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 22: Vehicle Software—Security and Safety Research

Item 3. Overview

Proposed Class 22 would allow circumvention of technical protection measures ("TPMs") "protecting computer programs that control the functioning of a motorized land vehicle"[1] for the specific "purpose of researching the security or safety of such vehicles."[2] John Deere opposes this exemption request because it could have the perverse and unintended effect of diminishing, rather than improving, vehicle safety and security. 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

[1] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Notice of Proposed Rulemaking*, 79 Fed. Reg. 73856, 73869 (Dec. 12, 2014) [hereafter, "*NPRM*"].
[2] *Id.*

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 22, and for no other purposes.

The safety and security of customers is the top priority at John Deere. John Deere developed formal product safety processes in the 1930's and continues to lead the industry with new product safety technology and training. Deere employees participate in organizations that set standards for agricultural machines and control systems. Product safety committees work to create and improve John Deere machines.

Although perhaps well-intentioned, Proposed Class 22 is likely to diminish, rather than improve, the security and safety of motorized land vehicles. As explained below, individual "enthusiasts" and "hobbyists" do not have the technical skills, experience, or knowledge to safely, reliably, and competently conduct such research without causing the vehicle to become susceptible to malicious attacks or erratic activity.[3] Indeed, the proponents' own evidence demonstrates that there is a significant likelihood that, in the process of attempting to conduct safety and security research on their vehicles, circumvention of the TPMs could cause the vehicle: (1) to act in unexpected ways or other ways that risk traffic accidents or personal injury, (2) to lack compliance with industry safety standards, (3) to violate vehicle emission regulations, and (4) to enable or exploit malicious attacks or security flaws in vehicle software. Because these individual automotive vehicle owners are likely to continue driving their vehicles after they (or someone else on their behalf) have circumvented the TPMs for their vehicle software, circumvention could harm not only the individual researchers but also other members of the public. As a result, the suggestion that granting the request would improve vehicle safety and security is not credible.

These concerns are particularly acute because the record in this proceeding establishes thousands of vehicle owners intend to use Proposed Class 22, if the exemption request is granted, to circumvent vehicle TPMs for purposes other than vehicle safety and security research. For

[3] While EFF states that "enthusiasts" discovered certain issues with vehicles shuddering and stalling, these issues appear to have been discovered through a review of existing engine control unit codes, rather than through circumvention and studying of the vehicle's copyrighted software programs. *See* Travis Okuliski, "Here's How To Fix The Scion FR-S and Subaru BRZ Engine's Idle Problem," *JALOPNIK* (Oct.2012), http://jalopnik.com/5948647/heres-how-to-fix-the-scion-fr-s-and-subaru-brz-engines-idle-problem.

example, nearly 2,000 individuals supporting the exemption for Proposed Class 22 indicate that vehicle software "should be 100% mine, to do as I want."[4] Another self-proclaimed "automotive enthusiast" supports Proposed Class 22 by describing how he modified his vehicle to "make the car go faster," how circumvention is necessary for car racing, and how "thousands" of individuals make their living in offering to the public circumvention services and tools (in clear violation of Section 1201(b) of the Digital Millennium Copyright Act).[5] Circumventing vehicle TPMs "to do as [the vehicle owner] wants" or to modify a vehicle for car racing clearly would not be permitted under Proposed Class 22, but the fact that individuals supporting this exemption apparently believe such activities would be allowed suggests that the "real world impact" of the exemption could be much broader, to the significant detriment of vehicle safety and security.[6] For these reasons, as well as those provided below, we request that the Register *not* recommend the requested exemption for Proposed Class 22.

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

TPMs that restrict access to copyrighted software owned by vehicle manufacturers or their suppliers may include security handshakes, passwords, keys, cryptographic keys, codes, encryption or other technical security mechanisms.

Significantly, these TPMs protect against the unauthorized reproduction and distribution of copyrighted works. For example, TPMs in 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.[7] In

---

[4] *See* Combined Comments (1816) Received Through Digital Right to Repair Website on Proposed Class 22.

[5] *See* EFF Comments on Proposed Class 22, Appendix A (Statement of David Blundell, Automotive Enthusiast).

[6] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 77 Fed. Reg. 65260, 65274 (Oct. 26, 2012) (stating that proponents have an "obligation to address the 'real world impact' of their proposed exemption").

[7] 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.

particular, a vehicle driver may listen to sound recordings, while passengers may watch or view television and movie content. TPMs for in-vehicle entertainment systems also encourage content providers' creation and distribution of highly-expressive copyrighted works that might otherwise be easily copied or pirated if the TPMs were circumvented.[8] In some agricultural vehicles, TPMs support the use of various creative software tools with imaginative interfaces or user-configurable interfaces,[9] where such vehicle software would be vulnerable to copying in the absence of TPMs. Further, TPMs protect access to copyrighted software code that ensures compliance with governmental rules and safety standards. Consequently, circumvention of these TPMs could have the unintended effect of encouraging the unauthorized reproduction, distribution, and use of copyrighted software and content.

Specifically, Proposed Class 22 could have the unintentional effect of encouraging a third-party software developer to conduct "research" of innovative—and otherwise safe and reliable—vehicle software programs in order to avoid funding years of its own research and development for competing products and services. This short-sighted result would encourage the unauthorized copying and use of copyrighted software and related trade secrets. Accordingly, allowing circumvention of the TPMs for copyrighted vehicle software tends to erode copyright protection in the U.S. instead of accomplishing the alleged purpose of Proposed Class 22.

Item 5. Asserted Non-infringing Use(s)

As a threshold matter, it is worth emphasizing that when an individual purchases a vehicle that person does not necessarily acquire copyrights for all the vehicle software and is not properly considered an "owner" of all such software. Rather, certain vehicle software is offered 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

[8] *See, e.g.*, *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 321-323 (SDNY 2000).

[9] *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 .

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 uses open-source software in the vehicle, the vehicle software may be subject to the restrictions of various third-party, open source licenses.[10] In the absence of an 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 therefore could violate copyright, trade secret, or contractual rights of the vehicle manufacturer, its suppliers, or its licensors.

Significantly, the practical effect of allowing the TPMs at issue here to be circumvented for purposes of "research" likely would be to stifle creativity and innovation for vehicle software. Third-party software developers and competing vehicle manufacturers and suppliers would be encouraged to free-ride off the creativity and significant investment in research and development of innovative and leading vehicle manufacturers and suppliers for vehicle software. This result 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.[11]

Significantly, the broad scope of Proposed Class 22 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]

---

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

[11] See, e.g., U.S. Constitution, art. I, sec. 8, cl. 8.

[12] 17 U.S.C. § 107.

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

The proposed exemption request is distinguishable from other circumstances where a limited exemption request was granted to enable research into known security vulnerabilities in at least one significant respect: unlike the short-term exemptions granted for sound recordings distributed in compact disc format and video games accessible on personal computers, allowing circumvention of TPMs protecting vehicle software would encourage non-compliance with safety and environmental regulations and interfere with the ability of manufacturers to identify and resolve software problems, to review warranty claims, and to provide software version upgrades.[13] Here, circumvention of TPMs is likely to impede on-road vehicle 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 a significant number of proponents are individual "enthusiasts" who desire to tinker with vehicle software out of curiosity or as a hobby.[14] Because these enthusiasts most likely would conduct research on the automotive vehicles they themselves own or automotive vehicles owned by other individuals consumers, the hacked vehicles would continue to be driven on public roads with contaminated computer software that may operate in violation of federal and state safety laws, industry safety standards, or emissions regulations.

Consequently, this factor should weigh against a finding of fair use.

---

[13] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 75 Fed. Reg. 43825, 43832 (July 27, 2010); Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 71 Fed. Reg. 68472, 68477 (Nov. 27, 2006).

[14] *See* EFF Comments on Proposed Class 22, at Appendix A (Statement of David Blundell, Automotive Enthusiast), Appendix C (Statement of Craig Smith, CEO of Theia Labs and Founder of Open Garages).

2. The copyrighted vehicle 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 includes creative elements as well. As explained above, the TPMs for vehicle software are used to protect against the infringement of creative software programs. Vehicle manufacturers employ skilled programmers not only to develop innovative software code that complies with governmental rules and safety standards, but also to develop software that enhances the vehicle cabin environment and aesthetics, such as operator-adjustable engine exhaust sound[15] and other operator-customizable settings for various vehicle features.[16] 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. 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 for backseat viewing) that might otherwise be easily copied or pirated.[17] Some agricultural vehicles support the use of various creative software tools with imaginative interfaces or user-configurable interfaces,[18] where such vehicle software would be vulnerable to copying in the absence of TPMs. The TPMs here may be related to public safety, environmental protection, or both as explained later in this document. Consequently, this factor should be given little weight under the circumstances.

[15] For example the 2013 Audi A7 allows adjustment of the exhaust sound. *See* http://www.cnet.com/products/2013-audi-s7/2/.

[16] Lexus RC350 Brochure, available at http://www.lexus.com/pdf/service/15RC350-With-Display-Audio-customer.pdf.

[17] *See, e.g.*, *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 321-323 (SDNY 2000).

[18] *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.

3. The third fair use factor weighs against a finding of fair use because the entire work is copied and used.

Electronic Frontier Foundation (EFF) concedes that circumvention of the TPMs protecting vehicle software would result in the reproduction and use of all of the copyrighted software.[19] 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. Even a well-intentioned, but unskillfully applied hack, research modification or attempted circumvention to an automotive vehicle's software can threaten the safety of the driver of a vehicle, other drivers, and pedestrians. The risks of 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, introduced or invited viruses and malware into the vehicle's systems. For example, vehicle research could include intentionally introducing and attempting to remove malware from vehicle software on used vehicles that are later resold to the unsuspecting public.

Because the proponents have not established that the proposed uses are non-infringing, the Register should deny the requested exemption.

[19] *See id.* at 10.

Item 6. Asserted Adverse Effects

A. Circumvention Is Unnecessary Because There Are Ample Research Alternatives.

Vehicle manufacturers and suppliers already are fully participating with academics, consulting firms, government entities, and other interested parties to research the safety and security of vehicles. For example, the Society of Automotive Engineers (whose meetings are public) has formed a committee of manufacturers, suppliers, semiconductor manufacturers, security, and consulting firms to study potential security vulnerabilities for vehicles and to develop standards and techniques to prevent cyberattacks.[20] In addition, comprehensive research and testing currently is being performed in connection with the National Highway Traffic Safety Administration's ("NHTSA") study of vehicle-to-vehicle ("V2V") communications.[21] NHTSA, in close collaboration with research and development partners in private industry, have developed a Connected Vehicle Safety Pilot Program, which is part of a major scientific research program to support the development of safety applications based on V2V and vehicle-to-infrastructure communications systems, including measurement of how effective these safety applications are at reducing crashes and how real-world drivers respond to these safety applications in their vehicles.

The willingness of manufacturers and suppliers to participate in and support these important research efforts is not surprising. Vehicle manufacturers and suppliers have every incentive to support legitimate research into vehicle safety and security. Building consumer trust in the safety and security of their vehicles is not only the right thing to do, but also is critical to manufacturers' and suppliers' commercial success. In contrast, and as explained in more detail below, widespread circumvention of TPMs by individual vehicle owners, who engage in security "research" as a hobby, is a recipe for disaster and consumer distrust. Accordingly, the Register is respectfully requested to decline the invitation to encourage spontaneous, amateur or random

---

[20] *See* Comments of SAE International on Proposed Class 22.

[21] *See, e.g.*, U.S. Dep't of Trans. Nat'l Highway Traffic Safety Admin, *Vehicle-To-Vehicle Communications: Readiness of V2V Technology for Application* (Aug. 2014), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf; Federal Motor Vehicle Safety Standards: Vehicle-To-Vehicle (V2V) Communications, *Advance Notice of Proposed Rulemaking; Notice of Availability of Technical Report*, 79 Fed. Reg. 49270 (Aug. 20, 2014), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/V2V-ANPRM_081514.pdf.

research on the vehicle software, safety and security that is not sponsored by the government, educational institutions, nor the vehicle industry.

B. The Requested Exemption For Proposed Class 22 Would Significantly Diminish, Not Improve, Vehicle Safety And Security.

The scope of Proposed Class 22 is sweeping. *Every* lawful owner of a vehicle and *any* third party acting on behalf of such person would be permitted to circumvent the vehicle TPMs for the purpose of researching the security or safety of the vehicle, regardless of his or her skill level, experience, or knowledge of vehicle operation or vehicle software.

The record in this proceeding demonstrates that many of the individuals who are likely to take advantage of the requested exemption, if it is granted, are not skilled technicians or experienced researchers, but rather "enthusiasts" and "hobbyists."[22] Vehicle hacking and security research poses significant dangers for the individuals conducting the research and the public. For example, a hobbyist or enthusiast relying on the *2014 Car Hacker's Handbook*—which is cited in EFF's comments and is authored by Craig Smith, whose statement EFF submitted—receives the following instructions:

- "A lot of engine lights will probably flash and go crazy during this test. That's because there is a lot more going on than just unlocking the car door. Ignore all the blinking warning lights and follow the same method as before. Remember you have a much higher chance of collisions this time, so you may have to play and record more than before."[23]

- "The CAN Bus and its components are fault-tolerant, however, if you are fuzzing or replaying a large amounts of CAN data back on a live CAN bus network, bad things will happen. Don't panic! Some common problems and solutions: . . .

    - The car won't turn off! This is obviously a bad situation, although fortunately it's rare. Make sure you are not flooding the CAN Bus. If you are disconnected, then you will need to get to the fuses and start pulling until the car goes off.

[22] *See, e.g.*, EFF Comments on Proposed Class 22, at Appendix A (Statement of David Blundell, Automotive Enthusiast) and Appendix C (Statement of Craig Smith, CEO of Theia Labs and Founder of Open Garages (describing Open Garages as a network of "hobbyists").
[23] Craig Smith, *2014 Car Hacker's Handbook*, at 35, available at http://opengarages.org/handbook/2014_car_hackers_handbook_compressed.pdf.

    - While driving, the vehicle responds recklessly. The problem is that you are an idiot. If you must audit a moving vehicle put it off the ground or on rollers. Injecting random packets in a moving car is a bad idea."[24]

- "There is often a note that failing to stick to these parameters will have unpredictable results. This is exactly what we will take advantage of. There are lots of ways of introducing faults, including with clocks, power, temperature, and light. We will cover some here."[25]

Even skilled researchers can harm public safety when circumventing vehicle TPMs to conduct security research. Notably, the DARPA-funded researchers quoted in EFF's comments, Chris Valasek and Charlie Miller, reportedly crashed a vehicle through a home garage while conducting vehicle security research in 2012.[26]

Unlike publicly-funded researchers conducting security testing of vehicles in a controlled environment, individual vehicle owners are likely to continue driving their automotive vehicles after they (or someone else on their behalf) circumvent the vehicle's TPMs and engage in security testing of the vehicle software. This further increases the likelihood of automobile accidents resulting from erratic behavior or security vulnerabilities introduced as a result of the circumvention and subsequent modifications of the computer programs.

These concerns are compounded by the fact that thousands of proponents in this proceeding appear to interpret Proposed Class 22 to allow circumvention for activities well outside research for vehicle safety and security. For example, nearly 2,000 individuals supporting the exemption for Proposed Class 22 state that vehicles software "should be 100% mine, to do as I want."[27] In addition, EFF's comments include a statement from David Blundell, a self-proclaimed "automotive enthusiast" who describes how he modified his vehicle to "make the car go faster," how circumvention is necessary for car racing, and how "thousands" of individuals make their living offering circumvention services and tools to the public, apparently

---

[24] *Id.* at 38.
[25] *Id.* at 58.
[26] Andy Greenberg, "DARPA-Funded Researchers Help You Learn To Hack a Car For a Tenth the Price," *Forbes* (Apr. 8, 2014), http://www.forbes.com/sites/andygreenberg/2014/04/08/darpa-funded-researchers-help-you-learn-to-hack-a-car-for-a-tenth-the-price/; *see also* EFF Comments on Proposed Class 22, Appendix B (Statement of Charlie Miller, PhD, Independent Security Researcher) and Appendix D (Statement of Chris Valasek, Director of Vehicle Security Research, IOActive).
[27] *See* Combined Comments (1816) Received Through Digital Right to Repair Website on Proposed Class 22.

in violation of Section 1201(b) of the Digital Millennium Copyright Act.[28] Circumventing vehicle TPMs "to do as [the vehicle owner] wants" and for car racing presumably would not be permitted under Proposed Class 22. But the fact that individuals supporting Proposed Class 22 apparently believe the exemption, if granted, would permit these other uses suggests that the exemption's "real world" harm to public safety and vehicle security could be substantial.[29]

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

A. Availability For Use Of Copyrighted Works.

The vehicle software is commercially available for use under the terms and conditions of any applicable license or subject to any applicable purchase or sales agreement for the vehicle. Because the copyrighted work is commercially available without circumvention, this statutory factor weighs against the requested exemption.

B. Availability For Use Of Works For Nonprofit Archival, Preservation, And Educational Purposes.

The purpose of Proposed Class 22 is expressly limited to "researching the security or safety of [motorized land] vehicles."[30] Consequently, the requested exemption would, by definition, not increase the availability of copyrighted works for nonprofit archival, preservation, or educational purposes.

C. Impact Of The TPM On Criticism, Comment, News Reporting, Teaching, Scholarship, Or Research.

Because the purpose of Proposed Class 22 is expressly limited to "researching the security or safety of [motorized land] vehicles," the requested exemption would, by definition, not affect criticism, comment, news reporting, teaching or scholarship. As discussed herein, although the stated purpose of Proposed Class 22 is purportedly for research, granting the requested exemption would be counterproductive because it would have the perverse effect of

[28] *See* EFF Comments on Proposed Class 22, Appendix A (Statement of David Blundell, Automotive Enthusiast).
[29] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 77 Fed. Reg. 65260, 65274 (Oct. 26, 2012) (stating that proponents have an "obligation to address the 'real world impact' of their proposed exemption").
[30] *NPRM* at 73869.

increasing, rather than decreasing, the risk of security vulnerabilities and accidents. The Proposed Class 22 calls for unrestricted and unqualified research by any vehicle owner, regardless of technical qualifications, funding, non-disclosure or publication obligations, or access to an off-road test track. For this reason, this statutory factor does not weigh in favor of the requested exemption.

D. Effect Of Circumvention Of Technological Measures On The Market For Or Value Of Copyrighted Works.

As explained above, Proposed Class 22 would have a significant adverse effect on the market for or value of copyrighted works in the vehicle. The market for used cars in particular 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.

E. Other Factors: The Register Should Reject Proposed Class 22 In Order To Facilitate Compliance With Safety Laws, Industry Safety Standards, And Environmental Regulations.

TPMs on automobiles and other motorized land vehicles vehicles promote vehicle safety by: (1) allowing manufacturers to freeze reliable, stable software and to track and investigate software issues (e.g., recalls, warranty claims, and updates) for on-road vehicles and to prepare applicable reports on recall information to the NHTSA, (2) encouraging conformity with industry safety standards, and (3) promoting compliance with EPA regulations on emissions. To facilitate these significant public policy benefits and avoid creating actual or potential conflicts with such legal requirements, we request that the Register not recommend the exemption for Proposed Class 22.

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

Under the U.S. Code for Motor Vehicle Safety, "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."[31] A manufacturer may conduct a "safety recall involving a motor vehicle or an item of motor vehicle equipment" independently or be "ordered by NHTSA" to do so.[32] 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."[33] 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."[34]

NHTSA regulates vehicle security to protect vehicle owners of on-road vehicles. For example, the addition of tamper-proofing devices to vehicles have been partially a response to investigations of potential defects in vehicles by the U.S. Department of Transportation.[35] NHTSA also is 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."[36] Accordingly, security measures such an asymmetric public key infrastructure (PKI) for encryption are under consideration for security, among other things.[37]

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

---

[31] *See* 49 U.S.C. § 30102(a)(8).
[32] *See* U.S. Dep't of Trans., Nat'l Highway Traffic Safety Admin., Process for Issuing a Recall, http://www-odi.nhtsa.dot.gov/owners/RecallProcess.
[33] *Id.*
[34] *Id.*
[35] U.S. Dep't of Trans., Nat'l Highway Traffic Safety Admin., *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-PE11037-8445.PDF (tamper-proof device added to prevent vehicle owners from adding coolant to vehicle battery to reduce risk of fire).
[36] U.S. Dep't of Trans., Nat'l Highway Traffic Safety Admin., Vehicle-to-Vehicle Security Credential Management System, *Notice of Request for Information on Advanced Notice of Proposed Rule Making* (Aug. 18, 2014), available at www.safercar.gov/v2v/pdf/V2V-SCMS-RFI-Oct-2014.pdf.
[37] *Id.*

susceptible to similar technical issues.[38] 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 manufactures tend to track, to investigate, and to manage various software technical issues for manufacturer recalls of software, 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.[39] 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 traction controls to turn-off intermittently, while normal braking is present. If the Copyright Office approves the proposed TPM exemption, researchers or 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

[38] Occasionally, off-road manufacturers of agricultural machinery can be subject to NHTSA regulatory authority if the off-road manufacturers supply engines or engine control units to manufacturers of on-road vehicles. *See*, e.g., NHTSA Campaign No. 07E024000, *Certain Caterpillar C7 Diesel Engines installed on certain Freightliner Chassis*, (Apr. 3, 2007), http://www-odi.nhtsa.dot.gov/owners/SearchSafetyIssues.

[39] 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.

compartment fires.[40] 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.[41] 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[42] or where improper software for the electronic brake control module or traction control module can result in increased vehicle stopping distances.[43] Certain automobile manufacturers reported to NHTSA that the above issues can increase the risk of a traffic accident.[44] Even deficient software for control of a defroster or climate controls might impair visibility for a driver of an automobile.[45] 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 researchers. 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

---

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] *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.

[45] 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.

are assuaged that vehicle software on each vehicle is professionally developed and tested, even if the consumer is purchasing a used vehicle.

Consequently, if the Register recommends Proposed Class 22, it likely will become more difficult for manufacturers to maintain uniform, safe software on makes and models of vehicles and for on-road vehicle manufacturers to report software issues to the NHTSA because vehicle software would be susceptible to a continuous state of flux from research modifications or attempted circumventions. Allowing a vehicle owner to circumvent the vehicle TPMs—even if for purposes of conducting security and safety research—would make it difficult to track and respond in the event of a vehicle recall and could result in unintended safety incidents that harm the vehicle operator, other drivers, or innocent bystanders.

2. TPMs Encourage Conformity With 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 can apply to agricultural, construction and forestry equipment.[46] 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

[46] 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.

standard, such as SIL3.[47] A researcher 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 researcher or vehicle owner, who seeks to repair his vehicle generally does not have the expertise to attain certification to applicable safety standards. The proposed TPM exemption is overly broad in scope because software modifications or circumvention for research purposes could deviate from applicable industry safety standards. Accordingly, circumventions of the TPMs for the proposed research purposes have the potential to further diminish the safety and security of the vehicle attendant with any deviations from industry standards.

3. TPMs Promote Compliance With EPA Emissions Regulations.

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."[48] 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."[49] 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."[50] Defeat devices can include computer software that alters fuel injunction timing.[51] 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.[52]

---

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

[48] Environmental Protection Agency (EPA), http://www2.epa.gov/enforcement/air-enforcement#engines.

[49] *Id.*

[50] *Id.*

[51] http://www2.epa.gov/enforcement/air-enforcement#engines.

[52] 40 C.F.R § 1068.101(b)(2).

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."[53] A "vehicle's emission control system is designed to limit emissions of harmful pollutants from vehicles or engines,"[54] and the "EPA works with manufacturers to ensure that they design their components with tamper-proofing."[55] The EPA may audit manufacturers on test equipment, test records, and tamper resistance methods, among other things.[56] If the manufacturer seals adjustable parameters, the sealing method must provide a visual and "physical deterrence to tampering."[57] The engine certification process includes a review of engine test information and tamper resistance, among other things.[58] Individual vehicle owners that tamper with emission controls 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.[59]

Most individuals (as vehicle owners) do not have the technical expertise, training, test equipment, or resources to test for emissions compliance or verify that the hacked vehicle software remains in conformity with industry standards. Consequently, the proposed exemption should be denied.

4. At A Minimum, The Register Should Narrow The Scope Of Proposed Class 22 To Certain Federal Government Labs And Universities.

If the Register concludes that proponents have satisfied their burden of demonstrating that circumvention for safety and security research is warranted, it is respectfully requested that, at a minimum, the Register narrow Proposed Class 22 to allow circumvention only by federal government labs and universities that conduct research on vehicle safety and security pursuant to a federal grant or federal contract.

---

[53] http://www2.epa.gov/enforcement/air-enforcement#engines.
[54] *Id.*
[55] *Id.*
[56] Certification Guidance for Heavy Duty On-Highway and Non-road CI Engines, 40 C.F.R. Part 86 and Part 89, Section II, Paragraph C, http://www.epa.gov/otaq/documents/nonroad-diesel/420b98002.pdf.
[57] *Id.* at Section II, Paragraph M.
[58] *Id.* at Appendix G and Appendix H.
[59] 40 C.F.R. § 1068.101(b)(1).

In the past, where proponents have "offered substantial and persuasive evidence" that an exemption is justified but the proposed class "is not fully congruent with the proponents' showing," the Register "has—to the extent a sufficient basis exists in the record—refined the class definition to ensure that it is appropriately tailored to her findings."[60] At this time, there does not appear to be a sufficient record "demonstrating that some version of [EFF's] exemption is warranted."[61] But if, based on proponents' reply comments or future testimony, the Register ultimately concludes that it can delineate narrower contours for the class, it is strongly urged that Proposed Class 22 be limited as described above in order to help ensure that circumvention of any vehicle TPMs is conducted solely by qualified individuals for legitimate research purposes.

Item 8. Documentary Evidence

None enclosed.

[60] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Final Rule*, 77 Fed. Reg. 65260, 65276 (Oct. 26, 2012)
[61] *Id.*