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

## Item 1. Commenter Information

Darin Bartholomew, Senior Intellectual Property Counsel
Global Intellectual Property Services
Deere & Company ("John Deere")
One John Deere Place
Moline, IL 61265

John Deere is a leading manufacturer of agricultural, construction and forestry equipment. John Deere employs engineers, software programmers and other experts to design and deliver high quality and innovative products with software that is subject to copyright protection. For example, John Deere equipment may have software that guides machines, controls engine behavior, or provides radio and other entertainment functions. Additional information is available at http://www.deere.com/en_US/regional_home.page.

## Item 2. Proposed Class Addressed

Proposed Class 21: Vehicle Software—Diagnosis, Repair, or Modification

## Item 3. Overview

Proposed Class 21 would allow "circumvention of TPMs protecting computer programs that control the functioning of a motorized land vehicle, including personal automobiles, commercial motor vehicles, and agricultural machinery,"[1] for the alleged "purposes of lawful diagnosis and repair, or aftermarket personalization, modification, or other improvement."[2] John Deere opposes the circumvention of TPMs for Class 21 because: (1) adequate diagnostic codes are already accessible to vehicle owners for diagnostic and repair purposes, without circumvention and without violating the vehicle manufacturer's copyrights in its software, or

[1] Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, Notice of Proposed Rulemaking, Fed. Reg. Vol. 79, No. 239, 73856, 73869 (Dec. 12, 2014).
[2] *Id.*

those of its suppliers; and (2) vehicle manufacturers, and their authorized dealers of parts and services already provide professionally developed software (or replacement electronic modules that contain the software) that are compliant with federal laws and regulations and safety standards. Although John Deere does not manufacture vehicles subject to on-road EPA (Environmental Protection Agency) and NHTSA (National Highway Traffic Safety Administration) regulations, John Deere's comments here cover on-road vehicles because of the breadth of the proposed exemption. John Deere's comments are limited to and solely provided for the purpose of copyright rule-making for Proposed Class 21, and for no other purposes.

The stated purpose for Class 21 is overly broad and goes beyond repair or diagnosis by explicitly referencing "aftermarket personalization, modification, or other improvement."[3] The unintended consequences of circumventing the TPMs are different than the alleged purposes referenced above in Class 21. Circumvention of the TPMs for Class 21 will make it possible for pirates, third-party software developers, and less innovative competitors to free-ride off the creativity, unique expression and ingenuity of vehicle software designed by leading vehicle manufacturers and their suppliers. For example, in the absence of TPMs third-party software developers could purchase vehicles to access instantly copyrighted, safe and regulatory-compliant software that is the result of years of extensive research and development by manufacturers and suppliers. In some vehicles as later explained herein, TPMs protect various creative software tools with imaginative interfaces or user-configurable interfaces, where such vehicle software would be vulnerable to copying in the absence of TPMs.

Moreover, TPMs for vehicle software for entertainment systems protects copyright owners of copyrighted content against the unauthorized reproduction and distribution of copyrighted works. For example, vehicle software for entertainment systems supports the playing of copyrighted music files and copyrighted audio books, among other expressive works. A vehicle driver may listen to sound recordings, while passengers may watch or view television and movie content. TPMs for in-vehicle entertainment systems encourage content providers to create and distribute highly-expressive copyrighted works that might otherwise be easily copied or pirated if the TPMs were circumvented. Consequently, circumvention of the above TPMs for purposes of "personalization, modification, or other improvement" is likely to encourage the unauthorized reproduction, distribution, and use of copyrighted software and content.

[3] *Id.*

The fundamental principle of our nation's copyright laws is to provide authors with exclusive rights in their works to create the incentive necessary to foster the development and distribution of works for the public's benefit.[4] The Copyright Office should not use its regulatory authority to facilitate myopic circumvention of TPMs, which would encourage the unauthorized copying and use of copyrighted software and related trade secrets of vehicle manufacturers and their suppliers.[5] Accordingly, allowing circumvention of the TPMs for copyrighted vehicle software will not accomplish the alleged purpose of Class 21, but will only further erode copyright protection in the U.S. compared to other jurisdictions on anti-circumvention of computer programs.[6]

Article 11 of the WIPO Copyright Treaty, adopted in Geneva on December 20, 1996, provides "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."[7] The United States signed the WIPO Copyright Treaty on April 12, 1997, ratified the treaty on September 14, 1999 and became effective on March 6, 2002.[8] To comply with Article 11 the Copyright Office should use its exemption authority cautiously and sparingly under Section 1201 to protect copyright holders and businesses in the U.S. against piracy and unauthorized copying of copyrightable vehicle software programs. Vehicle software programs that are subject to strong copyright protection, including TPMs, can allow creative and innovative manufacturers to differentiate their vehicles from global competitors.

Circumvention of TPMs for Class 21 is against public policy because individual vehicle owners do not have the technical resources to provide safe, reliable and lawful software for repair, diagnosis, or some dubious "aftermarket personalization, modification, or other improvement" that is not directed toward repair or diagnosis of the vehicle. TPMs protect access

---

[4] See, e.g., U.S. Constitution, art. I, sec. 8, cl. 8.
[5] See, e.g., U.S. Constitution, art. I, sec. 8, cl. 8.
[6] See., e.g., Section 296, Copyright, Designs and Patent Act 1988 (United Kingdom).
[7] WIPO Copyright Treaty, available at http://www.wipo.int/treaties/en/text.jsp?file_id=295166#P87_12240; Fed. Reg. Vol. 65, No. 209, 64556 (Oct. 27, 2000).
[8] WIPO Chart of Treaties, available at http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=16 .

to copyrighted software code that ensures compliance with governmental rules and industry safety standards. Vehicles and vehicle software are regulated by other federal government agencies, besides the Copyright Office, and are subject to voluntary compliance with industry safety standards. For example, programmers of certain vehicle software can use elaborate technical tools to test vehicle software for the Environmental Protection Agency's vehicle emissions compliance or industry safety standards. Therefore, the Copyright Office is respectfully requested to show regulatory deference to the other federal government agencies (and the self-regulatory, industry safety standards defined by technical experts) by leaving the TPMs in place for Proposed Class 21. Further, the Register is encouraged to consult with other federal government agencies, including the EPA, as part of the rulemaking process prior to deciding the outcome of Proposed Class 21.

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

Technical Protection Measures (TPMs) may include security handshakes, passwords, keys, cryptographic keys, codes, encryption or other technical security mechanisms to restrict access to copyrighted software owned by vehicle manufacturers, their suppliers or their licensors.

**Item 5. Asserted Non-infringing Use(s)**

In contrast to the seemingly benign stated purpose of the proposed exemption, the practical effect of circumventing the TPMs at issue will stifle creativity and innovation for vehicle software. Third-party software developers, pirates, and competing vehicle manufacturers will be encouraged to free-ride off the creativity and significant investment in research and development of innovative and leading vehicle manufacturers, suppliers and authors of vehicle software. The beneficiaries of the proposed exemption will not be individual vehicle owners who allegedly want to repair, redesign or tinker with vehicle software, but rather third-party software developers or competing vehicle manufacturers who—rather than spending considerable resources to develop software from scratch—instead would be encouraged to circumvent TPMs in order to make unauthorized reproductions of, and derivative works based on, the creativity of others. This perverse result of the circumvention is in direct conflict with the goals of our nation’s copyright laws, which reward authors for their creative expression by

restricting precisely these types of unauthorized activities. This result also is inconsistent with the copyright laws of other countries. For example, the U.K. software industry suggested that software piracy could be reduced by at least one third from adoption of harmonized rights, including technological protection measures, consistent with the EC Directive 2001/29/EC on May 22, 2001 on Harmonization of Certain Aspects of the Copyright and Related Rights in the Information Society.[9]

**The Proponents of the Exemption Have Not Met Their Burden of Establishing That The Proposed Uses Would Be Non-infringing.**

There is no material non-infringing use of the vehicle software that can be achieved by eliminating the prohibition on circumvention of the TPMs for the vehicle software under Section 1201. A vehicle owner does not acquire copyrights for software in the vehicle, and cannot properly be considered an "owner" of the vehicle software.[10] For example, certain software in the vehicle may be subject to click-wrap, shrink-wrap, or other software licenses that are granted at the time of sale or upon registration of the vehicle at a website of the vehicle manufacturer or its licensors. Manufacturers also may have electronic displays in the vehicles that display licenses to the purchasers or end users of the vehicles and that require acceptance of the software or return of the associated software and hardware that is subject to the proposed license.

In some cases, the manufacturer of the vehicle may not have title or ownership interest in the software and can transfer no more rights than the manufacturer has. For example, the vehicle owner may license software from one or more suppliers of components or licensors of software. If the manufacturer elects to use open-source software in the vehicle, the vehicle software may be subject to the restrictions of various third-party, open source licenses.[11] In the absence of an

---

[9] Copyright Directorate, The Patent Office Department of Trade and Industry, EC Directive 2001/29/EC on Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, Consultation Paper on Implementation of the Directive in the United Kingdom at 59 (para. 4.1 of Annex C)(7 August 2002).

[10] Analogously, the purchaser of a book does not receive ownership of the copyright in the materials (e.g., songs, images, drawings, text) disclosed in the book.

[11] Licence Agreement Supplement, Mercedes Benz available at http://moba.i.daimler.com/bai-cars/ba/foss/content/en/assets/FOSS_licences.pdf . If the open source license requires disclosure of source code, such obligations can be met typically by providing a storage medium, such as an optical disc, loaded with the open source software, rather than providing live read access to any

express written license in conjunction with the purchase of the vehicle, the vehicle owner receives an implied license for the life of the vehicle to operate the vehicle, subject to any warranty limitations, disclaimers or other contractual limitations in the sales contract or documentation. Even if TPMs for the vehicle software did not exist, accessing the vehicle software in contravention of these licenses could violate copyright, trade secret, or contractual rights of the vehicle manufacturer, its suppliers, or its licensors.

Significantly, such access would not be justified under the doctrine of fair use, which considers the following four statutory factors: (1) the purpose and character of the use, (2) the nature of the copyrighted work, (3) the amount and substantiality of the portion used, and (4) the effect of the use upon the potential market for or value of the copyrighted work.[12]

**1. The purpose and character of the use frustrates compliance with federal public safety and environmental regulations.**

The first fair use factor weighs against a finding of fair use because the purpose and character of the use will encourage non-compliance with environmental regulations and will interfere with the ability of manufacturers to identify and resolve software problems, conduct recalls, review warranty claims, and provide software version upgrades. Here, circumvention of TPMs is likely to impede manufacturers from reporting recall information that identifies and resolves software problems because of the confusing influence of third-party software and interloping modifications of the original vehicle software.

The record here is clear that the proponents are primarily individual hobbyists and "enthusiasts" who desire to "tinker" with and "hack" the vehicle software to, for example, "modify their engine controllers," "rac[e] on private courses," "make sure the lights turn on when the windshield wipers activate," "or to cap the speed when they lend the car to their teenage children."[13] Consequently, rather than using the vehicle firmware "for precisely the purpose for which it was designed," here the firmware in many cases is being used to undermine

---

subset of the vehicle software actually installed on the vehicle that is implicated by open source obligations.

[12] 17 U.S.C. § 107.

[13] EFF Comments, at 1, 6.

or reverse the purposes for which it was intended.[14] As explained in greater detail below, circumvention of the TPMs means that the vehicle software will be subject to contamination from the repair or modification efforts of individual vehicle owners, the vast majority of whom do not have programming or technical competence in the full range of applicable federal regulations and industry standards.

Contrary to Electronic Frontier Foundation's (EFF's) assertions, applying the holdings of the *Sega* and *Connectix* decisions to support a finding of fair use would be inappropriate here.[15] Significantly, in both *Sega* and *Connectix*, the defendants' resulting software programs did not themselves infringe plaintiffs' copyrighted material or use modified versions of the console's firmware. Rather, in each case, the defendants disassembled plaintiffs' copyrighted computer program in order to gain an understanding of the unprotected ideas and functional elements that were embodied in the copyrighted work so that the defendants subsequently could write their own original computer programs that did not contain any of plaintiff's protected computer code. Here, the record does not establish that the desired copying (and modification) of the vehicle software would be intermediate or transient. Instead, it appears that every time the individual would operate his or her hacked vehicle, the modified firmware would be copied and used in a slightly altered form.

Consequently, this factor weighs against a finding of fair use.

**2. The second factor weighs against a finding of fair use because the copyrighted software contains expressive elements and, in any event, facilitates compliance with federal law, rules, and industry standards.**

Although the vehicle software is to some degree functional in nature, it does include creative elements as well. Significantly, unlike in past triennial rulemaking proceedings considering jailbreaking of wireless telephone handsets—where the Copyright Office expressed concern that handset manufacturers used TPMs to protect restrictive business models—the TPMs

[14] *See* Recommendation of the Register of Copyrights, Fifth Triennial Proceeding, at 72 (Oct. 2012) (concluding that the first factor weighed in favor of fair use for jailbreaking wireless telephone handsets in large part because the firmware was used for the same purposes for which the firmware was designed).

[15] *See, e.g.*, *Sega Enterprises Ltd. v. Accolade, Inc*., 977 F.2d 1510 (9th Cir. 1992) (holding that using copyrighted material to study functional requirements was fair use); *Sony Computer Entm't Inc. v. Connectix Corp*., 203 F.3d 596 (9th Cir. 2000).

used to protect vehicle software deter the infringement of creative software programs. Further, here TPMs may be related to public safety, environmental protection, or both. As explained herein, in some cases these TPMs are required by or are utilized to comply with federal laws, regulations, and industry standards. Consequently, any weight to be given to this factor under the circumstances should be slight.

**3. The third fair use factor weighs against a finding of fair use.**

EFF concedes that circumvention of the TPMs protecting vehicle software would result in the reproduction and use of all of the copyrighted software.[16] Vehicle manufacturers employ skilled programmers not only to develop innovative software code that complies with governmental rules and safety standards, but to develop creative software that enhances the vehicle cabin environment and aesthetics, such as operator-adjustable engine exhaust sound[17] and other operator-customizable settings for various vehicle features.[18] Vehicles with entertainment system software and ancillary features, such as Bluetooth wireless interfaces for audio, support the playing of copyrighted music files and copyrighted audio books, among other expressive works.[19] TPMs for in-vehicle entertainment systems encourage content providers' creation and distribution of highly-expressive copyrighted works (e.g., musical works, sound recordings, television content, and movies) that might otherwise be easily copied or pirated.[20] Some agricultural vehicles support the use of various creative software tools with imaginative

[16] *See* EFF Comments, at 10.
[17] For example the 2013 Audi A7 allows adjustment of the exhaust sound. http://www.cnet.com/products/2013-audi-s7/2/.
[18] Lexus RC350 Brochure, available at http://www.lexus.com/pdf/service/15RC350-With-Display-Audio-customer.pdf.
[19] For example, John Deere offers certain sound systems that can read USB and SD cards, can play CD-R/CD-RWMP3 and WMA formats, and can support Bluetooth for interfacing with smartphones.https://www.deere.com/en_NAF/parts/agriculture_parts/tractor_parts/cab_comfort/cab_comfort.page. Similarly, Delphi Automotive LLP offers AM/FM Satellite Receivers with Bluetooth for off-road and on-road vehicles. http://www.delphi.com/docs/default-source/old-delphi-files/34b6470e-78d0-4514-99d5-cfed0b25298c-pdf.pdf?sfvrsn=0.
[20] *See, e.g.*, *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 321-323 (SDNY 2000).

interfaces or user-configurable interfaces.[21] Such vehicle software would be vulnerable to copying in the absence of TPMs. Consequently, this factor weighs against a finding of fair use.

**4. Circumvention would have an adverse effect on the potential market for and value of the copyrighted work.**

The alleged fair use will cause significant impairment to the market or potential market for the vehicle software and the secondary market for new and used vehicles. As explained herein, even a well-intentioned, but unskillfully applied hack to an automotive vehicle's software can threaten the safety of the driver of a vehicle, other drivers, and pedestrians. The risks of vehicle problems significantly increase if these hacks inadvertently or intentionally create security vulnerabilities that enable the installation of viruses, Trojan Horses, and other malicious software. Just a few publicized incidents could irreversibly diminish the public's trust in the safety and security of their vehicles, thereby diminishing consumer demand for new vehicles with enhanced features that are perfectly safe when protected by TPMs but that may be perceived as being more susceptible to hacking if the proposed exemption is granted.

In particular, the impact on the market for used cars is likely to be adversely impacted. Consumers looking to purchase a used car will be fearful that the previous owner could have tinkered with or hacked the vehicle in ways that could cause it to perform in unexpected ways, or, worse, have introduced viruses and malware into the vehicle's systems.

For the above reasons, because the proponents have not established that the proposed uses are non-infringing, the Copyright Office should deny the requested exemption.

[21] *See, e.g.*, John Deere, GreenStar™ 3 2630 Display, available at https://www.deere.com/en_US/products/equipment/ag_management_solutions/displays_and_receivers/greenstar_3_display_2630/greenstar_3_display_2630.page#viewTabs; GreenStar™ Ag Management Solutions from John Deere Brochure available at http://www.deere.com/en_US/docs/html/brochures/publication.html?id=dcbf8dee#6 .

**Item 6. Asserted Adverse Effects**

**There are commercially available alternatives to the asserted non-infringing use(s) without the need for circumvention. TPMs do not impede repair or access to diagnostic codes on vehicles.**

Most repairs for vehicles, such as automotive vehicles, do not relate to software, but to mechanical components.[22] For automotive vehicles, the most common repairs remove aftermarket alarms; replace intake manifold gaskets, ignition coils, exhaust gas recirculation valves, spark plugs, mass air flow sensors, catalytic converters, and oxygen sensors; and remedy loose fuel caps.[23] None of these repairs require circumvention to access controls on vehicles. For example, On-Board Diagnostic (OBD) II codes are available for diagnosing problems with the mass air flow sensor and oxygen sensor on most automotive vehicles, among the most common repairs.

Most recent on-road vehicles provide diagnostic codes through OBD II ports that can be read by scan tools or readers.[24] The Clean Air Act required all 1996 and later on-road, light-duty vehicle and trucks to be equipped with OBD II systems.[25] Since 2004, the EPA required medium-duty, on-road vehicles up to 14,000 pounds be equipped with OBD II systems.[26] "The OBD II system monitors virtually every component that can affect the emission performance of the vehicle to ensure that the vehicle remains as clean as possible over its entire life, and assists repair technicians in diagnosing and fixing problems with the computerized engine controls. If a problem is detected, the OBD II system illuminates a warning lamp on the vehicle instrument panel to alert the driver. This warning lamp typically contains the phrase Check Engine or Service Engine Soon. The system will also store important information about the detected malfunction so that a repair technician can accurately find and fix the problem."[27] Many on-road

---

[22] Jeanine Skowronski, The Ten Most Common Car Repairs, October 13, 2011, available at http://www.mainstreet.com/slideshow/most-common-car-repairs.
[23] *Id.*
[24] http://www.epa.gov/obd/basic.htm; Arvon L. Mitcham, EPA, On-Board Diagnostic Hand-Held Scan Tool Technology, EPA420-R-00-017, October 2000, available at http://www.epa.gov/otaq/regs/im/obd/r00017.pdf.
[25] http://www.epa.gov/obd/basic.htm.
[26] *Id.*
[27] *Id.*.

vehicle diagnostic codes are consistent with published standards or commercially available documentation.[28]

For off-road vehicles, diagnostic codes can be read with commercially available readers via diagnostic ports or remotely through wireless communications. For example, JDLink™ software for recent John Deere vehicles can provide artistic, visual and graphical representations of diagnostics, machine settings and/or states (for wireless transmission) to various web-enabled devices of vehicle owners without any need for circumvention of the software.[29] Other agricultural vehicles already provide diagnostic codes to vehicle owners through in-cab displays.[30]

To the extent that software in control modules requires updating or replacement, a new or refurbished control module with new software can be supplied by the original equipment vehicle manufacturers, their suppliers, or after-market manufactures with the requisite resources and skills to comply with emissions regulations and safety regulations. From time to time, such replacements of control modules to update software for on-road vehicles are made pursuant to manufacturer recalls tracked by the National Highway Traffic Safety Administration (NHTSA).[31] In some circumstances, the vehicle owner can simply return his old control module with obsolete software to his parts retailer to receive a rebate (e.g., core fee or recycling fee) for the old control module. It is possible for the vehicle owner to update software on a do-it-yourself basis by replacement of an old control module with a new control module; where the vehicle manufacturer may recommend that the vehicle owner checks with the vehicle dealer to ensure the latest software or appropriate software version is loaded on the new control module. No circumvention of the TPM is required to service or upgrade software in the aforementioned manner.

---

[28] Standard parameter identifiers for OBD-II codes are defined by SAE J1979, for example; See, e.g., http://en.wikipedia.org/wiki/OBD-II_PIDs.

[29] http://www.deere.com/en_US/products/equipment/ag_management_solutions/information_management/information_management.page?.

[30] See, e.g., Operator Manual for John Deere S670 Combine, available at http://manuals.deere.com/omview/OMHXE29687_19/?tM=.

[31] NHTSA Campaign No. 09V489000, Report Receipt Date December 23, 2009, Chevrolet Equinox and GMC Terrain 2010; NHTSA Campaign No. 07V227000, Notification Date June 5, 2007, International 9200I et al., 2007, available at http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues.

For many recent John Deere vehicles, the Service Advisor™ tool allows authorized technicians to access diagnostic trouble codes and to reprogram or update vehicle software with professionally developed code.[32] Similarly, the Service Advisor Remote™ (SAR) tool conveniently allows authorized technicians to access remotely diagnostic trouble codes and to reprogram or update remotely controllers on John Deere vehicles that are SAR-enabled and have adequate wireless service.[33] The above software updates are examples of commercially available alternatives for vehicle diagnosis and repair that eliminate the purported need for the proposed exemption.

**Item 7. Statutory Factors under 17 U.S.C. § 1201(a)(1)(C):**

**A. Availability for use of copyrighted works.**

As previously described, the vehicle software is commercially available for use under the terms and conditions of any applicable license or subject to any applicable purchase/sales agreement for a vehicle, for example. Upgrades of software are routinely provided by vehicle manufacturers, their software licensors, or their authorized suppliers, as explained above. Because the copyrighted work is commercially available without circumvention, the exemption is not required.

**B. Availability for use of works for nonprofit archival, preservation, and educational purposes.**

The purpose of the exemption for Class 21 is to diagnose, repair, personalize, modify or improve vehicle software,[34] rather than to use the work for nonprofit archival, preservation and educational purposes. The proponents primarily include individual hobbyists and "enthusiasts" who desire to "tinker" with and "hack" the vehicle software to, for example, "modify their engine controllers," "rac[e] on private courses," "make sure the lights turn on when the windshield wipers activate," "or to cap the speed when they lend the car to their teenage

[32] John Deere, *JDLink™/Service Advisor™ Remote Telematics System, Operator's Manual, Modular Telematics Gateway & Satellite Module*, OMPFP10493 Issue 10 at p. 36.
[33] *Id*.; John Deere, Service Advisor Remote product description, available at https://www.deere.com/en_INT/products/equipment/agricultural_management_solutions/jdlink_telematics/service_advisor_remote/service_advisor_remote.page; https://www.deere.com/en_CA/services_and_support/product_support/construction_technology_solutions/service_advisor_remote/service_advisor_remote.page
[34] Fed. Reg. Vol. 79, No. 239 at p. 73869.

children."[35] The proposed exemption does not cover any nonprofit archival purpose or preservation purpose of the vehicle software. Instead, "the circumvention would be allowed when undertaken by or on behalf of the lawful owner of the vehicle."[36] Because the proposed exemption is not limited to non-for-profit activity, the proposed exemption could be interpreted to allow for commercial use by the vehicle owner or on behalf of the vehicle owner. Accordingly, a use or publication that is "commercial as opposed to nonprofit is a separate factor that tends to weigh against a finding of fair use,"[37] and similarly weighs against authorizing circumvention under the analogous statutory factor of section 1201.

**C. Impact of TPM on criticism, comment, news reporting, teaching, scholarship, or research.**

This statutory factor tracks the language and appears to follow the reasoning associated with the judicially-created fair use doctrine that was codified in 17 U.S.C. § 107. Here, the TPMs protect access to vehicle software, and do not impede criticism, comment, news reporting, teaching, or scholarship. As for research, nothing in the proposed Class 21 exemption references using the vehicle software for research or educational purposes. Instead, research appears to be the intent of Class 22, which addresses circumvention for purposes of security research and was introduced by the same petitioner, EFF, as Class 21. Therefore, the above statutory factor does not support the proposed exemption.

**D. Effect of circumvention of technological measures on the market for or value of copyrighted works.**

The proposed exemption of the TPMs will have an adverse effect on the market for or value of copyrighted works in the vehicle. In particular, the impact on the market for used cars is likely to be adversely impacted. Consumers looking to purchase a used car will be fearful that the previous owner could have tinkered with or hacked the vehicle in ways that could cause it to perform in unexpected ways, or, worse, have introduced viruses and malware into the vehicle's systems, as explained herein.

---

[35] EFF Comments, at 1, 6.
[36] Fed. Reg. Vol. 79, No. 239 at p. 73869.
[37] *Harper & Row Publishers, Inc.. v. National Enterprises*, 471 U.S. 539, 562 (1985).

**1. The proposed exemption for Proposed Class 21: "Vehicle Software- Diagnosis, Repair or Modification" fails to meet the requirements of section 1201 based on public policy factors that are appropriate for the Librarian or Register to consider under 17 U.S.C. §1201(a)(1)(C)(v).**

Technical Protection Measures (TPM) on automobiles, commercial motor vehicles, and agricultural machines are in the public interest because, among other reasons: (1) TPMs for vehicle software do not impede the repair or access to diagnostic codes of vehicles, as discussed herein; (2) TPMs for vehicle software promote vehicle safety by allowing vehicle manufacturers to freeze reliable, stable software and to track and investigate software issues, where the NHTSA oversees such issues only for on-road vehicles, and (3) TPMs for vehicle software preserve air-quality by promoting compliance with EPA regulations on emissions.

This requested section 1201 exemption is entirely different than other exemptions that the Copyright Office previously has approved for portable electronic devices or cellular phones, such as jailbraking exemptions. Software used to control automobiles and off-road heavy equipment simply is not analogous to software in smartphones. While a smartphone may weigh only 4 ounces,[38] an agricultural machine can weigh over 44,000 pounds, which increases the potential impact of any circumvention-enabled software modifications.[39] The smartphone software might control an innocuous game (e.g., a digital Angry Bird game[40]), email, or a phone call. Meanwhile, the vehicle control software on an agricultural machine can control components such as an engine or steering of vehicle in motion. An agricultural machine can be equipped with a satellite navigation receiver (such as Global Positioning Systems, GPS) and auto-guidance software that automatically steers, controls speed and directs the machine in accordance with a path plan, such as parallel rows on a farm field.[41] A vehicle software system

[38] An Apple iPhone 5 smart-phone weights approximately 3.95 ounces (112 grams), available at https://www.apple.com/iphone/compare/.

[39] A John Deere S690 S-Series Combine, configured for corn without the header, weighs approximately 44,533 lbs. (or 20,200 kg.), available at http://www.deere.com/en_US/products/equipment/grain_harvesting/combines/s_series/s690/s690.page?.

[40] http://www.angrybirds.com/.

[41] John Deere Guidance and Machine Control, available at http://www.deere.com/en_US/products/equipment/ag_management_solutions/guidance/guidance.page?.

can be highly-complex and interdependent.[42] The Copyright Office should not authorize circumvention of TPMs that would expose critical control software of vehicles to unauthorized modification by the public because such unauthorized modification could pose a risk to public safety.

**2. TPMs promote vehicle safety by allowing manufacturers or the NHTSA to freeze reliable, stable software and to track and investigate software issues (e.g., recalls, warranty claims, and updates) for on-road vehicles.**

**A. On-road Motor Vehicle Safety Regulations**

Under the United States Code for Motor Vehicle Safety (Title 49, Chapter 301), "motor vehicle safety" is defined as "the performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident, and includes nonoperational safety of a motor vehicle."[43] An on-road vehicle manufacturer can conduct a "safety recall involving a motor vehicle or an item of motor vehicle equipment" independently or be "ordered by [the National Highway Traffic Safety Administration] NHTSA" to do so.[44] In either case, "the manufacturer must file a public report describing the safety-related defect or noncompliance with a Federal motor vehicle safety standard, the involved vehicle/equipment population, the major events that resulted in the recall determination, a description of the remedy, and a schedule for the recall."[45] NHTSA then "monitors each safety recall to ensure the manufacturers provide owners safe, free, and effective remedies according to the Safety Act and Federal regulations."[46]

NHTSA regulates vehicle security to protect vehicle owners of on-road vehicles. For example, one automotive manufacturer added tamper-proofing devices to vehicles to address an investigation of potential defects by the U.S. Department of Transportation.[47] NHTSA is also

---

[42] See, e.g., iFixit's Long-Form Comments, at 2.
[43] http://www-odi.nhtsa.dot.gov/owners/RecallProcess.
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] U.S. Department of Transportation, National Highway Traffic Safety Administration, Investigation PE 11-037, Post-Crash EV Fir Hazard for General Motors, 2011-2012 Chevy-volt http://www-odi.nhtsa.dot.gov/acms/cs/jaxrs/download/doc/UCM399396/INCLA-PE11037-

evaluating vehicle-to-vehicle communications (V2V) for collision avoidance "that can only work when participants in the system are able to trust the alerts and warnings issued by their V2V devices are based, at least in part upon information received from other V2V devices."[48] Accordingly, security measures such an asymmetric public key infrastructure (PKI) for encryption are under consideration.[49]

Although off-road manufacturers of agricultural machinery are not subject to NHTSA regulatory oversight for off-road vehicles, sometimes vehicle software in all vehicles can be susceptible to similar technical issues.[50] However, some differences in technical issues between off-road and on-road vehicles may exist because of the prevalence of diesel engine technology in off-road heavy equipment and voluntary compliance with different industry safety standards. As with on-road vehicle manufacturers, off-road vehicle manufacturers and regulators tend to track, to investigate and to manage various software technical issues, warranty claims from vehicle purchasers, and installed versions of software for many controllers on the vehicle that interact with each other.

In the context of automotive vehicles, Toyota has recalled certain Toyota Prius vehicles built during a four-year span to update software or to change a control module to prevent the vehicle from erroneously entering into a state that causes the vehicle to automatically shut down and enter a limp-home mode.[51] According to Toyota spokesperson, Shino Yamada, no injuries or accidents were reported because of the software issue with the Toyota Prius. Toyota also recalled other models to remedy a software issue that causes stability, anti-lock braking and

---

8445.PDF (tamper-proof device added to prevent vehicle owners from adding coolant to vehicle battery to reduce risk of fire).

[48] Department of Transportation, National Highway Traffic Safety Administration, Vehicle-to-Vehicle Security Credential Management System, Notice of Request for Information on Advanced Notice of Proposed Rule Making, dated August 18, 2014, available at www.safercar.gov/v2v/pdf/V2V-SCMS-RFI-Oct-2014.pdf.

[49] *Id.*

[50] Occasionally, off-road vehicle manufacturers, or their suppliers, can be subject to NHTSA regulatory authority if the off-road manufacturers, or their suppliers, supply engines or engine control units to manufacturers of on-road vehicles. *See*, e.g., NHTSA Campaign No. 07E024000, Report Receipt Date April 3, 2007, Certain Caterpillar C7 Diesel Engines installed on certain Freightliner Chassis, available at http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues.

[51] Hans Greimel, Toyota recalls Prius Models to Update Software, February 12, 2014, available at http://www.autonews.com/article/20140212/COPY01/302129954/toyota-recalls-prius-models-to-update-software.

traction controls to turn-off intermittently, while normal braking is present. If the Copyright Office approves the proposed TPM exemption, hackers or well-meaning, do-it-yourself vehicle owners would be enabled to alter engine controls, braking, steering or other functions on the vehicle that can result in severe public safety problems and injuries.

Proper programming of software by competent programmers with adequate technical resources and training, appropriate testing to comply with performance and safety standards, and installation of the software by skilled technicians can contribute toward avoiding or remedying problems with vehicle software. For example, a review of NHTSA campaign information shows that an automotive vehicle manufacturer modified the software in the powertrain control module to prevent damage to the intake manifold from back-firing and to minimize the risk of engine compartment fires.[52] In another instance, an on-road vehicle manufacturer modified electronic control module software on its vehicle to monitor the exhaust temperature sensor to avoid elevated exhaust temperatures and risk of fire.[53] Automobile manufacturers have also reported instances where improper software in the engine control module or powertrain control module can cause an engine to stall while driving[54] or where improper software for the electronic brake control module or traction control module can result in increased vehicle stopping distances.[55] Certain automobile manufacturers reported to NHTSA that the above issues can increase the risk of a traffic accident.[56] Even deficient software for control of a defroster or climate controls

[52] NHTSA Campaign No. 96V116000, Report Receipt Date July 1, 1996, Buick LeSabre and other models, 1996 and 1997, available at http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues.
[53] NHTSA Campaign No. 05V473000, Report Receipt Date October 12, 2005, Gillig Low Floor 2003-2004 and Phantom 2004, available at http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues.
[54] NHTSA Campaign No. 07V291000, Report Receipt Date July 3, 2007, Dodge Nitro and Jeep Wrangler 2007; NHTSA Campaign No. 97V228000, Report Receipt Date December 17, 1997, Mazda 626, 1998, available at http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues.
[55] NHTSA Campaign No. 97V064000, Report Receipt Date April 28, 1997, Buick Park Ave, Cadillac Deville, Cadillac Eldorado and Cadillac Seville, 1997, available at http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues.
[56] *Id.* and NHTSA Campaign No. 07V291000, Report Receipt Date July 3, 2007, Dodge Nitro and Jeep Wrangler 2007; NHTSA Campaign No. 97V228000, Report Receipt Date December 17, 1997, Mazda 626, 1998.

might impair visibility for a driver of an automobile.[57] The foregoing examples are merely illustrative of software issues that are tracked and addressed by vehicle manufacturers, regulators, or both to provide a safe vehicle environment for the public.

Vehicle manufacturers may use TPMs to control the versions of the software on the vehicle to facilitate recalls, updates, and installation of appropriate, reliable software; frequently with the technical benefits of statistically significant sample size of vehicles with same or uniform software. Meanwhile, consumers want to be able to purchase used vehicles with reliable software that has not been tampered with by hackers. For example, improper modifications to vehicle software can shorten vehicle longevity or lead to unpredictable vehicle operation. With the TPMs in force, the vehicle owner, repairman, manufacturer, and government regulators are assuaged that vehicle software on each vehicle is professionally developed and tested, even if the consumer is purchasing a used vehicle.

**B. Hacking and Third-Party Software**

On some vehicles, vehicle software controls the engine, brakes and other critical functions of the vehicle that can impact the safety of the vehicle operator.[58] Certain automobiles can be hacked wirelessly by computer experts or malicious individuals to control remotely any critical vehicle functionality.[59] The proposed TPM exemption facilitates hacking and the installation of third-party software or custom software into vehicles. This custom software could include viruses, Trojan horses, or other nefarious software that causes software problems; hence vehicle control problems.

For automotive vehicle manufacturers, custom software also may interfere with the ability of NHTSA to know whether a defect is caused by the manufacturer's original software in a vehicle controller or the hacker's software modification. TPMs restrict and discourage access in order to keep vehicle software stable and free of viruses, malicious software threats, and third party software. If the software has not been updated by third parties, the manufacturer can be

---

[57] NHTSA Campaign No. 09V489000, Report Receipt Date December 23, 2009, Chevrolet Equinox and GMC Terrain, 2010 (related to alleged noncompliance with Federal Motor Vehicle Standard 101 and 103) , available at http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues.
[58] http://www.pbslearningmedia.org/resource/nvsn6.sci.tech.carhack/car-hacking/ .
[59] *Id.* Various videos on car hacking are available at www.youtube.com by using search terms such as car, carjackers, attack, hack, hacking, and DARPA.

held accountable by regulators. However, if vehicle software contains third- party software and manufacturer's original software, the origin of a problem and the ability to address it are materially impaired. Accordingly, TPMs promote vehicle safety by allowing manufacturers and NHTSA to freeze reliable, stable software versions and track software, including in the event of a recalls.

### C. Industry Safety Standards

Automotive manufacturers, heavy equipment manufacturers, and their suppliers can voluntarily decide to follow various industry safety standards, unless regulations or laws mandate otherwise. The automotive industry uses a safety standard that is called ISO 26262, "Road vehicles-Functional safety." Under ISO 26262, an Automotive Safety Integrity Level (ASIL) refers to classification of safety goals by risk level and describes safety measures for accomplishing the safety goal or addressing the risk. In addition, IEC 62061, "Safety of machinery: Functional safety of electrical, electronic and programmable electronic control systems," applies to the automotive industry. IEC 62061 defines functional requirements and safety integrity requirements, where functional requirements include requisite response times, operating modes, and fault reaction functions.

ISO 25119, ISO-13849 and ISO-15998 apply to agricultural, construction and forestry equipment.[60] Accordingly, a vehicle manufacturer may design, specify, and test that their control systems are compliant with such safety standards, where appropriate. For example, an on-road vehicle manufacturer may purchase a controller that is certified to a certain safety standard, such as SIL3.[61] A hacker or vehicle owner who attempts to do his own repairs may be unaware that a software modification to a vehicle makes it non-compliant with a significant industry safety standard. A hacker or vehicle owner, who seeks to repair his vehicle generally

---

[60] Peter Els, Safety Standards govern modern off-road vehicle functional safety , available at http://www.functional-safety-nonroad.com/FormDownloadThankYou.aspx?target=http://www.functional-safety-nonroad.com/media/1000344/39918.pdf&eventid=1000344&m=39918#; Automotive IQ, Functional Safety for Non-road Vehicles Survey Results, available at http://www.functional-safety-nonroad.com/media/1000344/32985.pdf.

[61] Automotive IQ, Functional Safety for Non-road Vehicles Survey Results, available at http://www.functional-safety-nonroad.com/media/1000344/32985.pdf.

does not have the expertise to attain certification to applicable safety standards. Significantly, the proposed TPM exemption is overly broad in scope because even lawful software modification can be unsafe or inconsistent with applicable industry safety standards.

**3. TPMs promote compliance with EPA regulations on emissions and the environment.**

**A. Emissions Standards**

Under the Environmental Protection Agency's emission's standards, "[m]otor vehicle engines and off-road vehicles and engines must meet [Clean Air Act (CAA)] emissions standards," which "apply to cars, trucks, buses, recreational vehicles and engines, generators, farm and construction machines, lawn and garden equipment, marine engines and locomotives."[62] In addition to requiring "emissions labels for certified vehicles and engines," the CAA requires that "new vehicles and engines must have an EPA-issued certificate of conformity before import or entry into the United States demonstrating that the engine or vehicle conforms to all applicable emissions requirements."[63]

The CAA makes it unlawful "to manufacture, sell, or install a part for a motor vehicle that bypasses, defeats, or renders inoperative any emission control device."[64] The EPA has explained, for example, that:

> "computer software that alters diesel fuel injection timing is a defeat device. Defeat devices, which are often sold to enhance engine performance, work by disabling a vehicle's emission controls, causing air pollution. As a result of EPA enforcement, some of the largest manufacturers of defeat devices have agreed to pay penalties and stop the sale of defeat devices."[65]

Notably, EFF identifies the ability to "modify their engine controllers" as one of the specific purposes for which proponents desire to circumvent the vehicle TPMs.[66]

After-market suppliers already offer changes to engine control units to increase horsepower, torque or both based on lengthy test periods, with the risk that vehicle engines will

---

[62] Environmental Protection Agency (EPA) website at http://www2.epa.gov/enforcement/air-enforcement#engines.
[63] http://www2.epa.gov/enforcement/air-enforcement#engines.
[64] *Id.*
[65] http://www2.epa.gov/enforcement/air-enforcement#engines (emphasis added).
[66] EFF Comments, at 1, 6.

no longer comply with emission regulations.[67] The EPA may asses a civil penalty of up to $3,750 for any part that is knowingly manufactured, sold or installed that bypasses, impairs or defeats or disables the control of emissions of any regulated pollutant.[68]

Granting the proposed exemption could undermine the CAA, which "prohibits anyone from tampering with an emission control device on a motor vehicle by removing it or making it inoperable prior to or after the sale or delivery to the buyer."[69] It is worth emphasizing that a "vehicle's emission control system is designed to limit emissions of harmful pollutants from vehicles or engines."[70] The "**EPA works with manufacturers to ensure that they design their components with tamper-proofing**, addresses trade groups to educate mechanics about the importance of maintaining the emission control systems, and prosecutes cases where significant or imminent harm is occurring."[71] The EPA may audit manufacturers on test equipment, test records, and tamper resistance methods, among other things.[72] If the manufacturer seals adjustable parameters, the sealing method must provide a visual and "physical deterrence to tampering."[73] The engine certification process includes a review of engine test information and tamper resistance, among other things.[74] Individual vehicle owners that tamper with emission controls by changing software or otherwise can be fined up to $3,750 for each day the vehicle is in violation of emission standards, whereas dealers can be fined by to $37,500 for each day the vehicle is in violation of emission standards.[75] The EPA has attempted to estimate the increase of $NO_X$ emissions from tampering and mal-maintenance.[76]

---

[67] APR 2.0 TDI 140 HP Common Rail Diesel ECU Upgrade.
[68] 40 C.F.R § 1068.101(b)(2).
[69] http://www2.epa.gov/enforcement/air-enforcement#engines.
[70] *Id.*
[71] *Id.* (emphasis added).
[72] Certification Guidance for Heavy Duty On-Highway and Non-road CI Engines, 40 CFR Part 86 and Part 89, Section II, Paragraph C at p. 6, available at http://www.epa.gov/otaq/documents/nonroad-diesel/420b98002.pdf.
[73] *Id.* at Section II, Paragraph M.
[74] *Id.* at Appendix G and Appendix H.
[75] 40 C.F.R. § 1068.101(b)(1).
[76] United States Environmental Protection Agency, Development of Emission Rates for Heavy-Duty Vehicles in the Motor Vehicle Emissions Simulator Moves2010, Final Report, EPA-420-B12-049, August 2012 at p. 16, available at http://www.epa.gov/otaq/models/moves/documents/420b12049.pdf.

Most individuals (as vehicle owners) do not have the technical expertise, training, test equipment, staff, resources, or funding: (1) to repair properly vehicle software, (2) to test for emissions compliance, or (3) to verify safety of the resulting software in conformity with industry standards. Purchasers of vehicles with user-modified software may be unaware of previous modifications or repair that change the behavior or operation of vehicles, such as navigation for auto-guided tractors, throttle control, braking, steering, or otherwise, which poses a safety risk to vehicle operators and bystanders. Further, certain software modifications can reduce the longevity of vehicle components or the engine. Consequently, the proposed exemption should be denied.

**4. Potential or Actual Conflict Between the Agencies' Regulatory Authority Requires Deference By The Copyright Office.**

For on-road motor vehicles, the Department of Transportation and the NHTSA regulate vehicle software to protect public safety. On occasion, the NHTSA's regulatory activities have involved the addition of anti-tampering devices on automotive vehicles to protect consumers and the potential use of encryption security measures on communications between vehicles for collision avoidance. If the Copyright Office approves the above exemption to TPMs, the approval will thwart the ability of NHTSA to maintain uniform, safe software on makes and models of vehicles through the recall process. For example, the proposed TPM exemption facilitates the installation of custom software into on-road vehicles; the custom software may interfere with the ability of NHTSA, the manufacturer, or both to know whether a potential defect or recall issue is caused by the manufacturer's original software in a vehicle controller, or some software modification, virus, Trojan Horse, or malicious software from a hacker. For example, an on-road manufacturer may have difficulty in determining (and reporting to the NHTSA) whether a technical recall issue in a particular on-road vehicle controller arises from a change in software in the particular vehicle controller or another vehicle controller (e.g., with software modified pursuant to a TPM exemption) on a common vehicle data bus. Therefore, the Copyright Office should defer to NHTSA's regulatory need to manage or investigate software recall issues for on-road vehicles and should deny the proposed TPM exemption request.

Similarly, EPA regulations require the diagnostic codes (ODB II), ports, and readers for purposes of on-road emissions compliance, fuel economy and environmental regulation; such

diagnostic codes of on-road vehicles are within the regulatory authority of the EPA. The EPA has regulations that require manufacturers to have tamper-resistance with respect to emissions compliance. Accordingly, the EPA regulations appear to endorse the use of TPMs for purposes of tamper-resistance for emissions-related components of the vehicle. If the Copyright Office approves the above exemption to TPM, it could be in direct conflict with the EPA's ability to regulate and enforce emissions compliance on vehicles.

For these reasons, the Copyright Office is respectfully requested to defer to the regulatory authority of the NHTSA and the EPA where its activities would interfere with these other agencies' enforcement of existing regulations. Accordingly, the Copyright Office should not adopt the Proposed Class 21.

**5. Circumvention of Entertainment Systems on Vehicles Could Result in Unauthorized Piracy of Copyrighted Works and Create Security Risks**

Although circumvention of vehicle entertainment systems may not *appear* to pose the same risk to public safety, hacking of the wireless communications systems (e.g., cellular and Bluetooth) and vehicle data bus (e.g., Controller Area Network (CAN)) provide a potential security breach opportunity of vehicle control systems for nefarious hackers.[77] For example, a team of security experts could hack into the wireless communications system of the vehicle to upload software to flash the vehicle lights, unlock the doors, and start the engine to steal or control a vehicle.[78]

Notably, the vehicle manufacturer or software provider might provide software code updates for the vehicle owner or repair technician to upload to the entertainment module as long as the entertainment module does not contain any security flaws that allow unauthorized access to the vehicle data bus. Indeed, some vehicle manufacturers have voluntarily updated software for automobile entertainment systems. For example, Ford provided USB drives to certain vehicle owners to update the MyFord Touch infotainment and control system with improved touch screen and voice recognition to improve changing a radio station, adjusting the climate

[77] http://www.pbslearningmedia.org/resource/nvsn6.sci.tech.carhack/car-hacking/. Various videos on car hacking are available at www.youtube.com by using search terms such as car, carjackers, attack, hack, hacking, and DARPA.
[78] *Id.*

controls, or getting directions.[79] Microsoft and Ford apparently co-developed the MyFord Touch infotainment and control system.[80] Similarly, BMW lists software updates for certain vehicles equipped with a USB audio interface to support improvements (e.g., improved compatibility with various Smartphones, cellular phones or other devices).[81] These USB-based software updates from vehicle manufacturers of off-road and on-road vehicles are important marketplace alternatives that alleviate the need for the proposed exemption.

The proposed TPM exemption also is contrary to public policy because: (1) even lawful software modification can be unsafe or inconsistent with applicable industry safety standards, (2) the ability to circumvent TPMs exposes vehicle software to tampering and nefarious hacking, and (3) as explained above, these TPMs protect against unauthorized copying and distribution of copyrighted music, television, and film content. These risks are not outweighed by any need to repair, because rewriting software by a typical vehicle owner is not cost-effective, efficient, or practical. For these and the reasons described above, the requested exemption should be denied.

**Item 8. Documentary Evidence**

None enclosed.

[79] David Zax, A Software Update for Your Care?, Ford reboots infotainment system following consumer complaints, MIT Technology Review, available at http://www.technologyreview.com/videw/427153/a-software-update-for-your-car/.
[80] *Id.*
[81] BMW software update information is available at www.bmw.com/update; software update filename UPD05014.bin provided improved compatibility with various software devices.