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 researching the security or safety of such vehicles.*

I. The Commenting Party

The Electronic Frontier Foundation (EFF) is a member-supported, nonprofit, public-interest organization devoted to ensuring that copyright law promotes the progress of science and the arts, rather than stifling it. Founded in 1990, EFF represents tens of thousands of dues-paying members, including consumers, hobbyists, computer programmers, entrepreneurs, students, teachers, and researchers, who are united in their desire for a balanced copyright system that facilitates 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

[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.

like to test those vehicles for their own security and safety and the safety of others.

II. Proposed Exemption: Circumvention Necessary for Researching the Security and Safety of 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. If researchers can access the computer code within the ECUs, and within updates that will alter the functioning of that code, they can discover programming errors that endanger passengers, such as an error in the software that controlled the anti-lock braking system of the 2010 Toyota Prius.[5] They can also find errors that would allow a remote attacker to take control of a vehicle's functions.[6] Yet because most manufacturers deploy measures to prevent access to ECU firmware and updates, researchers are unable to access the firmware 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 researchers who wish to help enhance the security and safety of a vehicle's electronic systems. The first includes a set of challenge-response mechanisms, involving access

---

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

[6] Darlene Storm, *Untraceable $20 Device Can Allow Hacker to Control a Car 'From Miles Away'*, COMPUTERWORLD (Mar. 31, 2014, 5:57PM), http://www.computerworld.com/article/2476039/cybercrime-hacking/untraceable--20-device-can-allow-hacker-to-control-a-car--from-miles-away-.html.

codes, passwords, keys, or digital signatures.[7] The second technology is encryption, which is used to restrict access both to firmware contained in certain vehicle ECUs and to firmware update files.[8] The third involves the disabling of access ports, such as "JTAG pins," on the circuitry.[9]

D. Noninfringing Uses

1. Fair Use

The requested exemption is necessary to enable research and scholarship into vehicle security and safety. This research is an archetypical fair use codified in Section 107, undertaken to enhance public knowledge about the functioning of vehicles to which hundreds of millions of Americans trust their lives. Research and scholarship are purposes that are explicitly called out in Section 107 as supporting a finding of fair use, and access and disassembly of software that facilitates a greater understanding of the underlying technology has been recognized as a fair use.[10] A comparable exemption allowing "good faith testing for, investigating, or correcting security flaws or vulnerabilities" in video games was granted in the 2010 Rulemaking.[11] There, the Register found that "such good faith research constitutes fair use," noting the "socially productive purpose of investigating computer security and informing the public."[12]

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."[13] The Ninth Circuit has held 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.[14]

---

[7] *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).

[8] *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.

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

[10] *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).

[11] Final Rule in RM 2008-8, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (July 27, 2010) ("2010 Rule") 75 Fed.Reg. 43825, 43833-34, *available at* http://www.copyright.gov/fedreg/2010/75fr43825.pdf (to be codified at 37 C.F.R. pt. 201).

[12] *See id*. at 43834.

[13] *Sony Computer Entm't, Inc. v. Connectix Corp.*, 203 F.3d 596, 603 (9th Cir. 2000).

[14] *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.").

As for the third statutory factor, copying the entirety of a work is fair use when proportionate to the legitimate purpose of the user.[15] For reverse engineering, use of an entire work is typically necessary and therefore fair.[16] Vehicle security and safety research necessarily requires the use of the entire work, since vulnerabilities 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.

Finally, the fourth factor looks to direct harms on the market for the copyrighted work. This factor is concerned with the harm of market substitution, not any harm caused by substantive criticism of the copyrighted work.[17] 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."[18] As with the video game exemption granted in the 2010 Rulemaking, copying and distribution of vehicle-related software in the course of legitimate research is "unlikely to have an adverse effect on the market for or value of the copyrighted work itself."[19]

2. Section 117

Security researchers are further entitled to access, copy, and modify vehicle firmware under Section 117 of the Copyright Act. A researcher who owns a vehicle and the copy of the firmware embodied in an ECU conforms with Section 117 when extracting that firmware for analysis.

E. Adverse Effects

The research contemplated in this petition provides a critical public service by identifying potential vulnerabilities in vehicle safety. Such discoveries have been the focus of news reports and appeared on television to share their findings.[20] Researchers have demonstrated shortcomings in car networks' security,[21] prompting improvements by manufacturers.[22] They have even developed technology to protect drivers from flaws left open by manufacturers.[23] Researchers also investigate ECU firmware for bugs that impact the safety of vehicles on the road. These flaws are real,

---

[15] *See 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); *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.").

[16] *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.

[17] *See Campbell v. Acuff-Rose Music, Inc*., 510 U.S. 569, 591-92 (1993).

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

[19] 2010 Rule, 75 Fed.Reg. at 43834.

[20] *TODAY: Two experts demonstrate carjacking gone digital* (NBC television broadcast July 29, 2013) http://www.today.com/video/today/52609500#52609500.

[21] Andy Greenberg, *Hackers Reveal Nasty New Car Attacks—With Me Behind The Wheel*, FORBES (Aug. 12, 2013, 9:00AM), *available at* http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video.

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

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

dangerous, and shockingly common:[24] many high-profile recalls across a number of makes and models have been prompted by glitches in an ECU.[25]

Despite the importance of public security and safety auditing, vehicle manufacturers have generally not made car firmware publicly available. Independent vehicle security and safety research has been limited by the practical effect of TPMs. For example, out of twenty-seven locked ECUs examined by Valasek and Miller, they could only successfully inspect the firmware on two.[26] The legal cloud hanging over vehicle security research has also chilled publication of research results.[27]

Existing statutory exemptions are inadequate for a variety of reasons. For example, researchers often do not have a sole purpose that fits one of the exemptions, rightsholders may argue that vehicle owners have not properly sought or obtained permission for their conduct, and researchers 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 Software Glitches in the Auto Industry and What that Means for You*, PSC PROSERVICES, http://proservicescorp.com/auto-industry-software-glitches (last visited Oct. 17, 2014).

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

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

[27] *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, http://ftp.cse.sc.edu/reports/drafts/2010-002-tpms.pdf.