Before the
U.S. Copyright Office
Library of Congress
Washington, D.C.

In the Matter of

Exemption to Prohibition on	**)**
Circumvention of Copyright	**) Docket No. 2014-7**
Protection Systems for Access	**)**
Control Technologies	**)**

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

Item 1. Commenter Information

National Association of Manufacturers
733 10th Street NW, Suite 700
Washington, DC 20001
(202) 637-3000

Item 2. Proposed Class Addressed

These comments address Proposed Exemption 27: Software-Networked Medical Devices.

Item 3. Overview

The National Association of Manufacturers ("NAM") is a nonprofit trade association representing small and large manufacturers in every industrial sector and in all 50 states; the NAM is the preeminent U.S. manufacturers' association as well as the nation's largest industrial trade association.

The NAM opposes Proposed Exemption 27 on the grounds that:

- Proponents have failed to meet their burden of producing "highly specific, strong, and persuasive" evidence that the prohibition on circumvention of access controls related to "medical devices designed for attachment to or implementation in patients and in their corresponding monitoring devices, as well as the outputs generated through those programs" will cause a "substantial adverse impact" in their ability to make noninfringing uses;

- The availability of other means to achieve the ends described by the Proponents obviates the need for an exemption; and

- The potentially catastrophic adverse consequences that may result from an exemption to the prohibition on circumvention counsels in favor of denying the proposed exemption, or at least seeking further guidance from the Food and Drug Administration (FDA).

The NAM's concerns are particularly acute in the context of medical devices that are attached to or implanted in patients. These devices perform monitoring and regulation of critical human functions including, for example, the pace and rhythm of a heartbeat and glucose levels in the bloodstream. Manufacturers have invested significant time and resources to implement Technological Protection Measures (TPMs) in these devices to ensure that they operate according to the specifications designed and tested by the manufacturers and approved by the FDA. If a patient or researcher—no matter how well-intentioned—interferes with the expected operation of one of these devices, the consequences can be fatal.

The breadth of the proposed exemption makes it difficult, if not impossible, to comprehend all of the potential adverse effects of the proposed circumvention. Although the Proponents appear to focus on pacemakers, implantable cardioverter defibrillators, insulin pumps, and continuous glucose monitors, the class of medical devices designed for attachment to or implementation in patients is actually much broader. Even more troubling is the breadth of applications for the proposed exemption. As drafted, the exemption would permit "those conducting research"—a potentially limitless class—to circumvent TPMs on implanted or attached devices. Such a broad exemption would be extremely problematic and dangerous for patients.

On balance, the strong risks to patient safety from circumvention strongly outweigh the theoretical, unsubstantiated harms created by the prohibition. Accordingly, the totality of the statutory factors weighs in favor of denying the exemption.

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

The security and stability of the products that they sell is of the utmost concern to America's manufacturers. The use of TPMs enhances the customer experience by ensuring that the goods operate according to manufacturer specifications and by preventing unwanted or unintended tampering. Manufacturers apply a variety of different TPMs that are appropriate for the specific products at issue. When considering what type of TPM to adopt, manufacturers must account for, *inter alia*: (i) the nature of the protected material (whether the information is subject to privacy laws or otherwise constitutes private information and the effect that unintended access could have on the operation of the products at issue); (ii) the effectiveness of a particular TPM; (iii) the cost of implementing the TPM; and (iv) the how the use of that TPM will affect the operation of the device for its intended purpose. For example, the U.S. Government Accountability Office (GAO) has recognized that the limited battery life of some medical devices "hinders the possibility of adding security features" that "require more power than the battery can deliver."[1] Further, strong authentication protocols could "hinder[] health professionals' ability to provide care to patients in emergency situations."[2] Manufacturers, thus,

[1] *See* GAO, *Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices* 16 (Aug. 2012) ("GAO Report").

[2] *Id.* at 17.

must constantly evaluate, test, and re-evaluate the effectiveness of TPMs and strike the appropriate balance between security and functionality. Manufacturers may change the TPMs used in any particular device—subject to obtaining the necessary regulatory approvals—to incorporate new technology and respond to changing threats.

The NAM agrees with the Proponents that the TPMs that control access to medical devices and their corresponding monitoring systems "are wide-ranging."[3] While the number of methods that the Proponents have identified for circumventing these TPMs is plentiful, they are noteworthy both for their intrusiveness and for the potential strain that they will place on the target devices. For example, the Proponents explain that accessing the computer code and outputs of medical devices "requires significant experimentation."[4] Testing for defects and vulnerabilities, meanwhile, requires inputting "malformed data into a device in order to find its defects."[5] The prospect of anyone who self-identifies as a "researcher" applying trial-and-error experimentation methods to modify the software in life-saving medical devices is particularly troubling. At the very least, such efforts will tax the devices' scarce power resources, reducing the effectiveness of the devices. In recognition of the severity of these concerns, the Proponents claim that much of this work occurs on devices that are not being used for patient care.[6] As drafted, however, the exemption would permit the application of circumvention tactics to even active, implanted devices, with potentially catastrophic results.

Item 6. Asserted Adverse Effects

As the Copyright Office has acknowledged, the crux of the triennial rulemaking proceeding is "whether a 'substantial dimunition' of the availability of works for noninfringing uses is 'actually occurring' in the marketplace."[7] The Proponents of Exemption 27 have failed to satisfy their burden of demonstrating that the TPMs at issue have or are likely to have adverse effects on the asserted noninfringing uses. All the Proponents have offered is conjecture and speculation about what may potentially occur in the marketplace. In fact, there is little reason to believe that the use of TPMs will substantially restrict the use of the works for noninfringing uses. Manufacturers have both the incentive to ensure the security and stability of their products and demonstrated records of making their copyrighted software and code available for research, analysis, and testing by qualified independent parties. Moreover, it is incumbent on the Register and the Librarian to "take into account the adverse effects" the proposed exemptions have "on the market or value of the copyrighted works."[8] When considering these issues in their totality, it is evident that there is no justification to grant the proposed exemption.

---

3 *See* Medical Device Research Coalition, *Petition of a Coalition of Medical Device Researchers for Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, Docket No. 2014-07 2 (Nov. 3, 2014).

4 Medical Device Research Coalition, *Comment of a Coalition of Medical Device Researchers in Support of Proposed Class 27: Software – Networked Medical Devices*, Docket No. 2014-07 10 (Feb. 6, 2015) ("MDRC Comments").

5 *Id.*

6 *Id.*

7 *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, Notice of Inquiry, 79 Fed. Reg. 55687, 55690 (Sept. 17, 2014) ("NOI").

8 *Id.* at 55691.

A. The Proponents Have Not Satisfied Their Burden to Identify "Distinct, Verifiable, and Measurable Impacts" of the Section 1201 Prohibition.

As the Copyright Office repeatedly has acknowledged, proponents of an exemption to the Section 1201 prohibition bear the burden of demonstrating harm from the application of the applied TPMs.[9] Specifically, Proponents must show that "the prohibition is causing, or in the next three years is likely to cause, an adverse impact on those uses."[10] The legislative history to the DMCA explains that "the rulemaking proceeding should focus on distinct, verifiable and measurable impacts" and "should not be based upon *de minimis* impacts."[11] The Copyright Office applies this "distinct, verifiable and measurable impacts" standard.[12]

Proponents can satisfy the adverse effect requirement through one of two methods. First, they can demonstrate that a "'substantial diminution' of the availability of works for noninfringing uses is 'actually occurring' in the marketplace."[13] In making this showing, however, the Copyright Office has stressed that evidence of "mere inconveniences" or "individual cases" will not suffice.[14] Second, proponents can demonstrate that the prohibition will result in future impacts, but "'only in extraordinary circumstances in which the evidence of likelihood of future adverse impact during that time period is highly specific, strong and persuasive."[15]

The Proponents of Exemption 27 have failed to satisfy either standard for demonstrating distinct, verifiable and measurable adverse impacts. With regard to *actual* harm now resulting from the prohibition on circumvention, Proponents have cited to only a single example--a statement by Proponent Jerome Radcliffe, referring to limitations on research that he presented in 2011.[16] Despite the alleged adverse effects, however, Mr. Radcliffe explains that his research "gained international attention and led to a collaboration with the Department of Homeland Security and

---

9 *See Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, Final Rule, 77 Fed. Reg. 65260, 65261 (Oct. 26, 2012) ("2012 Final Rule") ("In order to establish a *prima facie* case for designation of a particular class of works, the proponent must show that: (1) Uses affected by the prohibition on circumvention are or are likely to be noninfringing; and (2) as a result of a technological measure controlling access to a copyrighted work, the prohibition is causing, or in the next three years is likely to cause, a substantial adverse impact on those uses.").

10 NOI at 55690; *accord* Digital Millennium Copyright Act of 1998, H.R. Rep. No. 105-551, pt. 2 at 6 (1998) ("Commerce Committee Report") ("The focus of the rulemaking proceeding must remain on whether the prohibition on circumvention of TPMs (such as encryption or scrambling) has caused any substantial adverse impact on the ability of users to make non-infringing uses."); *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, Final Rule, 75 Fed. Reg. 43825, 43826 (July 27, 2010) ("[P]roponents must show by a preponderance of the evidence that there has been or is likely to be a substantial adverse effect on noninfringing uses by users of copyrighted works."); Recommendation of the Register of Copyrights in RM 2002-4, at 177 (Oct. 27, 2003) ("2003 Register's Recommendation") ("The role of this rulemaking process is to determine whether noninfringing uses of particular classes of works are adversely affected by the prohibition on circumvention of technological measures that control access to works.").

11 Commerce Committee Report at 37.

12 *See* NOI at 55690.

13 *Id.*

14 *Id.*

15 *Id.* (quoting H. Comm. on the Judiciary, 105th Cong., *Section-by-Section Analysis of H.R. 2281 As Passed by the United States House of Representatives on August 4, 1998*, at 6 (Comm. Print 1998)).

16 *See* MDRC Comments at 20; Statement by Jerome Radcliffe, App'x D to MDRC Comments ("Radcliffe Statement"), ¶¶ 1,3.

the Food and Drug Administration."[17] Thus, any purported adverse effects on research resulting from the prohibition on circumvention are of the *de minimis* nature that does not meet the rulemaking standard. In fact, contrary to the unsupported assertion in the body of the MDRC Comments about a chilling effect on other researchers, Mr. Radcliffe observes that he is an anomaly, and that "[m]ost in the security industry do the research first and hope that they were on the right side of the law and don't get in trouble."[18] Thus, the Proponents have not satisfied their burden of demonstrating that the prohibition has had distinct, verifiable and measurable adverse impacts on the noninfringing uses.

Proponents also have failed to satisfy the heightened burden to provide "highly specific, strong and persuasive" evidence regarding the likelihood of future impacts. The Proponents offer no evidence to support their assertions about the "risk of the DMCA chilling this form of medical device research."[19] At most, the Proponents have inferred that manufacturers will expand their use of TPMs over the next three years.[20] This alone, however, will not result in a diminution of the works for noninfringing purposes, and it certainly does not constitute highly specific, strong and persuasive evidence thereof. Moreover, despite the increased use of TPMs, manufacturers and the FDA remain steadfast in their commitment to patient safety and to the security of implanted medical devices. As such, there is no basis for finding that the Proponents have met their rigorous burden of proof of establishing actual or likely adverse impact if no exemption is granted.

B. <u>There Is No Compelling Need for the Requested Exemption.</u>

Notwithstanding the failure of Proponents to satisfy their burden to establish a *prima facie* case for exemption, alternative means of accessing the works obviate the need for the requested exemption. Proponents identify two types of works to which they seek access: (i) the data outputs of medical devices; and (ii) the computer code that directs the operation of the protected devices. Both of these can be accessed for legitimate medical and research purposes without the need for circumvention.

The suggestion by Proponents that medical devices "withhold" data is completely misleading. Implantable cardioverter-defibrillators, such as the one used by one of the Proponents, measure data that, as Proponents concede, is available through periodic checkups with qualified medical professionals.[21] Medical professionals accesses this information using a programmer, which is "a specialized computer used to transmit data and to check the defibrillator's functionality and usage."[22] It is this through this controlled access to data stored on the devices that manufacturers are able to both protect sensitive patient information and ensure a safe and secure operating environment. Proponents have offered no evidence that patients are unable to obtain their data from qualified medical professionals when requested. The issue, then, is not that the TPM prevents patients from obtaining their data for a noninfringing use, but simply that the data is not

---

17 Radcliffe Statement ¶ 1.
18 *Id.* ¶ 3.
19 MDRC Comments at 20.
20 *Id.* at 9.
21 *Id.* at 3; Statement of Hugo Campos, App'x C to MDRC Comments ¶ 7.
22 GAO Report at 6.

available at a particular frequency or without the need to interact with a medical professional. This is not the type of "distinct, verifiable, and measurable" adverse impact that warrants an exemption to the prohibition.

Moreover, there are myriad alternatives for research and commentary regarding the security and performance of medical devices without the need for an exemption. For example, the FDA recently sponsored a public workshop regarding "Collaborative Approaches for Medical Device and Healthcare Cybersecurity."[23] The workshop brought together "all stakeholders in the healthcare and public health (HPH) Sector including but not limited to medical device manufacturers, healthcare facilities and personnel (e.g. healthcare providers, biomedical engineers, IT system administrators), professional and trade organizations (including medical device cybersecurity consortia), insurance providers, cybersecurity researchers, local, State and Federal Governments, and information security firms."[24] Additionally, device manufacturers work in conjunction with independent researchers to provide for testing and analysis of devices in a secure and safe environment. A leader in this effort is the Archimedes project at the Ann Arbor Research Center for Medical Device Security. Archimedes holds an annual workshop on medical device security and maintains a library of medical devices that can be used for many of the same research purposes identified by the Proponents.[25] Through these, and other, efforts, the use of TPMs does not substantially interfere with noninfringing use of the copyrighted works stored on medical devices.

Given the presence of numerous viable alternatives to circumvention, the requested exemption is unwarranted, particularly in light of the countervailing considerations explained below.

C. The Adverse Consequences of the Exemption Outweigh Any Possible Benefits.

Any consideration of the proposed exemption must start from the position that the devices at issue are highly-regulated devices that control vital human functions. In simple terms, if the process of circumvention interferes with the operation of a DVD player or a mobile telephone, the result is a non-functioning "brick"; if the process of circumvention interferes with the operation of an attachable or implantable medical device, the result to the patient could be fatal. The sequences that could lead to these devastating results are well-documented.

When evaluating a proposed exemption, the Register and the Librarian must account for "the adverse consequences that may result from the exemption to the prohibition on circumvention."[26] The Copyright Office has already recognized the potential import of this consideration in the context of the instant proposed exemption, asking "[w]hether granting the exemption could have negative repercussions with respect to the safety or security of the relevant medical devices, for example, making it easier for wrongdoers to access such medical devices' software or outputs."[27]

---

23 *See* FDA, *Public Workshop – Collaborative Approaches for Medical Device and Healthcare Cybersecurity, October 21-22, 2014*, http://www.fda.gov/MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm.

24 *Id.*

25 *See* Archimedes, www.secure-medicine.org.

26 2012 Final Rule at 65261.

27 *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, Notice of Proposed Rulemaking, 79 Fed. Reg. 73856, 73871 (Dec. 12, 2014).

Permitting circumvention of TPMs on medical devices could pose a grave risk to patient safety. First, tampering with a device that is implanted or attached or that may be implanted or attached at a later date, could interfere with the intended operation of the device. Given the life-saving nature of many medical devices, the consequences could be fatal. Second, any increased telemetry—whether to obtain data interpreted by the device or to extract and circumvent the device software—results in a greater use of electrical current than anticipated, which could, at best, shorten the life of the device and, at worst, cause non-operation. Finally, even in the rare circumstance where a vulnerability or flaw is detected, manufacturers are in the best position to control the publication and response to such issues, including coordinating with the FDA where appropriate, in a manner that is consistent with protecting patient safety.

The primary concern of any manufacturer is the safety of its products. Manufacturers of all types invest heavily in research and development to ensure that their products are safe to use. This is particularly true of medical device manufacturers. Implantable and attachable medical devices frequently provide vital functions—such as regulating the operation of critical organs and controlling the administration of essential hormonal supplements. In recognition of the potential risks should these devices not operate properly, they are subject to strict regulation by the FDA. As the GAO has explained, "FDA's regulation of medical devices is intended to provide the public with reasonable assurance that medical devices are safe and effective and do not pose a threat to public health."[28]

Permitting anyone purporting to conduct research "into the safety, security, and effectiveness" of such devices to circumvent the protective mechanisms installed by the manufacturer and approved by the FDA would undermine the public trust and cause a drastic setback in the quality of American healthcare. Manufacturers have developed extensive testing and quality control practices designed to ensure that their devices operate according to manufacturer specifications. No testing regime, however, can control for the possibility that a self-identified "researcher" will employ a trial-and-error experimentation process to circumvent TPMs and modify the underlying software. As a result, devices subject to circumvention would operate outside of the standards adopted by the manufacturer and approved by the FDA. The risk to patient safety from the use of what would essentially be unauthorized medical devices could be devastating to patients. Moreover, the proliferation of device failures due to circumvention activities could have the unintended consequence of deterring patients from utilizing these life-saving technologies.

Another concern relates to the toll that even skilled operation under the exemption would place on the effectiveness of implanted devices. Manufacturers design implantable devices to make efficient use of limited battery supplies, thereby extending the life of the devices. Any circumvention efforts that require greater use of telemetry than under normal operating conditions would accelerate battery drain, necessitating increased surgical procedures or, in the worst case scenario, causing the devices to stop performing their critical medical functions prematurely. Either scenario would increase the risk of harm to the patient.

Finally, permitting parties to circumvent TPMs in the name of conducting security research could jeopardize the security of implanted devices. The Proponents seek to downplay this risk, claiming that researchers are generally cautions about the information that they release and that,

[28] GAO Report at 8.

in any event, malicious attacks on medical devices are rare.[29] Even if most researchers are well-intentioned and careful about what information they publicly release, however, the consequences of placing the wrong information into the wrong hands are too grave to ignore. This is particularly true because even after a vulnerability has been identified and a solution developed, manufacturers typically must still obtain regulatory approval before deploying the solution to any devices. In the meantime, persons with malicious intent could exploit existing vulnerabilities published by the "researchers," creating a severe risk to patient safety. Manufacturers should be able to mitigate this risk by controlling the settings and terms under which independent research into device security and functionality is conducted by qualified researchers.

Item 7. Statutory Factors

When applying the statutory factors, the Register and the Librarian must balance any perceived benefits from granting the exemption against the adverse consequences documented herein. Given the substantial and potentially life-threatening adverse effects of circumvention, extreme caution is warranted. At the very least, denial of the proposed exemption would be appropriate until the FDA develops a more complete record about the benefits and risks of third party research into implanted and attached medical devices. In the meantime, manufacturers will continue to focus on developing products that improve patient health in a safe and reliable manner.

_____

Brian J. Raymond
Director, Technology and Domestic Economic Policy
National Association of Manufacturers
March 27, 2015

[29] MDRC Comments at 22.