged in fair use. Similar exemptions have been granted in past rulemakings to allow owners of devices containing copies of software to adapt those copies to add new capabilities, when such uses do not harm the interest of the copyright owner.[13]

The first fair use factor is the purpose and character of the use. Vehicle owners tinkering with their vehicles are interested in the functional aspects of the code that controls vehicle systems. Research into the functioning of vehicle code is a fair use because it does not supplant the purpose of the original work, but rather advances a "further purpose or different character."[14] Specifically, access and disassembly of software that facilitates a greater understanding of the underlying technology is a

[10] *See, e.g.*, Volha Bordyk, *Analysis of Software and Hardware Configuration Management for Pre-Production Vehicles*, 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 Oct. 19, 2014); *Factory Locked ECUs*, REVO, http://www.revotechnik.com/support/technical/factory-locked-ecus (last visited Oct. 19, 2014).

[11] *Id.* 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.

[12] Charlie Miller and Chris Valasek, *Car Hackers' Handbook*, http://opengarages.org/handbook/2014_car_hackers_handbook_compressed.pdf, at pp. 56-60.

[13] Final Rule in RM 2008-8, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (July 27, 2010) ("2010 Rule") 75 Fed.Reg. 43825, 43830, *available at* http://www.copyright.gov/fedreg/2010/75fr43825.pdf (to be codified at 37 C.F.R. pt. 201).

[14] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1993).

fair use.[15] It is also necessary to allowing for interoperability between the vehicle and aftermarket components – both physical elements of the vehicle and software written by enthusiasts. Interoperability is a legitimate purpose recognized by appellate courts[16] and the Librarian of Congress.[17]

The nature of vehicle firmware weighs in favor of fair use under the second statutory factor because it contains "unprotected aspects that cannot be examined without copying."[18] 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.[19]

As for the third factor, copying the entirety of a work is fair use when proportionate to the legitimate purpose of the user.[20] In reverse engineering cases, use of an entire work is typically necessary and therefore fair.[21] Tinkerers' access and copying of the entire firmware within an ECU or an update is essential to understanding the functionality of a vehicle and determining how much storage capacity is available in the hardware for additional functionality.[22] This process requires the use of the entire work, since functionality may be found anywhere in the code and the technological process of reading the firmware off of the ECUs or decrypting an update typically provides the entire program, with no means to access merely a portion.

As for the fourth statutory factor, "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."[23] A tinkerer must purchase an entire car in order benefit from modifying and accessing ECU firmware. An exemption for car modifications and repairs would not decrease the

---

[15] *See Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510, 1522-23 (9th Cir. 1992) (holding that use of copyrighted material to study functional requirements was fair use).

[16] *See, e.g., Sony Computer Entm't v. Connectix Corp.*, 203 F. 3d 596, 606 (9th Cir. 2000) (enabling use of the copyrighted work on a new platform); *Sega*, 977 F.2d at 1520-28 (gaining access to platform for compatibility with independently-created games); *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 818-20 (9th Cir. 2003) (using copyrighted images as thumbnails in search engine); *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1163-68 (9th Cir. 2007) (reaffirming *Kelly*).

[17] 2010 Rule, 75 Fed.Reg. at 43830.

[18] *Connectix*, 203 F.3d at 603.

[19] *Sega,* 977 F.2d at 1526. *See also Connectix*, 203 F.3d at 605 ("If 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.").

[20] *See Kelly*, 336 F.3d at 820 (holding that third fair use factor did not weigh against copier when entire-work copying was reasonably necessary). *See also 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."); *A.V. ex rel. Vanderhye v. iParadigms*, LLC, 562 F.3d 630 642 (4th Cir. 2009) (holding that copying that is not "excessive or unreasonable" in relation to the purpose is fair).

[21] *See Sega,* 977 F.2d at 1527 (holding that wholesale copying of computer software is due greater deference); *Connectix*, 203 F.3d at 606 (reaffirming *Sega*). *See also HathiTrust*, 755 F.3d at 99 (holding that copying that is not "excessive or unreasonable" in relation to the purpose is fair).

[22] *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).

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

market for car purchases and may increase demand by introducing additional functionality.[24]

2. Section 117

Vehicle owners are further entitled to access, copy, and modify the vehicle firmware under Section 117 of the Copyright Act. An individual who owns a vehicle and the copy of the firmware embodied in an ECU conforms with Section 117 when extracting it for analysis.

E. Adverse Effects

Vehicle owners expect to be able to repair and tinker with their vehicles. A booming aftermarket industry relies on owners' having this capability,[25] and vehicle owners have traditionally been the source of countless automotive innovations.[26] But TPMs on ECU firmware block such legitimate activities,[27] forcing vehicle owners to choose between breaking the law or tinkering and repairing their vehicles.

In the BMW aftermarket, the presence of strong encryption 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.[28] For an individual vehicle owner, it would be impossible to design and manufacture custom ECU hardware and software in order to regain control of one's vehicle in the face of TPMs. Section 1201(a)(1) also chills research that might help individuals circumvent vehicle TPMs.[29]

Existing statutory exemptions are not adequate for a variety of reasons: tinkerers often do not have a sole purpose that fits one of the exemptions, the interoperability exemption refers to interoperability between computer programs (not physical systems such as replacement parts), rightsholders may argue that vehicle owners have not properly sought or obtained permission for their conduct, and tinkerers often wish to share information relevant to their work, which may weigh against them under the statutory exemption factors even without constituting a violation of Section 1201(a)(2). Additionally, the legal ambiguity and complexity of the exemptions make Section 1201's requirements a trap for the unwary.

III. Conclusion

For the reasons described above, the Librarian should determine that the non-infringing uses described herein are, and are likely to be, adversely affected by the prohibitions of Section 1201(a)(1), and therefore approve the proposed exemptions for the period 2015-2018.

---

[24] *See, e.g.,* Stephen Edelstein, *Best Cars to Modify: 10 Starting Points for the Ultimate Custom Car*, DIGITAL TRENDS (Mar. 18, 2014), http://www.digitaltrends.com/cars/best-cars-to-modify.
[25] *About SEMA*, SEMA, http://www.sema.org/about-sema (last visited Oct. 19, 2014).
[26] *See, e.g., Factory Locked ECUs*, *supra*.
[27] *Calibrating Automotive Electronics*, ETAS, http://www.etas.com/en/products/solutions_calibrating_automotive_electronics.php (last visited Oct. 28. 2014).
[28] *See* Lavrinc, *supra*.
[29] *See* Ishtiaq Rouf et al., *Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study*, USENIX SECURITY 2010 12 (2010).