LONG COMMENT REGARDING
A PROPOSED EXEMPTION UNDER 17 U.S.C. § 1201

ITEM A. COMMENTER INFORMATION

Commenter:
The Motor & Equipment Manufacturers Association
("MEMA")
1425 K Street, NW
Suite 910
Washington, DC 20005

Contact:
Dan Jasnow
Arent Fox LLP
1717 K Street, NW
Washington, DC 20006
dan.jasnow@arentfox.com
(202) 857-8967

ITEM B. PROPOSED CLASS ADDRESSED

Class 12 (Computer Programs – Repair)

ITEM C. OVERVIEW

The Motor & Equipment Manufacturers Association ("MEMA") is the leading trade association representing U.S. motor vehicle parts manufacturers. Directly employing 907,000 U.S. workers, vehicle suppliers manufacture original equipment ("OE") and aftermarket parts, components, and systems for use in passenger vehicles and heavy trucks.[1] MEMA represents its members through four divisions: Automotive Aftermarket Suppliers Association ("AASA"); Heavy Duty Manufacturers Association ("HDMA"); MERA, The Association for Sustainable Manufacturing; and Original Equipment Suppliers Association ("OESA"). This diverse group of member companies gives MEMA a unique perspective on the real-world impact of exemptions that affect the vehicle industry.

On behalf of AASA and MERA, during the Eighth Triennial Rulemaking, MEMA submitted a petition that supported renewing the "Class 12 – Repair" temporary exemption for "Computer programs that control motorized land vehicles, including farm equipment, for purposes of diagnosis, repair, or modification of the vehicle, including to access diagnostic data." We supported this exemption because it balances the protection of consumer safety, valuable intellectual property, and consumer choice.

MEMA submits these comments in response to comments submitted by the Alliance for Automotive Innovation ("AAI") regarding the scope of the existing and proposed repair exemptions and potential liability for third party service providers under 17 U.S.C. § 1201(a)(2), (b)(1) (the "Anti-Trafficking Provisions").

ITEM D. TECHNOLOGICAL PROTECTION MEASURE(S) AND METHOD(S) OF CIRCUMVENTION

Vehicles contain a suite of electronic control units ("ECUs") and modules that control various vehicle functions. ECUs and modules contain computer software that enables a vehicle parts' functionality and ensures that the vehicle operates within the confines of safety and environmental regulations. The ECUs

[1] Vehicle parts suppliers are the largest manufacturing sector in the U.S. with a jobs presence in all 50 states. Direct, indirect, and induced vehicle supplier employment accounts for over 4.8 million jobs. Moreover, vehicle suppliers contribute 2.5 percent of U.S. GDP. "U.S. Labor & Economic Impact of Vehicle Supplier Industry" MEMA and IHS Markit. February 2021.

and modules control numerous aspects of the vehicle, such as the propulsion system, camera and radar-based safety systems, seat position settings, and a variety of other functions.

The software of ECUs is protected by technological protection measures ("TPMs"), such as encryption. The TPMs help ensure that the ECUs are not improperly tampered with. Also, TPMs protect the valuable intellectual property underlying these systems, namely the proprietary computer software embedded in the ECUs.

ECUs and modules may also collect and store vehicle data—in real time—about vehicle and system performance. If sent beyond the vehicle, it becomes telematics data. Telematics data provides valuable information about each individual vehicle. For example, the data might reveal the exact date and time when a vehicle system has malfunctioned and reveal to a technician the specific incident or event that led to the malfunction. Similarly, in exchange for a discount on their insurance premiums, some consumers choose to share their telematics data with automotive insurance companies, which lets the insurer verify safe driving habits. MEMA supports the rights of consumers to access and control how these data are used,[2] but such consumer choice is in some instances limited or restricted by vehicle TPMs.[3]

ITEM E. ASSERTED ADVERSE EFFECTS ON NON-INFRINGING USES

This next comment addresses the following question: Do the Anti-Trafficking Provisions impose liability on third party service providers who circumvent TPMs on lawfully acquired motor vehicles to perform non-infringing diagnostic, repair, or modification services on behalf of the owner?

In short, no. Third parties "whose circumvention [services] do not facilitate infringement are not subject to § 1201 liability."[4] Where, as in the case of an independent vehicle repair technician, copyright laws authorize consumers to repair, diagnose problems with, or modify the software embedded in their lawfully acquired vehicles, there is no infringement and therefore no liability for the third-party service provider under the Anti-Trafficking Provisions.

---

[2] See, e.g., Your Car. Your Data. Your Choice.™, an Auto Care Association and Automotive Aftermarket Suppliers Association (division of MEMA) education initiative created to engage car owners, policymakers, and other stakeholders on car data – what is it, why it matters, and its implications for consumer choice.

[3] The 2014 Memorandum of Understanding ("MOU") referenced in AAI's comments expressly excludes telematics data.

[4] *Chamberlain Grp., Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1195 (Fed. Cir. 2004). *See also Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307, 1318 (Fed.Cir.2005) ("[C]ourts generally have found a violation of the DMCA only when the alleged access was intertwined with a right protected by the Copyright Act."); *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004) (holding that a modification chip designed to make third party ink cartridges compatible with Lexmark printers was not primarily designed to circumvent copyright and thus did not violate the DMCA); *United States v. Reichert*, 747 F.3d 445, 458 (6th Cir. 2014) (Donald, dissenting) (discussing the legislative history of the DMCA which "makes clear that the anti-circumvention provision is not intended to function as a comprehensive ban on all circumvention technologies; rather, its purpose is to prevent those technologies from being used as a tool for copyright infringement and to provide remedies for copyright holders against individuals and entities who facilitate the widespread unauthorized reproduction of copyrighted works by making such technologies available to the public"); *Universal City Studios v. Corley*, 273 F.3d 429, fn. 14 (2d Cir.2001) ("When read together with the anti-trafficking provisions, subsection 1201(a)(3)(A) frees an individual to traffic in encryption technology designed or marketed to circumvent an encryption measure if the owner of the material protected by the encryption measure authorizes that circumvention"); *Nordstrom Consulting, Inc. v. M & S Techs., Inc.*, No. 06 C 3234, 2008 WL 623660, at *9 (N.D. Ill. Mar. 4, 2008) (applying "infringement nexus"). *But see MDY Indus., LLC v. Blizzard Entm't, Inc.,* 629 F.3d 928, 948 (9th Cir.2010) (rejecting the "infringement nexus" requirement set forth in *Chamberlain*).

1. There is No Liability Under the Anti-Trafficking Provisions When Circumvention Services Do Not Facilitate Infringement

Any analysis of the scope of the Anti-Trafficking Provisions should begin with the text of the statute, specifically, subsections 1201(a)(2) and (a)(3) and 1201(b)(1) and (b)(2). A close review of this statutory language is important because in both its September 2020 and February 2021 comments, AAI mischaracterizes the scope of the Anti-Trafficking Provisions. According to AAI, "[p]roviding a commercial service that requires circumventing access controls or copy controls (e.g., using or providing certain engine tuning software) is indisputably trafficking in an unlawful service under Sections 1201(a)(2) and (b)."[5] In fact, there is no *per se* prohibition on "commercial services that require circumvention." Rather, the Anti-Trafficking Provisions prohibit circumvention in certain clearly defined circumstances.

Under subsection 1201(a)(2), defendants may be liable for trafficking in circumvention services or devices if they, *inter alia*, "offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

> (A) is *primarily* designed or produced for the purpose of circumventing a technological measure that effectively ***controls access*** to a work protected under this title;
>
> (B) has only *limited commercially significant purpose* or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is *marketed* by that person or another acting in concert with that person with that person's knowledge *for use in circumventing* a technological measure that effectively controls access to a work protected under this title.

(the "Access Control Provision") (all emphasis added). In addition, liability under the Access Control Provision is further limited to circumstances in which circumvention is undertaken to avoid, bypass, remove, deactivate, or impair a TPM "*without the authority of the copyright owner*" (emphasis added).[6]

Under subsection 1201(b), defendants may be liable if they, *inter alia*, "offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

> (A) is *primarily* designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively ***protects a right*** of a copyright owner under this title in a work or a portion thereof;
>
> (B) has only *limited commercially significant purpose* or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or
>
> (C) is *marketed* by that person or another acting in concert with that person with that person's knowledge *for use in circumventing* protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

---

[5] AAI, Comment Regarding Proposed Class 12 Exemption, at 5 (February 9 2021); AAI, Comment in Response to Petitions to Renew the 'Streamlined Renewal Process' Exemption, at 2 (September 8, 2020).
[6] 17 U.S.C. § 1201(a)(3).

(the "Rights Control Provision") (all emphasis added). Liability under the Rights Control Provision is further limited to circumstances in which the circumvented TPM "effectively protects *a right of a copyright owner*" (emphasis added).[7]

Thus, a defendant who traffics in services that circumvent ***access*** controls may be subject to liability under the Access Control Provision if (i) circumvention is undertaken "without the authority of the copyright owner," and (ii) the service either (x) is primarily designed or produced for the purpose of circumvention; (y) has only limited commercially significant purpose or use other than circumvention; or (z) it is marketed for use in circumvention.

Defendants who traffic services that circumvent ***rights*** controls may be subject to liability under the Rights Control Provision if (i) they circumvent a TPM that effectively protects a right of a copyright owner; and (ii) the service either (x) is primarily designed or produced for the purpose of circumvention; (y) has only limited commercially significant purpose or use other than circumvention; or (z) it is marketed for use in circumvention.

As noted above, a close review of this statutory language is important because the DMCA does not, as AAI incorrectly asserts, make it *per se* illegal to "provid[e] a commercial service that requires circumventing access controls or copy controls."[8] Rather, it prohibits trafficking in circumvention services where the circumvention facilitates infringement *and* the services are primarily designed for the purpose of circumvention, have only limited commercial value, or are marketed for use in circumvention.

This reading of the Anti-Trafficking Provisions is consistent with the DMCA's legislative history and the majority of case law. Congress's primary concern in enacting 1201(a)(2) and (b) was devices that are "expressly intended to facilitate circumvention of technological protection measures for purposes of gaining access to a work." In contrast, the provisions were "not aimed at products that are capable of commercially significant non-infringing uses, such as consumer electronics, telecommunications, and computer products–including videocassette recorders, telecommunications switches, personal computers, and servers–used by businesses and consumers for perfectly legitimate purposes."[9] In the context of independent automotive repair technicians, the commercial service is motor vehicle repair, not circumvention. To the extent circumvention is necessary, it is incidental to the commercial service and adds little to the value proposition between the service provider and customer.

Courts have recognized that a *per se* rule against circumvention, of the type AAI proposes, is inconsistent with the careful balance Congress established in the DMCA. In *Chamberlain Grp., Inc. v. Skylink Techs., Inc*., 381 F.3d 1178, 1195 (Fed. Cir. 2004), the U.S. Court of Appeals for the Federal Circuit considered a case in which the plaintiff urged the court to read the DMCA as if "Congress simply created

[7] 17 U.S.C. § 1201(b)(2).

[8] AAI, Comment in Response to Petitions to Renew the 'Streamlined Renewal Process' Exemption, at 2 (September 8, 2020).

[9] H.R. Rep. 105-551(II), 38, 39-40 (July 22, 1998) ("As previously stated in the discussion of Section 102(a)(2), the Committee believes it is very important to emphasize that Section 102(b)(1) is aimed fundamentally at outlawing so-called 'black boxes' that are expressly intended to facilitate circumvention of technological protection measures for purposes of gaining access to a work. This provision is not aimed at products that are capable of commercially significant noninfringing uses, such as consumer electronics, telecommunications, and computer products–including videocassette recorders, telecommunications switches, personal computers, and servers–used by businesses and consumers for perfectly legitimate purposes").

a new protection for copyrighted works without any reference at all either to the protections that copyright owners already possess or to the rights that the Copyright Act grants to the public."[10] The court rejected the plaintiff's theory of a "per se violation of the DMCA," concluding that the plaintiff's "proposed construction of the DMCA ignores the significant differences between defendants whose accused products enable copying and those, like [defendant], whose accused products enable only legitimate uses of copyrighted software."[11]

Rather than a *per se* rule, a circumvention device or service violates the Anti-Trafficking Provisions only when there is a "nexus between access and protection." To establish this "infringement nexus," a plaintiff alleging a violation of § 1201(a)(2) must prove: (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological measure.[12]

While some courts have disagreed with the "infringement nexus" standard established by the Federal Circuit, most notably the Ninth Circuit in *MDY Indus., LLC v. Blizzard Entm't, Inc*., 629 F.3d 928 (9th Cir. 2010), several courts have followed the infringement nexus standard and held that circumvention technologies designed primarily for purposes other than to bypass copyright restrictions are not within the scope of the DMCA's Anti-Trafficking Provisions.[13]

In general, where a defendant traffics in a device or service that clearly violates some form of copyright, courts have found liability under the Anti-Trafficking Provisions. Thus:

- A circumvention device that allowed a player to play games not licensed in their territory (e.g., play a game only licensed in Japan in the U.S.) violated the Access Control Provision.[14]
- Distribution of computer technology designed to circumvent DVD encryption and to view or to copy a motion picture from a DVD violated the Access Control Provision.[15]
- A defendant violated the Access Control Provision by selling a computer software technology that was primarily designed, produced and marketed for the purpose of circumventing a technological protection measure in a video game, allowing users to play the game unattended.[16]

---

[10] *Chamberlain Grp., Inc. v. Skylink Techs., Inc*., 381 F.3d 1178, 1197 (Fed. Cir. 2004).
[11] *Id.*
[12] *Id.* at 1203.
[13] See *Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307, 1318 (Fed.Cir.2005) ("[C]ourts generally have found a violation of the DMCA only when the alleged access was intertwined with a right protected by the Copyright Act."); *Lexmark Int'l, Inc. v. Static Control Components, Inc*., 387 F.3d 522 (6th Cir. 2004) (holding that a modification chip designed to make third party ink cartridges compatible with Lexmark printers was not primarily designed to circumvent copyright and thus did not violate the DMCA); *Nordstrom Consulting, Inc. v. M & S Techs., Inc.*, No. 06 C 3234, 2008 WL 623660, at *9 (N.D. Ill. Mar. 4, 2008) (applying "infringement nexus").
[14] *Sony Computer Entm't Am., Inc. v. Gamemasters*, 87 F. Supp. 2d 976 (N.D. Cal. 1999).
[15] *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y.), judgment entered, 111 F. Supp. 2d 346 (S.D.N.Y. 2000), aff'd sub nom. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).
[16] *MDY Indus., LLC v. Blizzard Entm't, Inc*., 629 F.3d 928 (9th Cir. 2010).

In contrast, courts have declined to find trafficking liability where a device or service has a legitimate commercial use that does not implicate the owner's copyrights. For example:

- The manufacturer of universal garage door openers that reverse engineered the plaintiff's system and marketed its own opener was not liable under the Anti-Trafficking Provisions because the device enabled only legitimate uses of copyrighted software.[17]
- An entity that sold technology to "unlock" laser printers and let consumers replace toner cartridges with "unauthorized" third party cartridges did not violate the Anti-Trafficking Provisions because the protected software was not copyrightable.[18]

In short, contrary to AAI's comments, there is no *per se* rule of illegality for all circumvention services. Rather, circumvention services violate the Anti-Trafficking Provisions when they infringe or facilitate infringement of a protected right under the Copyright Act.

2. Automotive Repair Technicians Who Circumvent Vehicle TPMs on Behalf of Vehicle Owners or Lessees Do Not Infringe or Facilitate Infringement

When an independent automotive repair technician circumvents vehicle TPMs in order to diagnose, repair, or make lawful modifications to software on behalf of the lawful owner (or lessee) of that vehicle, the technician does not infringe or facilitate infringement of a right protected by the Copyright Act. This is because such conduct is non-infringing under 17 U.S.C. 117. [19]

Section 117 of the Copyright Act allows the owner of a copy of a computer program to "*authorize*" a third party to make a copy of a computer program, subject to certain limitations.[20] In 2016, the Copyright Office noted that if a consumer owns a copy of software that is embedded in a product, then "section 117(a) provides broad protections for repair and tinkering activities."[21] The Copyright Office goes on to note that under Section 117(a) "the owner of the copy of a computer program may make a new copy of that program or create an adaptation of that program if the 'new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine,' and 'is used in no other manner'" and that "the owner may authorize a third party—such as a repair technician—to make an additional copy or create an adaptation on his or her behalf."[22]

In the same report, the Copyright Office also rejected the argument that a consumer is not the "owner" of a copy of the software, noting, "[f]or example, specialized software controlling certain mechanical components of an automobile, like windshield wipers or transmission, may essentially be invisible to the consumer. In such cases, it would be unusual to characterize the sale of the automobile as involving the licensing of that software for purposes of the Copyright Act."[23]

---

[17] *Chamberlain Grp., Inc.*, 381 F.3d at 1198.
[18] *Lexmark Int'l, Inc.*, 387 F.3d 522.
[19] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 80 Fed. Reg. 65944-01, at 65954 (Oct. 28, 2015).
[20] 17 U.S.C. § 117.
[21] U.S. Copyright Office, Software-Enabled Consumer Products, A Report of the Register of Copyrights, at 36 (2016).
[22] *Id.* (quoting 17 U.S.C. § 117(a)).
[23] *Id.*

Because third party repair services are non-infringing under Section 117, a repair technician cannot be liable under the Anti-Trafficking Provisions, which only extend to cognizable rights under the Copyright Act. This is not to say that copyright owners do not have valid and enforceable rights in the vehicle software—just that those rights do not prevent consumers from having their cars serviced by third parties.

3. The Existing Exemption Permits Circumvention by Third Party Service Providers

The existing repair exemption[24] permits third party circumvention services to the extent permitted under existing Copyright law. Like the DMCA as a whole, the current version of the exemption reflects a careful balance between consumer safety, protection of intellectual property, and protection of consumer choice in the automotive aftermarket, and is a testament to the success of the Sixth and Seventh Triennial Rulemakings.

The Copyright Office first considered a temporary exemption for diagnosis, repair, or modification of vehicle computer programs during the Sixth Triennial Rulemaking. Under the resulting exemption, circumvention of vehicle TPMs for diagnosis, repair, and modification, was only permissible "when circumvention [was] a necessary step *undertaken by the authorized owner of the vehicle* to allow the diagnosis, repair or lawful modification of a vehicle function." The Copyright Office explained that it felt it necessary at the time to expressly restrict the eligible exemption beneficiaries in this manner due to concerns with the DMCA's Anti-Trafficking Provisions.

Subsequently, however, the Copyright Office acknowledged that the Anti-Trafficking Provisions likely do not prevent it from allowing exemption beneficiaries to seek third party assistance in certain circumstances. For example, the Copyright Office noted after the Sixth Triennial review that it is under no obligation to define the class of eligible exemption beneficiaries as restrictively as it did in the existing repair exemption.[25] In addition, the Copyright Office subsequently acknowledged that in adopting the Unlocking Act, Congress did not intend to create a negative inference against the lawfulness of third-party assistance generally.[26]

During the Seventh Triennial Rulemaking, MEMA and others successfully petitioned the Copyright Office to eliminate the restriction on exemption beneficiaries. Given that most diagnostic and repair work is conducted by skilled professionals, whether at dealerships or at independent automotive repair shops, MEMA noted that limiting the exemption's beneficiaries to only "authorized owners," while excluding third parties acting on behalf of such owners, meant that most consumers would be unable to benefit from the exemption. MEMA therefore recommended renewing the exemption for diagnosis, repair, and modification, but with appropriate modifications that would make it easier for consumers to have their vehicles serviced by third parties. The Copyright Office agreed, issuing the current version of the exemption without the limitation that circumvention be undertaken only by the authorized owner of the

---

[24] Computer programs that are contained in and control the functioning of a lawfully acquired motorized land vehicle such as a personal automobile, commercial vehicle, or mechanized agricultural vehicle, except for programs accessed through a separate subscription service, when circumvention is a necessary step to allow the diagnosis, repair, or lawful modification of a vehicle function, where such circumvention does not constitute a violation of applicable law, including without limitation regulations promulgated by the Department of Transportation or the Environmental Protection Agency, and is not accomplished for the purpose of gaining unauthorized access to other copyrighted works.

[25] U.S. Copyright Office, Section 1201 of Title 17, A Report of the Register of Copyrights, at 61 (2017).

[26] *Id.* at 59.

vehicle. It is important to note that the Copyright Office lifted this restriction in response, at least in part, to comments that expressly argued that third party independent vehicle repair technicians should be permitted to circumvent vehicle TPMs on behalf of the vehicle owners or lessees.

MEMA agrees with AAI that the existing exemption does not extend to conduct prohibited by the Anti-Trafficking Provisions.[27] It is also correct that the Copyright Office "expressed no view on whether particular types of third-party assistance may or may not implicate the anti-trafficking provisions."[28] Rather, the Copyright Office directed us to "separately analyze[]" the Anti-Trafficking Provisions "to determine whether third-party assistance would be permissible." Rather than undertaking this separate analysis, AAI tries to impose its own rule, namely, that all circumvention services violate the Anti-Trafficking Provisions. This *per se* rule of liability is inconsistent with the Copyright Office's own statements, as well as case law that directs a more searching inquiry into the nature of the circumvention services and the nexus between access and protection.

When we separately analyze the conduct discussed here—circumvention by independent automotive repair technicians for purposes of diagnosis, repair, or modification of software on a lawfully acquired vehicle—it is clear that such conduct is permissible under the Anti-Trafficking Provisions and therefore under the existing repair exemption, as well.

[27] AAI, Comment Regarding Proposed Class 12 Exemption, at 3 (February 9 2021).
[28] AAI, Comment in Response to Petitions to Renew the 'Streamlined Renewal Process' Exemption, at 2 (September 8, 2020) (quoting 83 FR 54022).