Hastings Business Law Journal

Volume 15
Number 1 *Winter 2019*

Article 5

Winter 2019

A Peek Under the Hood: Why Lawmakers Should Strengthen the Current DMCA Exemption for Security and Safety Research into Car Software

Holden Benon

A Peek Under the Hood: Why Lawmakers Should Strengthen the Current DMCA Exemption for Security and Safety Research into Car Software

Holden Benon *

In the last five years, society has witnessed advancements in automobile technology that Henry Ford himself could not have dreamed. Vehicle software now allows cars to drive themselves; indeed, as of October 2018, five dozen vehicle manufacturers have received permits from the California Department of Motor Vehicles for autonomous testing.[1] And recently, in a shocking revelation, vehicle software embedded in 11 million Volkswagen cars allowed these vehicles to deceive emissions tests and violate environmental regulations undetected.[2] The same way the American legal system was forced to adapt to the technological advancements of the early 20th century, unprecedented changes in road vehicles require governmental regulation to enhance road safety and limit pollution while striking a balance between the interests of consumers and auto manufacturers.

Many of the advancements in automobile technology involve copyright law, the primary body of law that protects computer source code.[3] Essentially, each line of vehicle source code is protected the same way a film script is protected. Just as camera directions in the script are

* A recent UC Hastings graduate, Benon now works in the litigation arm of Clyde & Co's San Francisco office. In his former role as a legal intern at the Electronic Frontier Foundation, he helped Staff Attorneys prepare for the 2018 DMCA review proceedings and matters concerning digital privacy, civil liberties, and copyright fair use. In his spare time, Benon enjoys cooking, traveling, and playing with his bull terrier, Dexter.

1. *See* Department of Motor Vehicles, *Information for Manufacturers Testing of Autonomous Vehicles* https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/permit, [https://perma.cc/8L9F-75VP].

2. *See* Jack Ewing, *Volkswagen says 11 Million Cars Worldwide are Affected in Diesel Deception*,(Sept. 22, 2015), https://www.nytimes.com/2015/09/23/business/international/volkswagen-diesel-car-scandal.html [https://perma.cc/M5BV-N8VD].

3. *See Computer Assocs. Int'l v. Altai*, 982 F.2d 693, 702 (2d Cir. 1992) ("It is now well settled that the literal elements of computer programs, i.e., their source and object codes, are the subject of copyright protection"); *Whelan Assoc. v. Jaslow Dental Lab., Inc.*, 797 F.2d at 1222, 1233; *CMS Software Design Sys., Inc. v. Info Designs, Inc.*, 785 F.2d 1246, 1247 (5th Cir. 1986); *Apple Computer, Inc. v. Franklin Computer Corp.*, 714 F.2d 1240, 1249 (3d Cir. 1983).

hidden from movie-goers, the source code underlying vehicle software is encrypted and given a second layer of protection through the Digital Millennium Copyright Act ("DMCA").[4]

Members of MIT's Media Lab have already begun conducting research into the safety ramifications of artificially intelligent cars.[5] Because researchers should be able to view the source code underlying the guidance systems for these cars, the DMCA exemption for vehicle software research leans toward the need for an open source philosophy, where licenses grant the ability to share source code in a nondiscriminatory way. With increased transparency comes decreased information costs that could arguably enhance roadway safety and decrease carbon in the atmosphere. Opponents of such an exemption for vehicle software research assert that open-sourcing this code could make the software vulnerable to cybersecurity attacks.

This article explores alternatives to the DMCA Triennial Review Process with a focus on the Class 22 Exemption for vehicle software research. By weighing corporate interests against those of the public, I suggest a refinement of section 1201's language that will inevitably benefit the public at large. Part one of this article explores two recent controversial case studies on vehicle source code. These case studies underscore the importance of creating an exemption for vehicle software research. Part two provides some background on the DMCA. Part three examines the Triennial Review Process, provides criticism of that process, and examines a case study on the Cell Phone Unlocking Exemption. Part four focuses on the Class 22 Vehicle Software - Security and Safety Research Exemption, and offers a proposal to strengthen this exemption.

I. RECENT CONTROVERSIES SURROUNDING CAR TECHNOLOGIES

In 2015, the Environmental Protection Agency ("EPA") advised against the exemption for circumvention of Technological Protection Measures ("TPMs") into car software, stating that it could lead to car owners tinkering with their software in ways that might violate the Clean Air Act.[6]

4. While the DMCA contains a wide variety of provisions, such as the anti-trafficking provision, and the notice and takedown provision, this article focuses on the anti-circumvention provision of the DMCA. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 CFR Part 201 (2015).

5. *See* MIT Media Lab, *Moral Machine*, http://scalable.media.mit.edu/#modalmm [https://perma.cc/X65G-WXXY].

6. *See* Letter from Geoff Cooper, Gen. Couns., EPA, to U.S. Copyright Off., Libr. of Cong. (July 17, 2015) *available at* https://copyright.gov/1201/2015/USCO-letters/EPA_Letter_to_USCO_re_1201.pdf [https://perma.cc/VU96-3GN4]; Kyle Wiens, *Opinion: the EPA Shot Itself in the Foot by Opposing*

Only two months later, independent researchers in West Virginia discovered that Volkswagen cars contained certain software that allowed them to deceive emission tests.[7] As it turned out, Volkswagen secretly programmed their vehicles' software to enable the vehicles to deceive emissions tests.[8] The software, however, instructed the vehicles to emit more pollutants during non-test driving.[9] This resulted in at least 11 million cars emitting nitrogen oxides at levels up to 40 times the standard proscribed by the Clean Air Act.[10] As a result of its actions, the EPA issued Volkswagen a notice that it was violating the Clean Air Act.[11] All of this resulted in a multi-billion-dollar settlement agreement reached between the EPA and Volkswagen.[12]

The Volkswagen emissions scandal demonstrates why vehicle software research is needed. Because Volkswagen obfuscated the source code using codewords such as "acoustic software" to confuse potential onlookers,[13] this instance illustrated the need for increased access into vehicle source code for good faith-testing. The Volkswagen case study exemplifies the need for the exemption to cover research conducted in good faith, but it also shows how far the DMCA's regulatory use has been stretched.

That semi-autonomous vehicles are already on our roads further demonstrates the need for a permanent exemption to the DMCA's anti-circumvention provision for good-faith testing into vehicle software. In California, companies can already apply for autonomous vehicle testing permits.[14] As of October 12, 2018, 60 companies have received permits, including Volkswagen Group of America, Mercedes Benz, Subaru, Faraday

Rules that Could've Exposed VW, (Sep. 25, 2015), http://www.theverge.com/2015/9/25/9397171/epa-dmca-volkswagen-diesel-scandal [https://perma.cc/4E8U-D6VK]; Stan Adams, *The EPA, the DMCA, and VW: Research, Not Copyright, Should Protect the Environment*, (Oct. 25, 2015), https://cdt.org/blog/the-epa-the-dmca-and-vw-research-not-copyright-should-protect-the-environment/ [https://perma.cc/4ZFX-LMTC].

7. Sonari Glinton, How a Little Lab In West Virginia Caught Volkswagen's Big Cheat (Sept. 24, 2015), http://www.npr.org/2015/09/24/443053672/how-a-little-lab-in-west-virginia-caught-volkswagens-big-cheat [https://perma.cc/3GDF-8HKT].

8. Environmental Protection Agency, *Learn About Volkswagen Violations*, https://www.epa.gov/vw/learn-about-volkswagen-violations [https://perma.cc/3GDF-8HKT].

9. *Id*.

10. *Id; See* Jack Ewing, *Volkswagen says 11 Million Cars Worldwide are Affected in Diesel Deception*, (Sept. 22, 2015), https://www.nytimes.com/2015/09/23/business/international/volkswagen-diesel-car-scandal.html [https://perma.cc/M5BV-N8VD].

11. Environmental Protection Agency, *supra* note 8.

12. *Id*.

13. Chris Ziegler, *Volkswagen Used Codewords to Conceal Diesel Emissions Cheating*, (Apr. 19, 2016). http://www.theverge.com/2016/4/19/11462456/volkswagen-code-words-investigation-diesel-emissions-scandal [https://perma.cc/2NHQ-BEPH]; Christoph Rauwald, *VW Says Diesel Emissions Fix Progress Makes Trial Unneeded*, (Apr. 18, 2016), https://www.bloomberg.com/news/articles/2016-04-19/vw-cheating-code-words-said-to-complicate-emissions-probe [https://perma.cc/8U2M-3L3M].

14. *See* Department of Motor Vehicles, *supra* note 1.

& Future, Tesla Motors, NVIDIA Corporation, and Wheego Electric Cars, Inc.[15] Autonomous vehicles, while touted to be safer than human drivers, will inevitably contain flaws.[16] For instance, in July 2016, a self-driving Tesla collided with a passing truck, resulting in the first-ever autonomous car fatality.[17] The vehicle, which was driving in autopilot mode, could not distinguish the white truck against a brightly lit sky.[18]

The 2016 Tesla collision highlights the difficulty faced by vehicle software developers to account for the vast number of uncertainties that exist on the road. Take the familiar scenario of a child running into the middle of a suburban roadway in pursuit of a soccer ball. Would an autonomous vehicle know to stop for the ball because a child is likely to follow? Vehicles may require individualized lines of code to instruct the vehicle to properly deal with nuanced situations such as this one: stop and wait for a child if the car recognizes a ball bouncing across a suburban street, but proceed without stopping if the same soccer ball escapes from the back of a pickup truck on a busy highway. Mike Regan, a researcher from the University of New South Wales, draws a comparison to aviation automation and how it has been known to fail.[19] He suggests that the autonomous vehicles industry will handle its programming the same way the aviation industry refined its autopilot system; each crash will usher in a wave of research aimed at preventing a reoccurrence.[20] Inevitably, he posits, after enough of these processes, these cars will be safer than the cars that we currently drive.[21]

This process of finding errors in real time and making immediate adjustments to the source code should not be confined to the research labs of each individual auto manufacturer. Running these crash-and-fix processes individually could needlessly multiply the number of accidents as each company will encounter these issues and solve them independently, and at their own pace. Hypothetically, if Toyota wrote the source code to properly handle the above soccer ball situation, it would best serve the public good if Toyota were to share that source code with Tesla, assuming Tesla had not yet written those instructions and had deployed autonomous

15. *Id.*

16. *See* Hal Hudson, *The Four Main Roadblocks Holding Up Self-Driving Cars*, (Feb. 11, 2015), https://www.newscientist.com/article/mg22530082-100-the-four-main-roadblocks-holding-up-self-driving-cars/ [https://perma.cc/5NPQ-PSRJ] ("Car Companies will probably pore over their software more intently than the average app developer, but they will still miss things.").

17. *See* Alice Klein, *Tesla Driver Dies in First Fatal Autonomous Car Crash in US*, (July 1, 2016), https://www.newscientist.com/article/2095740-tesla-driver-dies-in-first-fatal-autonomous-car-crash-in-us/ [https://perma.cc/262J-6YKR].

18. *Id.*

19. *Id.*

20. *Id.*

21. *Id.*

cars on the streets. To ensure road safety, this code should be shared among other car manufacturers and be made visible to independent third-party researchers. This is a realm where free software licensing would be the best solution, allowing for improvements to software to be implemented by all automakers.

Open sourced software for research purposes has yielded beneficial results in past situations.[22] MIT's Media Lab has recently been described as "a unique model in which a consortium of companies—many of them competitors—would fund the work and share all of the intellectual property."[23] In 2017, the Media Lab received a 27 million dollar grant from the Ethics and Governance of Artificial Intelligence Fund.[24] At the Media Lab, researchers engage in "unbiased, sustained, evidence-based, solution-oriented work that cuts across disciplines and sectors," and seek to advance public understanding of artificial intelligence.[25] In fact, the Media Lab is already exploring the moral complexities that can arise with respect to autonomous vehicles.[26] The "Moral Machine," a platform at MIT Media Lab, generates moral dilemmas, such as where a driverless car is forced to choose the lesser of two evils: killing five middle-aged passengers or two adolescent pedestrians.[27]

Resulting data from initiatives like the Media Lab should resemble the code that underlies self-driving cars. This requires a level of transparency that may only be possible if the Class 22 Exemption, or similar exceptions, continue to exist. Before autonomous vehicles begin to roll off the assembly line, independent researchers should have access to the underlying source code that will perform autonomous navigation. Accordingly, a clear-cut exemption to the DMCA's anti-circumvention provision is necessary.

II. THE DMCA ANTI-CIRCUMVENTION PROVISION PROTECTS COPYRIGHTED DATA IN A DIGITAL AGE

Congress enacted the DMCA in 1998 to conform to a more globalized copyright regime instated by the World Intellectual Property

22. *See* Joi Ito & Jeff Howe, WHIPLASH 30 (Grand Central Publishing, 1st ed. 2016).

23. *Id*.

24. *See* MIT Media Lab, *MIT Media Lab to Participate in New $27 Million Initiative on Ethics and Governance in AI*, (Jan. 10, 2017), https://www.media.mit.edu/posts/mit-media-lab-to-participate-in-new-27-million-initiative-on-ethics-and-governance-in-ai/ [https://perma.cc/UGT2-Z9BG] ("[t]he Ethics and Governance of Artificial Intelligence Fund's mission is to catalyze global research that advances AI for the public interest, with an emphasis on applied research and education.").

25. *See id.*

26. *See id.*

27. *See* MIT Media Lab, *supra* note 5.

Organization.[28] Congress' primary intention in enacting the DMCA was to strengthen copyright protection in a digital age.[29] The anti-circumvention provision states "no person shall circumvent a technological measure that effectively controls access to a work."[30] James Boyle, co-founder of the Creative Commons, describes such technological measures as the technological equivalent of barbed wire; just like barbed wire that surrounds and protects a farmer's crop, TPMs "fence off" copyrighted material from unwanted trespass, providing "an additional layer of 'physical' protection to the property owner's existing legal protection."[31] Another analogy characterizes the circumvention of a TPM as "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book."[32] While TPMs come in all shapes and sizes, they often come in the form of an *encryption device*: an algorithm that is engineered in such a way to only allow authorized parties to access particular data.[33] The DMCA's anti-circumvention provision, then, makes it illegal to circumvent TPMs, subjecting violators to significant fines or even jail time.[34]

The first reported case involving the DMCA anti-circumvention provision is *Universal City Studios v. Reimerdes*, where a TPM, namely a Content Scrambling System ("CSS"), allowed the owner of a DVD to watch the movie, but disallowed the owner to make a copy of the DVD.[35] Computer hackers discovered a way to circumvent the CSS, allowing them to create digital copies and circulate bootlegged versions throughout the internet.[36] Thus, the *Universal City Studios* court was presented with a classic use of the DMCA that fit squarely within the goal of copyright law.[37] This Constitutional goal is "to promote the progress of science and the useful arts."[38] By targeting pirating, the DMCA upholds the monetary incentive for movie studios to continue producing films, furthering the stated goal of copyright. The DMCA, functioning as a well-oiled machine,

28. H.R. REP. NO. 105-551, pt. 2, at 1 (1998); *see also MDY Indus*., *LLC v. Blizzard Entm't, Inc*., 629 F.3d 928, 942 (2010); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 440 (2d Cir. 2001).

29. *See MDY Indus*., *LLC*, 629 F.3d at 942.

30. 17 U.S.C. § 1201(a)(1)(A) (1998).

31. James Boyle, THE PUBLIC DOMAIN: ENCLOSING THE COMMONS OF THE MIND, 86 (2008).

32. *Universal City Studios v. Reimerdes*, 111 F.Supp. 2d 294, 316 (2000).

33. *See, e.g*., Lidiya Mischenko, *The Internet of Things: Where Privacy and Copyright Collide*, 33 SANTA CLARA HIGH TECH. L.J. 90, 100 (2016) (describing that TPMs are often encryption devices).

34. *See* H. Maria Perry, *The Consequences of a DMCA Violation*, (last visited March 11, 2017) http://legalbeagle.com/8335872-consequences-dmca-violation.html [https://perma.cc/6A9Z-FR26].

35. *See Universal City Studios*, 111 F.Supp at 308.

36. *Id*. at 303.

37. *But see* Samuelson, *Freedom to Tinker*, 17 THEORETICAL INQ. L. 563, 593 (2016) ("The *Reimerdes* decision initially had a severe chilling effect on the activities of computer security researchers who wanted to study how and how well TPMs work.").

38. U.S. CONST. art. I, § 8, cl. 8.

protects these copyrighted works where the public's interest of having open access to the work is outweighed by the private interest of monetizing the copyrighted work.

III. DMCA TRIENNIAL RULEMAKING PROCESS

Absent the DMCA, consumers are generally within their rights to tinker with their appliances, cars, technology and gadgets. People tinker with their technology for a variety of reasons: "to be playful, to learn how things work, to discern their flaws or vulnerabilities, to build their skills, to be more actualized, to tailor the artifacts to serve one's specific needs or functions . . . and occasionally, to be destructive."[39] Barring the public from circumventing TPMs restricts this freedom.[40] So, Congress mandated a Triennial Rule Making proceeding as a "fail-safe mechanism,"[41] to create and re-evaluate exemptions to the DMCA.[42] The Librarian of Congress, taking recommendations from the Copyright Office, is tasked with creating new exemptions for various classes of work.[43] These "classes of works" are subsets of the categories of the copyrightable subject matter listed in section 102 of the Copyright Act.[44] The Copyright Office takes into account a laundry list of factors such as the copyrighted work's availability for use; the copyrighted work's availability for nonprofit archival, preservation, and educational purposes; the DMCA's impact on copyright fair uses such as criticism, comment, news reporting, teaching, scholarship, and research; and the DMCA's effect on the market for copyrighted works.[45] The Librarian then issues the final determination every three years.[46]

Exemptions to the DMCA are subject to a Triennial Review Process where new exemptions are created, and each pre-existing exemption is reexamined.[47] The Triennial Rulemaking Proceeding, while helpful in applying the DMCA fairly to rapid changes in technology, also makes determinations by carefully balancing consumer rights against protections for copyright holders. Every three years, proponents of new exemptions

39. Samuelson, *supra* note 37, at 593.

40. *See generally* Samuelson, *supra* note 37; *see* Elizabeth F. Jackson, *The Copyright Office's Protection of Fair Uses Under The DMCA: Why The Rulemaking Proceedings Might Be Unsustainable And Solutions For Their Survival*, 58 J. COPYRIGHT SOC'Y 521, 525 (2011).

41. *See* H.R. REP. NO. 105-551, pt. 2, at 36 (1998).

42. *See* Jackson, *supra* note 40, at 528 .

43. 17 U.S.C. § 1201(a)(1)(C) (1998).

44. *See* Jackson, *supra* note 40, at 522523; 17 U.S.C. § 102 (2006) (listing literary works; musical works; dramatic works; pantomimes and choreographic works; pictorial, graphic, sculptural works; motion pictures and other audiovisual works; sound recordings; and architectural works).

45. 17 U.S.C. § 1201(a)(1)(C) (1998).

46. *Id*.

47. *Id*.

gather before the Copyright Office and submit reasons for why an exemption should be granted or why a pre-existing exemption should be reinstated.[48] Opponents, typically copyright industry participants, such as members of the motion picture industry; recording industry; and, as of late, the automotive industry, argue why any particular exemption should not be granted.[49]

The process begins with proponents filing summaries, typically five pages, for each proposed exemption.[50] The Copyright Office, after reviewing these summaries, may select certain exemption classes on which it wants further briefing on.[51] Then begins a four-month long process in which the proponent submits a brief, followed by an opponent's reply brief, and then an additional reply brief from the proponents that is tailored to opponent's arguments made in their reply brief.[52] After briefing, parties are required to make oral arguments before the Copyright Office in various locations, including Washington D.C. and Los Angeles.[53] Newly added exemptions typically do not go into effect until a year after implementation. DMCA expert Erik Stallman considers this delayed exemption deeply problematic because "a researcher who knows that her work will be lawful under Section 1201 in October 2016 but is not necessarily lawful now is robbed of much of the certainty that triennial exemptions are intended to provide."[54] Furthermore, a significant amount of time and resources must be invested every three years to propose these exemptions at the Triennial Review Proceedings. The Electronic Frontier Foundation spent between approximately $20,000 and $25,000 in researching, writing, as well as preparing for oral arguments in front of the Copyright Office.[55] Similarly, the auto industry spent approximately between $30,000 and $50,000 in opposing the Class 22 Exemption.[56] While this may seem like a fair cost to explore reasons for and against a brand-new DMCA exemption, these legal

48. *See id*.

49. *See* Krzysztof Bebenek, *Strong Wills, Weak Locks: Consumer Expectations and the DMCA Anticircumvention Regime*, 26 BERKELEY TECH. L.J. 1457, 1471.

50. Proposed exemptions often include pre-existing exemptions. Telephone Interview with Kit Walsh, Staff Attorney, Electronic Frontier Foundation (Feb. 12, 2017).

51. *Id*.

52. *Id*.

53. Telephone Interview with Kit Walsh, Staff Attorney, Electronic Frontier Foundation (Feb. 12, 2017); *see e.g*., Final Agenda for the Sixth Triennial 1201 Rulemaking Hearings (May 19, 2015).

54. Erik Stallman, *Needed Reforms to Section 1201 of the DMCA*, (Mar. 8, 2016), https://cdt.org/blog/needed-reforms-to-section-1201-of-the-dmca/ [https://perma.cc/J5A3-Z2UU].

55. E-mail from Diana Kruze, Partner, Morrison Foerster, to Holden Benon, UC Hastings Graduate, UC Hastings Coll. of the Law (Apr. 4, 2017, 11:48 PST) (on file with author). Kruze represents clients in a wide range of technical disciplines including software, medical devices, nanotechnology, smartphones, satellite systems, and semiconductor processing and packaging. She arrived at these figures by reviewing parties' briefs and making estimates based on a blend of San Francisco Bay Area billing rates.

56. *Id*.

expenses are burdensome on parties where a perfectly sound exemption must be proposed repeatedly every three years.[57] This highlights what is arguably the largest concern surrounding the Triennial Review Process; these exemptions are by no means permanent fixtures of law. Any exemption is subject to be repealed at a later review process.

Even though the DMCA can offer legitimate protection that meets the stated goal of copyright,[58] it can also be too far-reaching. The ability to "unlock" smartphones, codified in a recent exemption, betrays the tension between consumer interests and interests of the private copyright holder. Bypassing a TPM, the owner of a cell phone can reprogram the cell phone to designate an alternate carrier, which in turn opens the door for increased interoperability, resulting in a better overall experience for users. The Librarian of Congress, recognizing that this subsect of the public wanted to tinker with their phones, created a new exemption to the DMCA.

The Librarian mandated the unlocking exemption in 2006 and 2009, allowing users to modify their phones in ways that would enable them to interoperate with networks other than the network that the device was originally assigned to.[59] Proponents of the exemption argued that the owners of software should be free to do what they want with smartphone software, since, after all, they purchased the phone which comes along with the software.[60] This argument is based on the assumption that the owners of cell phones are also owners of the copies of the computer programs on those phones, bestowing the purchaser more rights.[61] The proponents of the unlocking exemption highlighted the anti-competitive nature of having a restriction that would prevent users from unlocking a phone to make it compatible with other networks.[62] This ability to unlock cell phones should be viewed as an expansion of consumer rights at the expense of a less air-tight business model for the cellphone providers.

Cellphone providers, in conjunction with technology companies such as Apple, felt that this exemption threatened their business model.[63] For

57. Furthermore, the Copyright Office must also expend valuable tax dollars to reviewing exemptions every three years.

58. *See generally, Universal City Studios*, 111 F.Supp at 345.

59. *See id*. at 311*; See* David Cline, *Consumer Choice: Is there an App For That?*, 10 J. TELECOMM. & HIGH TECH. L. 147, 150 (2012) (highlighting the Copyright Office's opinion following the 2010 decision that unlocking cell phones was not a copyright violation because it was based mainly issues other than copyright law).

60. Nicholas Hasenfus, *Unlocking Will Get You Locked Up: A Recent Change to The DMCA Makes Unlocking Cell Phones Illegal*, 15 J. HIGH TECH. L. 301, 314315 (2015).

61. *See id.* at 315.

62. *See id.* (citing supporters' claims that "ending the exemption will lead to higher device prices for consumers, increased electronic waste, higher costs associated with switching service providers, and widespread mobile customer 'lock-in.'").

63. *See* Timothy J. Maun, *iHack, Therefore iBrick: Cellular Contract Law, the Apple iPhone, and Apple's Extraordinary Remedy for Breach*, 2008 WIS. L. REV. 747, 758 (2008) (analyzing Apple's

instance, an agreement between Apple and AT&T involved unprecedented revenue sharing, such that Apple was contractually obligated to prevent consumers from using the iPhone on networks other than AT&T.[64] Opponents also held the position that locking phones is vital to their business models because, for example, wireless companies often subsidize cellphone manufacturing which leads to more affordable, higher quality devices.[65]

In 2012, the Librarian of Congress heeded these opponents and essentially removed the exemption for unlocking cell phones.[66] According to the 2012 class of exemptions, the new exception "applies only to mobile phones acquired prior to the effective date of the exemption or within 90 days thereafter."[67] This effectively wiped out any allowance on unlocking cellphones that were purchased 90 days after the act was passed. In making this change, the Librarian relied on a new ruling, *Vernor v. Autodesk, Inc.*,[68] which severely limited consumer rights. Under this new ruling, "a software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions."[69] Under *Vernor*, the purchaser of a cell phone likely does not own the cell phone's underlying code, but rather *is merely licensed to use the code*. The Librarian also noted that there were other alternatives to circumvention,[70] however did not state what these alternatives were, nor did she discuss the attractiveness of these alternatives in the eyes of the consumer.

The Librarian's ruling was met with criticism. Several commentators noted that this had less to do with upholding core copyright principles and more to do with protecting a business model.[71] It is important to keep in mind that sometimes these two are one and the same. This criticism

model that provides consumers with subsidized headsets where the cost is recouped by the wireless provider over a one or two-year contract, therefore necessitating phone locking mechanisms).

64. *See id*.

65. *See id*.

66. Hasenfus, *supra* note 60, at 323.

67. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 CFR Part 201.40 (2015).

68. Vernor v. Autodesk, Inc., 621 F.3d 1102, 1111 (9th Cir. 2010).

69. *See id*.

70. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 CFR Part 201 (2015) ("The Register further concluded that the record before her supported a finding that, with respect to new wireless handsets, there are ample alternatives to circumvention.").

71. Corynne McSherry, *The Wrong Tool For the Job: Cell Phone Unlocking Bill Creates New Problems*, ELECTRONIC FRONTIER FOUNDATION (Feb. 23, 2014), [http://perma.cc/AQP8-C4P3] (arguing that phone locking is designed to protect a business model); *see also* Hasenfus, supra note 60 at 325.

nevertheless caused Congress, under the Obama administration, to pass the Unlocking Consumer Choice and Wireless Competition Act ("Unlocking Act").[72] For the first time since section 1201 was enacted, Congress made its first serious intervention with regard to the anti-circumvention regime.[73] The Unlocking Act restored the exemption allowing owners of smartphone devices to unlock their smartphones when given authorization by the network they seek to gain service from.[74] Although the unlocking exemption was later restored by congressional intervention, the removal of the unlocking exemption from the DMCA demonstrates that such exemptions are subject to the vagaries of politics.

IV. THE CLASS 22 EXEMPTION FOR GOOD FAITH RESEARCH INTO VEHICLE SOFTWARE: PROBLEMS AND PROPOSAL

In 2015, the Librarian of Congress created an exemption for motor vehicles, stating "[c]omputer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates solely for the purpose of good-faith security research and does not violate any applicable law."[75] The ability to have independent vehicle software research is of the utmost importance given recent findings that "[n]ew high-end cars are among the most sophisticated machines on the planet, containing 100 million or more lines of code."[76] To provide a frame of reference, Facebook contains about 60 million lines of code.[77] The computer code underlying automobiles has impact on almost every electronic feature the car offers.[78] In one instance, security researches discovered a way to disable a car's brakes by using an infected MP3 file inserted into the car's audio system.[79] To ensure the safety of pedestrians and drivers on the road, it is imperative that researchers are able to circumvent TPMs without violating the DMCA. Protecting the public from otherwise harmful vehicle software, the Electronic Frontier

72. *See* Unlocking Consumer Choice and Wireless Competition Act, 133 P.L. 144, 128 Stat. 1751 (2014) (enacted) (allowing circumvention of a TPM that restricts wireless telephone handsets or other wireless devices from connecting to a wireless telecommunications network).

73. Stallman, *supra* note 54.

74. *See* Hasenfus note 60, at 327.

75. This exemption applies specifically to car software. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 CFR Part 201 (2015) (applying to good-faith security research into car software).

76. David Gelles, Hiroko Tabuchi, and Matthew Dolan, *Complex Car Software Becomes Weak Spot Under the Hood* (Sept. 26, 2015), https://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html?_r=0 [https://perma.cc/QP4S-WLH2].

77. *Id*.

78. *See* Gelles, *supra* note 76.

79. Darlene Storm, *Remote attacks to hack and set cars to self-destruct?*, Computerworld (Aug. 21, 2012), http://www.computerworld.com/article/2472673/cybercrime-hacking/remote-attacks-to-hack-and-set-cars-to-self-destruct-.html [https://perma.cc/QP4S-WLH2].

Foundation fought tooth and nail to convince the Copyright Office to propose this exemption in 2015. Every three years, the Copyright Office will assess the viability of this exemption at the Triennial Review Proceeding.

Auto manufacturers vehemently lobbied against this exemption and will likely continue to do so as long as the Class 22 Exemption is subject to the Triennial Review Process. Specifically, companies such as John Deere,[80] and General Motors,[81] as well as organizations like the Auto Alliance,[82] have actively opposed these measures for good-faith security research. Given that new car models can now likely be considered complex information systems,[83] it is in these companies' best interests to shield this code from the public. Those who have taken a class in torts are familiar with the millions, if not billions, of dollars in damages that may arise in a defective automobile design case.[84] Thus, it comes as no surprise that auto-manufacturers are compelled to absolve themselves from liability wherever possible. A tiny bug in the software could translate to auto-collisions and costly vehicle recalls and it is still uncertain how vehicle autonomy will affect these defective design mass tort cases. Thus, car manufacturers rely on various protections, including a "security by obscurity" approach, where source code is obfuscated, or rendered unintelligible by computer algorithms.[85]

80. United States Copyright Office, Long Comment of John Deere Regarding a Proposed Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201, https://www.copyright.gov/1201/2015/comments-032715/class%2022/John_Deere_Class22_1201_2014.pdf [https://perma.cc/9HFT-2NTX].

81. United States Copyright Office, Comments of General Motors LLC Regarding a Proposed Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201, https://www.copyright.gov/1201/2015/comments-032715/class%2022/General_Motors_Class22_1201_2014.pdf [https://perma.cc/CRP8-GE9B].

82. United States Copyright Office, Long Comment of Auto Alliance Regarding a Proposed Exemption to Prohibition on Circumvetion of Copyright Protection for Access Control Technologies Under 17 U.S.C. 1201, http://copyright.gov/1201/2015/comments032715/class%2022/Auto_Alliance_Class22_1201_2014.pdf [https://perma.cc/5VGV-T5PT].

83. *See* Stallman, *supra* note 54.

84. *See* Grimshaw v. Ford Motor Co., 119 Cal. App. 3d 757 (1981) (awarding injured plaintiff $125 million in punitive damages where an automobile manufacturer, Ford, placed a car on the market with knowledge of dangerous defects); Andrew Pollack, $4.9 Billion Jury Verdict in G.M. Fuel Tank Case, (July 10, 1999), http://www.nytimes.com/1999/07/10/us/4.9-billion-jury-verdict-in-gm-fuel-tank-case.html [https://perma.cc/2EN9-55KC] ("General Motors Corporation was ordered . . . to pay $4.9 billion to six people severely burned when the fuel tank of their 1979 Chevrolet Malibu exploded after a rear-end collision."); *see also* Bill Vlasic, *G.M. Begins Prevailing in Lawsuits Over Faulty Ignition Switches* (Apr. 10, 2016), https://www.nytimes.com/2016/04/11/business/gm-begins-prevailing-in-lawsuits-over-faulty-ignition-switches.html [https://perma.cc/X4KP-QP8V] (General Motors spent more than $2 billion settling claims in relation to faulty ignition switches that cut engine power and disabled airbags)

85. In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07, Comment of Bruce Schneier on Proposed Class 22 (May 1, 2015); *see also* Technopedia https://www.techopedia.com/

Auto manufacturers, in their opposition briefs, suggest that the threat of DMCA violations may deter hackers from gaining access to software.[86] Although studies show that the current complexity of vehicle technology could allow hackers to access even the physical components to the car such as the steering wheel,[87] many argue that the threat of a DMCA violation is not enough to deter a malicious hacker from bypassing a TPM.[88] Shielding the complex code via this "security by obscurity"[89] approach would instead have a severe chilling effect on good-faith vehicle researchers.[90]

Independent research into vehicle software could instead yield the opposite result. Having additional good-faith vehicle researchers dedicated to finding and repairing vulnerabilities in security software would likely make it more difficult for hackers to access the functional aspects of the automobile.[91] Also, this exemption likely prevents corporate bad practices that negatively impact public safety or the environment, as the programmers writing potentially harmful source code are no longer operating in complete darkness. In creating this exemption, the Librarian also boosted consumer freedom to tinker, moving the current law further away from anti-consumer rulings such as *Vernor*.[92]

Thus, the Class 22 Exemption's enhancements to road safety,

definition/16375/obfuscation [https://perma.cc/BDE5-QTKP].

86. *See generally* In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07, Long Comment of John Deere on Proposed Class 22 (Mar. 27, 2015) *available at* https://www.copyright.gov/1201/2015/comments-032715/class%2022/John_Deere_Class22_1201_2014.pdf [https://perma.cc/H89B-L3W2].

87. *See* Cale Guthrie Weismann, *Hackers were Able to Remotely Control a Jeep Cherokee's Radio and Even Turn Off the Transmission*, (July 21, 2015), http://www.businessinsider.com/researchers-show-the-ability-to-remotely-hack-and-control-a-car-2015-7 [https://perma.cc/TF9R-GYL8].

88. *See* In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07, Comment of Bruce Schneier on Proposed Class 22 (May 1, 2015) ("The truth is that the bad guys conduct their own security research, and this rulemaking will have no effect one way or another on how much of that goes on. If the good guys are prohibited from conducting that same research, the bad guys win."); Samuelson, *supra* note 37, at 590-91, ("the payoff of infringement may be large, and it is often easy for destructive tinkerers to hide in the darknet.")

89. *See id*.

90. *See id*. ("I know of many security researchers who have refrained from conducting important security research because they fear the DMCA. I know of even more security research where the results are not being published because the researchers fear the DMCA."); *see also* Stallman, *supra* note 54, ("in some cases, Section 1201 has limited or prevented security research into those vulnerabilities altogether).

91. *See* In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07, Petition for Exemption: Applied Cryptography, Security, and Reverse Engineering Research of Matthew D. Green at https://www.copyright.gov/1201/2014/petitions/Green_1201_Initial_Submission_2014.pdf ("If legitimate security researchers are able to help identify and fix security vulnerabilities before black hats are able to exploit them, then malicious hacking would become increasingly difficult"); *See also* Samuelson, *supra* note 37, at 597.

92. *See supra* note 70.

consumer freedom and environmental protections seem to outweigh the risks the speculated uptick in software hacks.[93] For each of these reasons, it is extremely important that the Class 22 Exemption not be subject to re-examination. Instead, it should be cemented in permanent form.

Assuming, *arguendo*, that the Class 22 Exemption is removed in a future Triennial Review Proceeding, and a researcher violated the DMCA while engaging in good-faith research, the researcher violating the DMCA could raise the fair use doctrine. This would be an unreliable protection however, as the question of whether fair use can be raised as an affirmative defense to a DMCA violation has been largely unanswered.[94] Even if fair use is a defense to a DMCA violation, investment into this research could dwindle in fear of having to litigate a fair use case in court. For these reasons, Congress should consider creating an allowance in the DMCA to allow vehicle software testing.

Congressional intervention to the DMCA occurred in 2013 with the enactment of the Unlocking Act, where Congress created a statutory exception for unlocking cell phones.[95] This act could be an additional protection if extended to allow circumvention of TPMs protecting automobile software for good-faith research. The legislative history underpinning the Unlocking Act provides in part: "It shall not be a violation of this section to circumvent a technological measure in connection with a work protected under this title if the purpose of such circumvention is to engage in a use that is not an infringement of copyright under this title."[96] Thus, according to the legislative history, if a user's actions fall under fair use, then the fair use should not be considered a violation of the DMCA, because fair use is, by its nature, non-infringing. However, as it stands, the Unlocking Act does not encompass vehicle software research.

The security research community, and all who depend on their efforts, would benefit from a more permanent solution. Sure enough, section 1201(j) provides a statutory exemption for good-faith security testing, however its vaguely-written language makes it unattractive to researchers seeking protection. According to 1201(j), "it is not a violation of that

93. Some also worry that this exemption could allow consumers to modify the code themselves, cutting against road safety and environmental regulations. However, the Librarian addressed this issue by instating the Class 21 Exemption for Vehicle Software – Diagnosis, Repair, and Modification. Acknowledging the long-standing practice of home garage modifications, the Librarian granted the exemption for *lawful* modification of a vehicle function.

94. *See MDY Indus., LLC*, 629 F.3d at 950 n.12; *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1199 n.14 (Fed. Cir. 2004).

95. *See* Unlocking Consumer Choice and Wireless Competition Act, 133 P.L. 144, 128 Stat. 1751 (2014) (enacted).

96. Unlocking Technology Act of 2013, 113 H.R. 1892.

subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section."[97] The statute lists several factors in determining exemption including "whether the information derived from the security testing was *shared directly* with the developer of the computer," and whether "information derived from the security testing was used or maintained in a manner that *does not facilitate infringement* under this title *or a violation of applicable law other than this section*, *including a violation of privacy or breach of security*."[98]

As Matthew D. Green correctly points out in his petition to the Copyright Office, this exception contains "ambiguities" and "burdensome requirements."[99] He highlights that these provisions "include complex multifactor tests that cannot be evaluated ex ante, potential restrictions on the dissemination of research results, and requirements to seek authorization in advance of performing research."[100] Specifically, the statute is vague as to what is meant by "shared directly" with the developer. This seems to suggest that a researcher, before sharing her findings to the press, must first share her findings with the automobile manufacturer (the presumed developer of such computer) and obtain permission to further disclose the findings. These factors are vague as they factor in "breach[es] of security." A security researcher may need to decrypt a TPM in order to discover flaws in the underlying computer code. Decryption could be read as a "breach of security."[101] So, to factor in breaches of security implies that the researcher, in avoiding a decryption, would need to access the code by obtaining permission from the auto manufacturer. According to proponents of the Class 22 Exemption, "[m]aking non-infringing research dependent upon permission from rights holders with incentives to deny or limit important research is not an adequate alternative to circumvention."[102] Lastly, the statutory language that states "does not . . . facilitate a violation

97. 17 U.S.C. § 1201(A)(1)(j) (1998).

98. *Id*. (emphasis added).

99. *See* In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07, Petition for Exemption: Applied Cryptography, Security, and Reverse Engineering Research of Matthew D. Green at https://www.copyright.gov/1201/2014/petitions/Green_1201_Initial_Submission_2014.pdf [https://perma.cc/Q7EJ-GMZQ].

100. *Id*.

101. Cambridge Dictionary, http://dictionary.cambridge.org/us/dictionary/english/decrypt [https://perma.cc/A8YB-BBQJ] (defining decrypt as to change electronic information or signals that were stored, written, or sent in the form of a secret code back into a form that you can understand and use normally).

102. In the matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies Under 17 U.S.C. 1201 Docket No. 2014-07, Reply Comment of the Electronic Frontier Foundation, 13 (Feb. 6, 2015) http://copyright.gov/1201/2015/comments020615/InitialComments_longform_EFF_Class22.pdf.

of applicable law under this section."[103] As Erik Stallman points out, a researcher arguably violates the Computer Fraud and Abuse Act simply by exceeding the authorization given.[104] Thus, this final clause seems to be a catch-all that would give copyright holders the upper hand in litigation. While the Copyright Office's 2015 ruling suggests that vehicle software testing likely does not constitute infringement,[105] the legal expense of having to litigate a 1201(j) defense could nevertheless deter research. Had Congress laid out section 1201(j) in a way that allowed researchers to rely on its measures, then the time and resources spent in deciding the Class 22 Exemption could have been used in other ways.

Congress should strongly consider clarifying the language in section 1201(j). The current language is vague and does not provide the intended result of encouraging research into vehicle software. If Congress intended to create an exemption for computer software testing, and this intention was reiterated in clearer form by the Librarian of Congress through the addition of certain DMCA exemptions,[106] then Congress should amend section 1201(j) in a way that mirrors these exemptions. The Triennial Review Process is helpful in that it responds to changes in technology every three years, likely faster than Congress can pass laws. However, it is flawed in that it leaves perfectly sound exemptions vulnerable to unneeded scrutiny every three years. As it stands, there is no need to remove an exemption that allows good-faith, unbiased actors the chance to determine whether vehicle code poses a risk to road safety. The fact that these exemptions are temporary is deeply problematic for sustained research into vehicle safety. If a party is seeking to commence research into vehicle code that could take longer than three years, that researcher is gambling that her research will not be upended at the succeeding triennial review process.[107] This uncertainty can be removed by embodying this exemption in permanent form. By doing so, Congress has the power to decrease information costs related to vehicle software, as the legality of research would no longer have a three-year timer. This would lead to safer, greener vehicles as research endeavors would be more attractive to investors and institutions.

103. § 1201(a)(1)(j)(B).

104. Stallman, *supra* note 54.

105. *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 CFR Part 201 (2015)

106. *See id*. The Librarian of Congress also laid out a clear exemption for computers and machines generally, as well as a separate exemption for medical device research.

107. Stallman, *supra* note 54.

V. CONCLUSION

Although critics question whether computer software produced for non-copyright reasons should be subject to copyright protection, the source code that underlies this technology is in fact governed by copyright law.[108] The DMCA seems to be the proper mechanism for this type of inquiry and will likely remain so the foreseeable future. The government should be diligent in expanding and contracting the DMCA's far-reaching protection as needed.

Far beyond what the DMCA drafters intended to encompass, the Class 22 Exemption is vital to road safety given the recent strides in artificial intelligence. Accordingly, this exemption should be crystallized in statutory form instead of having parties repeat this process every three years. This should be done by clarifying the language in section 1201(j). As demonstrated, a permanent exemption which expands research into vehicle software will help keep our roadways safe and our atmosphere clean.[109] Such a decision would stand to protect consumer freedom, keeping alive the principle that the owner of a good should have the freedom to do what he or she wants with that item. Traditionally, car owners have had the freedom to 'peek under the hood,' to examine and develop a rich understanding of how their cars operate. Research into car software allows individuals to learn by tinkering with their products, engendering an organic dissemination of knowledge. This engagement is largely what inspires the next wave of designers, engineers, and mechanics. Strengthening this exemption would also foster long-term independent research into these machines that we trust with our lives, ultimately making the roads we travel safer, and the air we breathe cleaner.

108. *See supra* note 3.
109. *See supra* Part I.

***