UNITED STATES COPYRIGHT OFFICE

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

[ ] Check here if multimedia evidence is being provided in connection with this comment.

ITEM A. COMMENTER INFORMATION

The Advanced Medical Technology Association (AdvaMed) is a trade association representing the world's leading innovators and manufacturers of medical devices, diagnostic products, digital health technologies, and health information systems. Together, our members manufacture much of the life-enhancing and life-saving health care technology purchased annually in the United States and globally. AdvaMed members range from the largest to the smallest medical technology producers and include hundreds of small companies with fewer than 20 employees. Our members are committed to developing new technologies and services that allow patients to lead longer, healthier, and more productive lives. The devices made by AdvaMed members help patients stay healthier longer and recover more quickly after treatment and enable clinicians to detect disease earlier and treat patients as effectively and efficiently as possible. Strong intellectual property protections, including copyright protection for source code and device outputs, are essential to developing and bringing medical technologies to market.

Christopher L. White
General Counsel & Chief Policy Officer
Advanced Medical Technology Association (AdvaMed)
1301 Pennsylvania Avenue, NW
Suite 400
Washington, DC 20004
cwhite@advamed.org
202-783-8700

ITEM B. PROPOSED CLASS ADDRESSED

Renewal Class 12: "Computer Programs—Repair of Medical Devices and Systems."[1]

[1] Exemptions To Permit Circumvention of Access Controls on Copyrighted Works, 88 Fed. Reg. 72,013, 72,021–22 (Oct. 19, 2023) ("2023 NPRM").

ITEM C. OVERVIEW

The exemption from liability under 17 U.S.C. § 1201(a)(1)(A) for repair of medical devices and systems ("the Exemption") was wrongly granted and should not be renewed. The Exemption covers "Computer programs that are contained in and control the functioning of a lawfully acquired medical device or system, and related data files, when circumvention is a necessary step to allow the diagnosis, maintenance, or repair of such a device or system."[2] In other words, the exemption allows for the circumvention of technological protection measures (TPMs) to access computer programs and related data files in medical devices and systems.

Original equipment manufacturers (OEMs) include computer programs and data files with the medical devices and systems they sell. Countless medical devices and systems now include software and data files that perform operations ranging from calibrating imaging data to determining the dose of radiation that is provided in a procedure. This breadth of issues and works makes it nearly impossible for proponents (or the Office) to show the effects of the exemption, much less a "particular" class of works under the statute that are worthy of this exemption.

However, no analysis of particular works is required to see that the exemption fails on its face. The exemption only covers non-transformative uses that are entirely for commercial gain. These uses are infringing—not fair use—and therefore, circumventing TPMs to perform those infringing uses cannot be exempted under § 1201(a)(1)(C).

The key error in the Office's 2021 analysis was the finding that the first fair use factor, the purpose and character of the use, favored fair use. The finding as to the first factor led to an incorrect conclusion that the exemption would protect fair uses of copyrighted materials. The exemption, as written, only covers non-transformative uses because the exemption is explicitly limited to repair and does not protect circumvention for modifying or otherwise changing the copyrighted works. Moreover, other recent factual and legal developments undermine the Office's prior rulemaking: the Supreme Court's recent decision in *Andy Warhol Found. for the Visual Arts v. Goldsmith*, and the FDA's 2023 publication of new guidance—Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Guidance for Industry and Food and Drug Administration Staff ("2023 FDA Cybersecurity Guidance").[3] These changes to the legal and factual bases of the exemption warrant a reconsideration of the 2021 decision to grant the exemption.

The first fair use factor weighs the commercial nature of the work against the transformation of that work by the copier of the work.[4] Here, the uses are purely commercial uses by for-profit independent service organizations (ISOs). The exemption does not allow modification of the

---

[2] 37 C.F.R. § 201.40(b)(15) (2023).

[3] *Available at* https://www.fda.gov/media/119933/download. *See also* 88 Fed. Reg. 66,548 (Sept. 27, 2023) (announcing the availability of the Guidance document following notice and comment on same).

[4] *Andy Warhol Found. for the Visual Arts, Inc. v. Goldsmith*, 598 U.S. 508, 532 (2023) ("*Warhol*").

underlying works, so the copiers cannot "transform" the work itself. Since the works are not transformed at all, the uses at issue here are purely commercial non-transformative uses. Those uses decisively cut against a finding of fair use. The Office, therefore, should have found that this non-transformative copying of medical device files and software in the for-profit repair context was not fair use and that a § 1201 exemption could not be granted to allow circumvention for this class of infringing uses.

Additionally, the Office wrongly considered only the public policy considerations favoring an exemption, while ignoring federal policy considerations against the exemption. In particular, the FDA has increased its efforts and guidance on cybersecurity as both a public health and national security issue. If public policy should be considered at all, the FDA's statements about the importance of limiting access to medical devices should be considered determinative. Instead, the Office only relies on public policy arguments to support the exemption.[5] The Office has previously dismissed the public policy problems created by the Exemption's conflict with the FDA's cybersecurity guidance.[6] However, the latest FDA guidance, published in September 2023 (after the present notice of proposed rulemaking), only strengthens the public policy case against the exemption.[7] In other words, if the effect on the medical device market is considered, the Office should look to the FDA—not for-profit ISOs—to decide the policy questions around device security, safety, and repair.

In sum, the Exemption denies DMCA protection to OEM device manufacturers and enables widespread commercial copying of medical device software and files. This kind of commercial non-transformative copying has never been within the scope of fair use, as confirmed by *Warhol*. At the same time, the Exemption undercuts the FDA and industry cybersecurity programs. The result for the US medical system is that thousands of lightly regulated ISOs are free to circumvent security controls on medical devices under an "honor system," so long as they claim not to modify the devices after they obtained unauthorized access. Without the ability to police device access under the DMCA, manufacturers have few options to protect their devices from unauthorized access or to even protect the intellectual property that OEMs invest in creating for their devices. In short, the sweeping 1201 exemption gives government approval to a largely unregulated grey market of commercial medical device hacking, where the effects on patient safety and the industry are impossible to measure. The exemption should not be renewed.

---

[5] See 2023 NPRM at 72021 (quoting a petitioner's assertions about the exemption's benefits to "availability" and "affordability" of medical care).

[6] See U.S. Copyright Office, Section 1201 Rulemaking: Eighth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights 229 ("2021 Recommendation") ("[T]he Register generally does not consider other regulatory schemes as part of the adverse effects analysis ....").

[7] U.S. Food & Drug Administration, Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, Guidance for Industry and FDA Staff (Sept. 27, 2023), *available at* https://www.fda.gov/media/119933/download ("2023 FDA Cybersecurity Guidance").

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

Healthcare demands special care from policymakers and businesses to protect human life, and the TPMs at issue here are recognized as a key to that process. Over the last three years, the FDA has only strengthened its guidance to industry instructing and requiring the use of TPMs in medical devices, culminating in the 2023 FDA Cybersecurity in Medical Devices Guidance.[8]

The FDA instructs OEMs to "identify, assess, and mitigate cybersecurity vulnerabilities as they are identified throughout the supported device lifecycle."[9] OEMs can identify, assess, and mitigate such issues using TPMs. Installing TPMs on medical devices allows OEMs to *identify* the unauthorized access to those devices, *assess* the risks from the unauthorized access, and *mitigate* the risks of unauthorized access by enforcing TPMs and IP rights. The TPMs provide a first line of defense to *identify*, *assess*, and *mitigate* unauthorized access, even before the medical device has been modified, altered, or "hacked" to remove sensitive IP or patient data.

Limiting access to device files and software to only users with special training or certifications is commonly achieved using TPMs. The FDA explains that "cryptographically strong authentication" should be used "to authenticate personnel, messages, commands updates, and as applicable, all other communication pathways."[10] In fact, the 2023 FDA Cybersecurity Guidance explains that "cybersecurity is part of device safety and effectiveness."[11] That document includes 57 pages of guidance about medical device security, including examples of TPMs that should be included to comply:

- Authentication;
- Authorization;
- Cryptography;
- Code, Data, and Execution Integrity;
- Confidentiality;
- Event Detection and Logging;
- Resiliency and Recovery; and
- Updatability and Patchability.[12]

FDA guidance instructs manufacturers that they "are responsible for identifying cybersecurity risks in their devices and the systems in which they expect those devices to operate, and implementing the appropriate controls to mitigate those risks."[13] OEM equipment manufacturers

[8] *See* 2023 FDA Cybersecurity Guidance at 5–6 (explaining that cybersecurity is required by the FDA's quality system regulations including 21 C.F.R. § 820.30).

[9] *Id.* at 19.

[10] *Id.* at 33.

[11] *Id.* at 9

[12] *Id.* at 22.

[13] *Id.* at 20.

(like AdvaMed's members) work to implement FDA guidance in their products to protect the public from Cybersecurity threats.

Petitioners point to an August 2021 Letter from the FDA to the Copyright Office—that the exemption would not "necessarily" harm the safety and effectiveness of medical devices "with respect to cybersecurity" as supporting their position.[14] That same August 2021 Letter concludes that the FDA "has sought stakeholder input on this topic and is evaluating FDA's approach to cybersecurity."[15] Today, the Office continues to rely on this same statement from 2021 as dispositive to whether the exemption jeopardizes healthcare by weakening cybersecurity.

However, the 2023 Guidance shows that the FDA's position on the cybersecurity of medical devices has changed over the last three years. And that change is consistent with guidance across the federal government warning of growing cybersecurity risks. For example, on February 14, 2022, the Health and Human Services Cybersecurity and Infrastructure Security Agency (HHS CISA) issued a "Shields Up" Notice warning stating:

> Every organization in the United States is at risk from cyber threats that can disrupt essential services and potentially result in impacts to public safety. … we are mindful of the potential for the Russian government to consider escalating its destabilizing actions in ways that may impact others outside of Ukraine. Based on this situation, CISA has been working closely with its critical infrastructure partners over the past several months to ensure awareness of potential threats—part of a paradigm shift from being reactive to being proactive.[16]

In sum, the August 2021 Letter cannot be read as the FDA putting its stamp on grey-market device hacking today, when current FDA guidance instructs OEMs to prevent such hacking.

ITEM E. ASSERTED ADVERSE EFFECTS ON NONINFRINGING USES

At the outset, an exemption to 17 U.S.C. § 1201 is only meaningful if there is a protected (i.e., copyrighted) work that is being accessed. Section 1201 only forbids circumvention of technological measures that "control access to a protected work under this title." See

[14] Letter from Suzanne B. Schwartz, Dir., Office of Strategic P'ships & Tech. Innovation, FDA, to Kevin R. Amer, Acting Gen. Counsel & Assoc. Register of Copyrights, U.S. Copyright Office at 3 (Aug. 13, 2021).

[15] *Id.*

[16] HHS CISA Shield's Up Alert Report 202202141700 (Feb 14, 2022)*, available at* https://www.hhs.gov/sites/default/files/cisa-shields-up-alert.pdf.

1201(a)(1)(A). Thus, proponents of the exemption cannot dispute that they are circumventing TPMs to access works protected by the DMCA.[17]

The exemption inherently facilitates copyright infringement because the uses at issue are purely commercial and non-transformative. First, the exemption does not cover access for modification of the copyrighted software or data files. Therefore, the plain language of the exemption prevents the kind of transformative uses of the works that could be fair use. Second, the uses protected by the exemption are purely commercial—not expressive, critical, or educational. This purely non-transformative copying for commercial purposes is copyright infringement, not fair use.

Critically, the Register incorrectly analyzes the "use" of the works at issue here. "[T]he first fair use factor considers whether the use of a copyrighted work has a further purpose or different character." *Warhol*, 598 U.S. at 532–33. Here, both the original "use" of the work (operating a medical device or system) is identical to the use of the work after the copying of the works by the ISO. The work—the software or files on the medical device—is not transformed at all by the ISOs. In fact, the work cannot be transformed under the exemption, which forbids modification. Thus, there is no transformative "use."

The Register relies on its own previous exemptions and determinations to argue that "repair" as a category is fair use.[18] But those decisions are not analogous to the present exemption. For example, the Office points to a finding that "jailbreaking" cell phones is allegedly fair use.[19] However, the Register characterized circumventing those TPMs as "noncommercial and personal" uses.[20] Here, the exemption is exactly the opposite: it covers *commercial* servicing of equipment for *public* health. As another example, the Register points to its finding that circumvention of vehicle systems to "create new applications and/or tools that can interoperate with [vehicle] software" is an allegedly fair use.[21] But here, the exemption does not protect "new" applications or tools, since it does not permit ISOs to modify the machines they work on.

---

[17] Proponents have previously suggested that the TPMs protect allegedly non-copyrightable "data files, error logs, configuration files." *See* 2021 Recommendation at 200 n.1093. But the 2021 Recommendation recognized that at least some "medical device and system data files may be protectable compilations" and therefore that a fair use analysis was required to determine if the TPMs were being circumvented for noninfringing uses. *Id.*

[18] See 2021 Recommendation at 211 n.1167 (citing 2018 Recommendation discussing vehicle repair before discussing video game consoles and 2015 Recommendation discussing phone jailbreaking and vehicle repair).

[19] U.S. Copyright Office, Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyrights 234-235 (2015) ("2015 Recommendation").

[20] U.S. Copyright Office, Section 1201 Rulemaking: Fifth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention, Recommendation of the Register of Copyright 74 (2012).

[21] 2015 Recommendation at 234.

Simply put, the Register relies on prior findings about various noncommercial uses (jailbreaking) and transformative uses (creating new vehicle software) and stretches them to support the present exemption that covers *commercial* and *non-transformative* uses. Had the drafters of the DMCA or the Copyright Act wished to universally exempt repair services from copyright, they had ample opportunity to do so. But neither the DMCA nor the Copyright Act carve out such an exemption.[22]

On the contrary, a correct analysis of the fair use case law shows that these uses are not fair. To start, the Supreme Court in *Campbell* explained that the first factor is "whether the new work 'merely supersede[s] the objects' of the original creation."[23] Or whether it "adds something new, with a further purpose or a different character, altering the first with new expression, meaning or message … in other words, whether and to what extent the new work is 'transformative.'"[24] Here, the "new work" is an unmodified exact copy of a medical device software file. The use of those files is for the same purpose—operating the same medical machine—and by the terms of the exemption, the copiers add no new "expression meaning or message." Thus, a proper analysis of the "use" of the copyrighted works here shows that those uses are non-transformative.

Warhol only strengthens this argument. *Warhol* held that the "first fair use factor considers whether the use of a copyrighted work has a further purpose or different character." The *work* (the software subject to the exemption) is used for the same purpose and character—operating the medical devices and systems. *Warhol* confirms that when "an original work and a secondary use share the same or highly similar purposes, and the secondary use is of a commercial nature, the first factor is likely to weigh against fair use."[25] That is exactly the situation here. In short, *Warhol* confirms that the Register must look to the *use* of the copied work to determine whether the ultimate use of the infringing work is transformative. Since the "use" of the software and data files is the same before and after the repair, that "use" is not a transformative fair use.

Finally, the Supreme Court's analysis of fair use in the software field further undercuts the Register's analysis. The 2023 NPRM continues to rely on *Google LLC v. Oracle America, Inc.* as supporting the determination that repair is fair use.[26] But in *Google,* the copying at issue was a Java API created by Oracle that allowed programmers to call up other implementing programs—not the entirety of the work. The Court explained that Google's use of those APIs was "to create new products" and to "expand the use and usefulness of Android-based smartphones."[27] Google's use of Oracle APIs was based on the "very creativity that was needed to develop the

---

[22] 17 U.S.C. § 117(c) protects specific uses of copying software for repair when "such a new copy is used in no other manner and is destroyed immediately after the maintenance or repair is completed." The Register's 2021 analysis focused on the broader fair use analysis which is not as limited as 17 § USC 117.

[23] *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994).

[24] *Campbell*, 510 U.S. 569.

[25] *Warhol*, 598 U.S. at 532

[26] 2023 NPRM at 72022.

[27] *Google LLC v. Oracle Am.*, Inc., 141 S. Ct. 1183, 1203 (2021)

Android software for use not in laptops or desktops but in the very different context of smartphones."[28] Thus, the Supreme Court recognized that Google's use of the Oracle code was transformative because it created new products, expanded the usefulness of those products, and adapted that code to a different computing environment (smartphones) instead of desktops. None of the facts in *Google* that favored a finding of transformative use are present here. Again, the ISOs' use of copyrighted works is for exactly the same use (operating the machine) in exactly the same computing environment (the same machine) and, under the terms of the exemption, the ISOs cannot modify the code at all, much less perform the kinds of innovative improvements that Google claimed.

Cases decided both before and after *Warhol* confirm that the analysis of the use depends on how the work is being put to use. In *Oracle v. Rimini Street*, the defendant Rimini made much the same argument as the Office does here—that the context of its use (creating software tools) was different in character than the original work (Oracle's software).[29] The district court rejected the argument that Rimini's use was transformative, holding that "when Rimini made copies of PeopleSoft to develop and test its Automated Tools, Rimini 'put those [PeopleSoft] copies to the identical purpose as the original software. Such a use cannot be considered transformative.'"[30]

Rimini's argument in *Oracle* was essentially the same as the Register's argument here—that the context of the infringement can be a transformative use, even if the copy of the work is used in the same way as the original work. But the district court in *Oracle* held, citing *Warhol* and *Harper*, that the correct analysis was whether the copies were "put … to the identical purpose as the original software."[31] Here, as in *Oracle*, any copies being made by ISOs are "put … to" the identical purpose as the original software: operating the medical device or system. Thus, those uses are not transformative, whether they are in the "context" of developing other tools (as in *Oracle*) or in the context of repairing existing tools (as in the present exemption).

Pre-*Warhol* precedent came to this same conclusion. In *Wall Data Inc. v. Los Angeles County Sheriff's Department*, the Ninth Circuit explained that "a use is considered transformative only where a defendant changes a plaintiff's copyrighted work or uses the plaintiff's copyrighted work in a different context *such that the plaintiff's work is transformed into a new creation*."[32] Here, the ISOs' use cannot change the copyrighted work under the exemption. And the ISOs clearly do not use the work in a "different context such that the plaintiff's work is transformed into a new creation." Instead, the "creation" of an ISO is at best a machine that works as it originally did—not a "transformed … new creation" that could be a fair use.

---

[28] *Id.* at 1202

[29] *Oracle Int'l Corp. v. Rimini St., Inc.*, No. 2:14-CV-01699-MMD-DJA, 2023 WL 4706127, at *76 (D. Nev. July 24, 2023)

[30] *Id.* (alteration in original) (quoting *Wall Data Inc. v. Los Angeles Cnty. Sheriff's Dep't*, 447 F.3d 769, 778 (9th Cir. 2006)).

[31] *Id.*

[32] 447 F.3d 769 (9th Cir. 2006) (emphasis added).

The defendant in *Wall Data* also raised similar arguments to the ISO proponents of the exemption here, claiming that the commercial harm to the plaintiff was insignificant and that uses of the work saved time, effort, and money.[33] But the Ninth Circuit rejected these arguments and concluded that the use was "not transformative, did not promote an advancement of the arts, and was commercial in nature"—ultimately holding that a fair use defense did not apply.[34]

In sum, the exemption wrongly protects large-scale, non-transformative commercial use that is not protected by fair use. The adverse effect on non-infringing uses is, therefore, minimal (or nonexistent). Moreover, the cybersecurity and health implications of the exemption involve issues of national security and patient safety that deserve special consideration from the Office to avoid undercutting the executive branch's policies. The Copyright Office should not renew the exemption.

DOCUMENTARY EVIDENCE

None.

[33] *Id.* at 779.

[34] *Id.* at 780.