Before the
United States Copyright Office
Library of Congress

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. 2014-7

REPLY COMMENTS OF PUBLIC KNOWLEDGE

1. Commenter Information

These reply comments are respectfully submitted by Public Knowledge. Public Knowledge is a nonprofit organization dedicated to representing the public interest in digital policy debates. Public Knowledge promotes freedom of expression, an open Internet, and access to affordable communications tools and creative works.

Interested parties are encouraged to contact Sherwin Siy (ssiy@PublicKnowledge.org) as Public Knowledge's authorized representative in this matter. Public Knowledge's contact information is as follows:

Public Knowledge
1818 N St. NW
Suite 410
Washington, DC 20036
(202) 861-0020

2. Proposed Class Addressed

These reply comments address Proposed Class 27: Software – networked medical devices. Specifically, they address objections to the proposed exemption raised by the Advanced Medical Technology Association ("AdvaMed"), the Intellectual Property Owners Association ("IPO"), Jay Schulman, LifeScience Alley, and the National Association of Manufacturers ("NAM"). These reply comments refer to these commenters as "Respondents."

3. Overview

The Office and the Librarian should grant the exemption request made by the Medical Device Research Coalition and the Berkman Center. Objections raised by Respondents are tangential or irrelevant to the factors at issue in this proceeding, and

would require that a proceeding in a forum nominally about and expert in copyright law should act as a barrier to progress in matters of health, safety, and privacy.

Respondents' objections tend to focus upon two areas: concern for patient safety and privacy (and thus an appeal for the involvement of the Food and Drug Administration ("FDA")) and whether or not there is a demonstrated harm absent the exemption. Respondents also object to the breadth of the exemption request, and some assert that the proposed uses infringe copyrights in software or data formats.

Each of these objections fails to overcome the compelling case made by Petitioners for the need to access medical devices and the clearly noninfringing nature of their proposed uses.

4. **Technological Protection Measures**

Respondents note the wide range of technological protection measures ("TPMs"), and the wide range of their uses. In fact, Respondents specify that TPMs are used to prevent access to a variety of systems and information, including trade secrets, patient information, patents,[1] and raw data. None of these things constitute works protected by copyright, and thus circumvention of TPMs that restrict access to them would *per se* not violate Section 1201, and thus not be within the scope of this rulemaking.

Nonetheless, many TPMs are likely to restrict access to more than one type of information, including copyrighted works. To the extent that Respondents' TPMs are intended to protect patient information, trade secrets, and other uncopyrightable matter, the fact that circumvention incidentally also allows access to a copyrighted work should not act as a barrier.

Respondent NAM also notes the need for manufacturers to constantly evaluate, test, and change TPMs. The rapidity of such changes is one of many reasons why Proponents must request exemptions for a broadly defined class of works, TPMs, and circumvention methods. In the time between triennial reviews, TPMs and their applications can change rapidly in medical devices. Such changes should not bar legitimate circumvention, which they easily could in the face of an overly narrow exemption grant.

5. **Noninfringing Uses**

Respondent IPO baldly states that "permitting unregulated access to the software would permit infringement of copyright in the software." This is either simply false, or a tautology. Proponents are not asking for permission to infringe copyrights, nor is it within the scope of this rulemaking for the Librarian or Office to grant permission to infringe. If IPO means that granting circumvention for noninfringing purposes would create conditions that allow infringement, its argument proves little. First, an individual who has

[1] How access to patented information is effectively restricted by a TPM, when a core requirement of patent law is public disclosure of the invention, is unclear.

the means to circumvent TPMs and the interest in infringing copyrights is unlikely to be stopped by a legal prohibition on the circumvention. Secondly, it is understood and uncontroversial that users circumventing for a noninfringing purpose will, having circumvented a TPM, have the opportunity to make infringing uses of the work. This has never been a barrier to the Librarian or the Office granting exemptions in the past, nor should it be now.

IPO does not specify what users' activities it believes will infringe its copyrights. Simple use of the software, including essential-step copies made by patients or researchers in the course of using the devices alongside new data outputs, would be fleeting enough not to generate "reproductions" cognizable under Section 106;[2] would be protected under Section 117's essential-step[3] and repair[4] defenses; or would be fair uses.

While fair use us a fact-based analysis, the bounds of the Proponents' request provide sufficient certainty that any use qualifying under the exemption would be fair. The purpose of the use would be furthering research—a quintessential fair use[5]—or for the purposes of improving the health and well-being of individual circumventing patients. The copyrighted works involved are purely functional in nature, containing arguable amounts of creative expression mixed in with unprotectable facts and functional elements. While the whole of the program will likely be used in gaining access, using the totality of a work is never a bar to a finding of fair use, either.[6] Nor will Proponents' proposed uses supplant the market for or cannibalize the value of the copyrighted software at issue. Merely accessing and modifying single copies of the embedded software does not supplant the fact that the software has been paid for already—if indeed there is a market for the software itself, as opposed to the devices that contain it.

Respondent AdvaMed provides its own fair use analysis, but can only speculate that Proponents *might* not meet the purpose and amount and substantiality prongs. With regard to purpose, it asks if a given circumventer might be doing so for profit. Even if the answer to this rhetorical question were "yes," this would not bar a finding of fair use.[7]

In contrast to a fair use analysis based upon the known characteristics of the exemption class, AdvaMed's analysis speculates that a single portion of a single non-dispositive element may in some cases militate against a finding of fair use. AdvaMed does not attempt to argue that the nature of the copyrighted works or the effect on the

---

[2] *See*, *e.g., Cartoon Network, LP v. CSC Holdings, Inc.*, 536 F.3d 121 (2d Cir. 2008).
[3] 17 U.S.C. § 117(a)(1).
[4] 17 U.S.C. § 117(c).
[5] 17 U.S.C. § 107 (uses for the purposes of "scholarship or research" are fair).
[6] *See, e.g., Campbell v. Acuff-Rose Music*, 510 U.S. 569, 586-87(1994) (analysis is not merely quantity taken, but whether the quantity taken is "reasonable in relation to the purpose of the copying"); *Perfect 10, Inc. v. Amazon, Inc.*, 508 F.3d 1146, 1167-68 (9th Cir. 2007).
[7] *See*, *e.g., Campbell*, 510 U.S. 569, 584. "The language of the statute makes clear that the commercial or nonprofit educational purpose of a work is only one element of the first factor enquiry into its purpose and character... If, indeed, commerciality carried presumptive force against a finding of fairness, the presumption would swallow nearly all of the illustrative uses listed in the preamble paragraph of § 107, including news reporting, comment, criticism, teaching, scholarship, and research, since these activities are generally conducted for profit in this country."

potential market for or value of the works (arguably the most significant of the four factors) weigh against fair use. Taken together, none of the arguments made by AdvaMed can overcome the weight of the elements in favor of a finding of fair use.

AdvaMed also raises infringement concerns regarding the data outputs generated by medical devices: "[C]opyright protection in device outputs *may* extend to, for example, the structure, format, and arrangement of the output data" (emphasis added). The mere *possibility* of a portion or the output being copyrighted is insufficient to deny the exemption for all proposed circumventions.

Moreover, the possibility of infringement of a data format copyright is low. AdvaMed cites *Engineering Dynamics*[8] and *Positive Software Solutions*[9] for the simple proposition that certain arrangements of data can be protected by copyright. Neither case, however, holds that all structures, formats, or arrangements of data are protectable, nor does either case contradict the bedrock principle that the use of the factual data housed within them is not infringing.

Since at least *Baker v. Selden*,[10] it has been clear that a system or arrangement of factual information can very easily fall outside of the realm of copyright. Merely stating the possibility of a copyrightable data structure does nothing to indicate that the medical devices at issue here are producing data structured and arranged in such a way as to be copyrightable.

Furthermore, the data being used by Proponents is not necessarily the structured outputs that might bear a thin copyright protection. Unlike the alleged infringers in *Engineering Dynamics* and *Positive Software Solutions*, who sought to make competing products, Proponents intend to use the output data to convey the raw information contained within any data structures.

Finally, even assuming *arguendo* that some data structures may be copyrightable *and* that the copyrightable expression is what is taken by Proponents, its use in the context of the proposed exemption as easily falls within the scope of fair use as the use of any potential copyrighted software.

6. **Adverse Effects and Alternatives**

In setting standards for this rulemaking, Section 1201 requires the Librarian to assess the adverse effects of the circumvention prohibition upon users, not potential adverse effects that might follow from the grant of an exemption. While those latter effects are relevant to the rulemaking consideration, they must fit within the additional statutory factors including "the effect of circumvention on the market for or value of copyrighted works." Respondent comments directed towards effects on patient privacy and safety are therefore dealt with in part 7 below.

[8] 26 F.3d 1335 (5th Cir. 1994).
[9] 259 F. Supp. 2d 531 (N.D. Tex. 2003).
[10] 101 U.S. 99 (1880).

Respondents fail to counter Proponents' extensive record of inability to access medical device software and data and the harms that result. Instead, they claim that a lack of litigation demonstrates a lack of adverse effects from prohibition, that access to data via contact with a doctor or other medical professional will suffice, or that a select number of specific research programs can serve to provide access to all. Each of these arguments is inadequate.

Litigation Is Not the Sole Means of Measuring Adverse Effects

IPO claims the exemption is unnecessary, absent "reports of a Section 1201 action ever being threatened or brought against any medical device researcher" or "evidence that any research has been stopped by a Section 1201 claim." As with all exemption categories, the presence of a statutory prohibition is sufficient to act as a barrier to law-abiding users. A legal communication from a rightsholder, much less a complaint, is not a prerequisite to showing an adverse effect upon lawful activity. Even the potential for liability chills legitimate activity, especially when directed at individual patients already facing medical costs or researchers having to justify potential legal risks of a proposed project. Not all institutions or organizations have a legal department willing to measure, much less take on the legal or financial risk of a lawsuit.

Furthermore, it should be obvious in the medical context that litigation is not the only measure of adverse effects upon a user group. Proponents have shown in detail how chilling independent research leads to reduced device safety, and how lack of timely information to patients can directly threaten an individual patient's health. These are far more concrete and direct harms than a head count of complaints asserted under Section 1201 can provide.

Existing Means of Access Fail as Substitutes for Circumvention

LifeScience Alley cites the existence of DHS investigations of particular cybersecurity breaches, a set of Congressional hearings on cybersecurity issues, and a single collaboration between NIST and the University of Minnesota as evidence that an exemption is unnecessary. NAM notes that the FDA once held a public workshop on device security, and that manufacturers will occasionally collaborate with independent researchers to test their own products. AdvaMed cites the same FDA workshop and notes one more planned for this month. These scattered examples of work in the relevant and adjacent fields do not suggest by any means that the demand for access is being met. A Congressional hearing at which Members hear testimony about cybersecurity risks is no substitute for laboratory investigations of those risks, much less a substitute for a patient knowing the current status of her own device.

Even the actual research cited by Respondents does not indicate that Proponents lack a need for circumvention. For any given researcher or patient, the existence of a research project in some distant institution, working on a device unrelated to their own, hardly provides an alternative to the ability to conduct their own research or access their own device.

Appeals to manufacturers' own product safety and security testing are also unavailing. Manufacturers naturally have an incentive to restrict outside research that may reveal potential product liabilities as soon as they are discovered, and manufacturers will frequently lack incentives to address individual patients' lack of data access.

In short, claiming that a few isolated efforts each with different objectives meets the broad and diverse needs of researchers and patients ignores the unmet demand for alternative security, patient access, and patient-centered health efforts across different devices.

It is particularly telling that one of the more developed patient-initiated device hacking projects has taken as its slogan the hashtag "#wearenotwaiting."[11] Patients around the world are eager to access their data and devices, often long before manufacturers are willing to allow them to do so.

NAM and IPO claim that patients have no need for access to information communicated by their devices because they can access that information via their doctors or other medical professionals. It is at best disingenuous to claim that making an appointment with a medical professional to relay information that was generated by a device on the patient's person is a reasonable alternative to receiving the data—already being generated by the device—directly from the source. The adverse effect in evidence here is the massively heightened barrier to vital information whose relevance and importance—such as blood sugar levels or heart rhythms—are often immediate. While some might argue that increasing the time to access a book from seconds to hours may be a "mere inconvenience," it is implausible to say that a similar increase in time to access news of a rapid change in blood sugar is merely inconvenient.

7. Statutory Factors

The bulk of Respondents' objections focus on creating uncertainty and doubt regarding the effects of circumvention on patient safety and privacy. Such considerations are not germane to this proceeding, unless they can be convincingly included in one of the five statutory factors—the catchall "any other factor that may be appropriate for the Librarian to consider."

However, such concerns are not appropriate for the Librarian to consider, particularly in view of the paucity of evidence Respondents have provided to substantiate their hypothetical concerns. Moreover, the Librarian and this rulemaking proceeding are poorly placed to make determinations on patient privacy and safety. As such, they should grant the exemption request to ensure that Section 1201, unrelated to the relevant regulatory regimes, does not act as an impediment to their appropriate application.

---

[11] *See*, *e.g.,* Nightscout, http://www.nightscout.info/; https://twitter.com/hashtag/wearenotwaiting; Healthline, *"We Are Not Waiting" = Diabetes Data Innovation Now!*, http://www.healthline.com/health/diabetesmine/innovation/we-are-not-waiting.

A. **Patient safety and privacy are protected through circumvention**:

Each of the oppositions to the proposed exemption mentions Respondents' concern that circumvention may affect patient safety and privacy. Such concerns are not properly within the scope of this proceeding. Furthermore, the concerns are based upon mistaken assumptions, exaggerations, and errors regarding the nature of the requested uses and the relevant law.

Patient Safety

AdvaMed claims that any activity "outside the manufacturer's design" creates the "possibility" of malfunction. LifeScience Alley similarly states that "anyone having access to reprogram…implantable devices *could* compromise the health of these patients." (emphasis added).

These statements, while literally true, mean little in themselves. The possibility for risk is never zero, and Respondents fail to measure, state, or even hazard an estimate of adverse effects caused by errors in accessing device firmware, instead merely hinting at some hypothetical risk of injury or death.

This is particularly unconvincing in the case of circumvention for the purposes of security research. For instance, NAM worries that "applying trial-and-error experimentation methods to modify the software in life-saving devices is particularly troubling." While ICDs as a category of devices are indeed life-saving, a particular ICD not implanted within or associated with a current patient—the sort which researchers would be conducting extensive trial-and-error tests upon—is free to be poked, prodded, and even destroyed with no risk of harm to any human. Rules and regulations relevant to patient safety can easily distinguish between research conducted upon devices currently being used for a patient's treatment, and the same devices sitting in isolation on a laboratory or workshop bench.

AdvaMed claims that granting the requested exemption would create incentives for device misuse, but fails to describe what these incentives might be, or how granting the exemption might alter any existing incentives for misuse. In fact, any incentives for an attack are lessened by granting the exemption. Disclosed and known attacks are less valuable to malicious hackers, since preventative measures can be more easily developed. Allowing research for both security and patient purposes allows discovery and disclosure of vulnerabilities.

It beggars belief that anyone with an existing incentive for malicious use of a medical device would alter their calculus based upon potential liability under Section 1201. Malicious users willing to put the health and safety of others at risk are not being deterred by the remedies in 17 U.S.C. §§ 1203-04, which pale in comparison to the penalties for actually threatening or visiting bodily harm upon another human. Instead, legitimate researchers who would disclose risks to manufacturers and the public will be less willing to begin their research if they faced liability for going public, even absent any

malicious intent. The fact that some do anyway is a testament to their determination, but hardly a sign that more cannot be done to encourage more researchers to investigate device safety.

As Petitioners have demonstrated, the health risks associated with existing software flaws present real, documented risks that have led to device recalls and patient deaths. Research that uncovers miscalibrations, programming errors, or intrusion vulnerabilities therefore improves, rather than harms, patient safety.

NAM and Jay Schulman claim that allowing independent research into potential vulnerabilities of devices may undermine the public trust in such devices and treatments. If anything undermines public trust in a system, it is Respondents' apparent belief that these devices will not withstand research scrutiny. Consumer advocates and security researchers regularly discover flaws in existing products; the knowledge of those flaws and the risks they present should not be hidden from the patients whose lives depend upon them. To the extent that Respondents fail to trust patients to rationally assign risks, they denigrate the agency both of the patients and the competence of their healthcare providers to explain the balance of risks, instead assuming that it is up to them to decide what truthful information should or should not be doled out to those most directly affected.

LifeScience Alley, AdvaMed, and NAM all mention but one concrete effect that circumvention may have upon device operation: battery life. However, they vastly inflate the risks to battery life and ignore remedies to the problem, instead cherry-picking disparate aspects of different kinds of devices and different types of use in order to imply that circumvention will lead to the premature inactivation of all devices.

This is far from the case. For one thing, many uses run no risk of altering device performance. Accessing data already being transmitted by the device on its own schedule will have no effect upon its ordinary operation and will have no effect on its battery life. Even more robust querying of many devices will have a minimal effect. For instance, if any novel use of an insulin pump were to reduce its battery life, changing the battery is a trivial affair.[12]

Patient Privacy

AdvaMed briefly mentions concerns about violation of privacy rights; IPO states that granting an exemption would "risk HIPAA violation." These concerns are at best misplaced.

The Health Insurance Portability and Accountability Act ("HIPAA") governs the behavior of "covered entities:" health care providers, health plans, and health care

[12] *See, e.g.*, Medtronic, *Changing Your Battery*, http://www.medtronicdiabetes.com/customer-support/device-settings-and-features/utility-settings/battery ("To insert a battery, you will need your pump, a new AAA alkaline battery, and a thick coin (nickel or quarter).").

clearinghouses.[13] Petitioners fit none of these categories, and thus cannot "violate HIPAA." Neither HIPAA, nor any other privacy statute, prevents patients from accessing or gathering their own medical records, nor does it prevent patients from disclosing their own records to third parties directly. Where there is no patient (e.g. with discarded or non-implanted devices), HIPAA or other privacy statutes cannot apply.

The general concern for patient privacy ignores the basic fact that Petitioners seek to make uses of patient information with the express involvement of the patients themselves. An individual cannot violate privacy laws by making disclosures about themselves; nor do Respondents have the authority or ability to tell patients with whom they may share their own data.

FDA Involvement Would Be Unhelpful and Burdensome In a Copyright Proceeding

The above arguments about patient safety and privacy suffer one additional major flaw: the Librarian and the Office are ill equipped to make determinations about privacy and patient safety.

LifeScience Alley states that the FDA is the correct administrative body to monitor medical devices. AdvaMed states that the FDA should retain regulatory supremacy over medical device operations. We agree.

Where we appear to differ with Respondents is in how the FDA may properly remain in charge of its domain. So long as Section 1201 serves as a potential bar to medical device activity, it hampers any potential progress that might be made at the FDA. Should the FDA decide tomorrow, or next year, or two years from now that any of Petitioners' activities should be approved, Respondents would have Petitioners still prevented from proceeding because of an outgrowth of copyright law.

In this case, Respondents confuse the Librarian doing nothing with the Librarian properly ceding jurisdiction. In fact, the opposite is true. If the FDA is to have the practical authority to decide upon the legality of various activities, it is incumbent upon the Librarian and the Office to remove the potential impediments of Section 1201.

FDA input in this proceeding is unnecessary; FDA regulations on medical devices already apply and are in force. Meanwhile, the FDA lacks useful expertise on copyright law or Section 1201. The Librarian and Office should resist the temptation to delegate to the FDA their responsibilities in determining whether or not proposed uses infringe copyright or affect the interests of copyright holders, just as we expect FDA does not delegate judgments of device usage and safety to the Librarian and the Office.

[13] 45 C.F.R. § 160.103.

B. **Warranty and Trade Secret Claims Are Even More Inapposite to This Proceeding**

LifeScience Alley notes that alteration of devices may void device warranties. Provided that the user is aware of the warranty status, this is irrelevant to any copyright concern. LifeScience Alley and AdvaMed also claim that circumvention risks exposing trade secrets. Again, the Copyright Office is tasked with judging whether or not circumventions for purposes that do not infringe *copyright* are to be granted. Effects on a copyright holder's trade secrets are no part of the statutory factors for determining an exemption. Furthermore, to the extent that proprietary code might be revealed by reverse engineering, trade secret provides an uncertain remedy.[14]

Appeals by Respondents to effects upon their interests such as trade secret and device reputation reveal that their interests in prohibiting circumvention of TPMs reside far from any interest in protecting access to copyrighted works, but instead seek to use TPMs to control unrelated interests.

C. **A Broad Exemption is Warranted**

AdvaMed and IPO object to the breadth of the proposed exemption, but fail to counter Petitioners' demonstrated need for a broad exemption.

AdvaMed uses the breadth of the proposal to name a wide variety of medical devices, and theorize the worst possible outcome of tampering with each. This does little to suggest that the exemption should be narrowed—the specific devices mentioned by Petitioners, including ICDs and insulin pumps, are already known to play critical roles in patient safety. Noting that a cochlear implant may also create issues does not change the fact that safety issues are not relevant to the circumvention question.

Regardless of the particular device at issue, or the particular TPMs they may employ, the relevant facts of any activity under the proposed exemption are the same. Requiring each separate type of device to have a separate request based upon its specific characteristics is impracticable. The advance of technology in the hardware and software of these devices requires an exemption that grants maximum flexibility. And allowing the FDA and other relevant agencies the ability to set rational, expert standards requires an exemption that will minimally interfere with their determinations. In other words, it is in the best interests of all concerned that the Librarian and Office ensure that Section 1201, to the greatest extent possible, remove itself from the realm of medical devices.

* * *

For the foregoing reasons, the Librarian should grant the proposed exemption.

[14] *See, e.g.*, *Aqua Connect, Inc. v. Code Rebel, Inc.*, 2012 U.S. Dist. LEXIS 17962 (C.D. Cal. Feb. 13, 2012) (noting that California's implementation of the Uniform Trade Secret Act specifically allows reverse engineering).