BEFORE THE UNITED STATES COPYRIGHT OFFICE
LIBRARY OF CONGRESS

REPLY COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. § 1201
DOCKET NO. 2014–07

REPLY COMMENT OF A COALITION OF MEDICAL DEVICE RESEARCHERS IN SUPPORT OF PROPOSED CLASS 27: SOFTWARE – NETWORKED MEDICAL DEVICES

Multimedia evidence is not being provided in connection with this comment.

Pursuant to the Notice of Proposed Rulemaking for Exemption to Prohibition on Circumvention of Copyright Protection System for Access Control Technologies,[1] the Coalition of Medical Device Researchers[2] (the "Coalition") submits the following reply comments to provide additional legal and factual support regarding:

> **Proposed Class 27: Software – Networked Medical Devices.** Computer programs, in the form of firmware or software, including the outputs generated by those programs, that are contained within or generated by medical devices and their corresponding monitoring systems, when such devices are designed for attachment to or implantation in patients, and where such circumvention is at the direction of a patient seeking access to information generated by his or her own device or at the direction of those conducting research into the safety, security, and effectiveness of such devices.

Comments are submitted by the Coalition through their counsel:

Andrew F. Sellars
Clinical Fellow, Cyberlaw Clinic
Berkman Center for Internet & Society
Harvard Law School
23 Everett Street, Second Floor
Cambridge, MA 02138
(617) 384-9125
asellars@cyber.law.harvard.edu

[1] 79 Fed. Reg. 73,856 (Dec. 12, 2014) [hereinafter NPRM].

[2] The members of this Coalition are Hugo Campos, Stanford Medicine X; Jerome Radcliffe, Rapid7; Karen Sandler, Software Freedom Conservancy; and Benjamin West, an independent medical device researcher. *See* COMMENT OF A COALITION OF MEDICAL DEVICE RESEARCHERS Appx. A (Feb. 6, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_Coalition_ of_Medical_Device_Researchers_Class27.pdf [hereinafter COALITION COMMENT]. Their institutional affiliations are provided for identification purposes only.

I. Introduction

Five comments that were filed in Class 27,[3] and one that was filed in Class 25 but appears to relate instead to Class 27,[4] express opposition to the Coalition's proposed exemption. The primary argument of all six comments is that conducting the sort of research discussed by the Coalition may harm patients. But the Coalition is not asking the Copyright Office to start allowing independent research into medical devices; it is asking that independent medical device research be allowed to continue. Such research has been going for years, and has done so without incident.[5] The Coalition's proposed exemption is only necessary now because manufacturers, as a result of independent research discovering vulnerabilities in their devices,[6] have begun to

---

[3] *See* ADVANCED MEDICAL TECHNOLOGY ASSOCIATION, COMMENTS REGARDING PROPOSED CLASS 27 (March 27, 2015), *available at* http://copyright.gov/1201/2015/comments-032715/class 27/AdvaMed_Class27_1201_2014.pdf [hereinafter ADVAMED COMMENT]; INTELLECTUAL PROPERTY OWNERS ASSOC., IN THE MATTER OF EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS (March 27, 2015), *available at* http://copyright.gov/1201/2015/comments-032715/class%2027/ Intellectual_Property_Owners_Association_Class27_1201_2014.pdf [hereinafter IPO COMMENT]; LIFESCIENCE ALLEY, LONG COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. 1201 (March 27, 2015), *available at* http://copyright.gov/1201/2015/comments-032715/class 27/LifeScience_Alley_Class27_1201_2014.pdf [hereinafter LIFESCIENCE ALLEY COMMENT]; NAT'L ASSOC. OF MANUFACTURERS, LONG COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. 1201 at 4-5 (March 27, 2015), *available at* http://copyright.gov/1201/2015/comments-032715/class%2027/ National_Association_of_Manufacturers_Class27_1201_2014.pdf [hereinafter NAM COMMENT]. JAY SCHULMAN, IN RE: NOTICE OF INQUIRY ON EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS (March 27, 2015), *available at* http://copyright.gov/1201/2015/comments-032715/class%2027/ Jay_Schulman_Class27_1201_2014.pdf [hereinafter SCHULMAN COMMENT].

[4] *See* MEDICAL DEVICE INNOVATION, SAFETY AND SECURITY CONSORTIUM, SHORT COMMENT REGARDING A PROPOSED EXEMPTION (March 27, 2015), *available at* http://copyright.gov/1201/2015/comments-032715/class25/Medical_Device_Innovation_Safety_and_Security_Consortium_Class25_1201_2014.pdf [hereinafter MDISS COMMENT].

[5] *See* COALITION COMMENT, *supra* note 2, at 2–3, 18–19, App'x B; Nancy G. Levenson & Clark S. Turner, *An Investigation of the Therac-25 Accidents*, 26 COMPUTER 18 (1993) (reviewing the software failure of a medical device in the early 1990s). Independent researchers have been investigating electronics in medical devices as far back as the 1960s. *See generally* Don Witters, *Medical Devices and EMI: The FDA Perspective*, FDA, http://www.fda.gov/MedicalDevices/ DeviceRegulationandGuidance/GuidanceDocuments/ucm106367.htm (last updated May 4, 2014) (discussing early independent research into electromagnetic interference).

[6] Numerous independent scholars were consulted for the Government Accountability Office's review of the FDA, which determined that the agency should consider cybersecurity more as part of its review process. *See generally* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-816, FDA SHOULD EXPAND ITS CONSIDERATION OF INFORMATION SECURITY FOR CERTAIN TYPES OF DEVICES (2012) [hereinafter GAO REPORT]. The FDA in turn issued new guidance on premarket

implement technological protection measures ("TPMs") as defined under Section 1201. Device research was being conducted before – and continues to be conducted today – on devices that do not have TPMs using the exact same techniques contemplated here. As to devices that employ TPMs, however, such research cannot happen, and flaws that may be unique to a particular device will not be discovered.[7]

For all their bluster, and despite the lengthy history of this research, the commenters do not cite a single instance where existing research posed a risk to human life or enabled others to carry out malicious activity. In fact, they cite very little of anything at all. In what is supposed to be a rulemaking substantiated by "specific, 'real-world examples supported by evidence over speculative, hypothetical observations,"[8] the opposition comments lack nearly any substantiation. The six comments cite almost exclusively to the text of the NPRM, the Coalition's initial comments, and assorted federal agency statements about policies on medical device safety[9] – statements that, the commenters fail to mention, were explicitly informed by independent medical device research.[10] And in terms of concerns over piracy and infringement, the issues that lie at the heart of this rulemaking,[11] the opposition commenters say nearly nothing at all. The word "piracy" is never mentioned, and the word "infringement" only appears in one conclusory statement from one commenter.[12]

The commenters also overlook evidence previously introduced by this Coalition. Several comments spend numerous pages in an attempt to scare the Copyright Office into thinking that if this exemption were granted, patients would begin vulnerability testing on their own life-

---

submissions, which, while not formally binding, greatly influence medical device manufacturing development. *See* COALITION COMMENT, *supra* note 2, at 9 (citing FDA, CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (2014), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf [hereinafter FDA CYBERSECURITY GUIDANCE]).

[7] *See* COALITION COMMENT, *supra* note 2, at 24.

[8] NPRM, *supra* note 1, at 73,857.

[9] Through all six comments, the *only* citations not referencing one of the categories above were to prior recommendations and rules in this rulemaking; one website referencing a House Committee hearing; the website for the firm Rapid7; three news articles about a Coalition member's prior research; the homepages for two university research centers; a Business Wire article about powered prostatic joints; and three copyright cases. *See* ADVAMED COMMENT, *supra* note 3, at 3–6; IPO COMMENT, *supra* note 3, at 2; LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 3; NAM COMMENT, *supra* note 3, at 4–5.

[10] *See infra* notes 42–47 and accompanying text.

[11] 17 U.S.C. § 1201(a)(1)(C) (the Librarian, Register, and Assistant Secretary should consider, *inter alia*, "the effect of circumvention of technological measures on the market for and value of copyrighted works"); H.R. REP. NO. 105-511, pt. 2, at 37 ("The primary goal of the rulemaking proceeding is to assess whether the prevalence of these protections . . . is diminishing the ability to use these works in ways that are otherwise lawful.").

[12] *See* IPO COMMENT, *supra* note 3, at 1 (stating, without substantiation, that the exemption "would permit infringement of copyright in the software").

sustaining devices.[13] In effect, the commenters suggest that a person with the intelligence and computer engineering skills necessary to intercept, decipher, and analyze the inputs and outputs of a medical device would somehow lack the common sense not to conduct these tests on a device attached to a patient. This is absurd. The devices used for vulnerability testing are not the same ones that go into patients, and the Coalition explicitly stated as much.[14] Currently-implanted or attached devices are only implicated by the proposed exemption in circumstances where patients seek to access their own data through the passive monitoring of data already being transmitted.[15]

To suggest that independent research would "cause a drastic setback"[16] in the quality of devices is to completely ignore the vital role that such research has always played in the development of medical technologies. Such research currently informs manufacturers, policymakers, patients, and doctors, and should be allowed to continue to serve these important roles even as device manufacturers begin to employ TPMs. This is especially true in the area of personalized access to one's own data, where research is increasingly showing how greater access to such information can radically improve patient outcomes.[17]

The opposition commenters also warn that conducting this sort of research will enable malicious actors. They again cite no evidence of this. As noted by the Food and Drug Administration ("FDA") itself, regulatory bodies and the public are "not aware of any patient injuries or deaths associated with cybersecurity incidents, nor are [they] aware that any specific devices or systems in clinical use have been purposefully targeted at this time."[18] Rather than enable malicious hackers, allowing open input into security research improves the overall security of devices, informs policymakers about how to regulate the space, and serves an important role in helping the public understand the nature and extent of this concern.[19]

The opposing commenters suggest that existing efforts to solicit and fund research by manufacturers obviates the need for this exemption. This, too, is without merit. As the Register noted in the 2010 rulemaking, reliance on investigations sanctioned by manufacturers alone is insufficient to protect the public from misconfigured or vulnerable software.[20] Indeed, there are

---

[13] *See, e.g.*, ADVAMED COMMENT, *supra* note 3, at 1–2; LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 7; NAM COMMENT, *supra* note 3, at 6–7.
[14] COALITION COMMENT, *supra* note 2, at 10 (noting that security research is "done on devices not used in patient care").
[15] *Id.* ("Accessing the . . . outputs of medical devices usually requires a form of radio transmission interception, often combined with reverse engineering techniques."). AdvaMed indicates that such passive monitoring would be acceptable to them if the Copyright Office grants this exemption. *See* ADVAMED COMMENT, *supra* note 3, at 3.
[16] NAM COMMENT, *supra* note 3, at 7.
[17] *See infra* notes 54–77 and accompanying text.
[18] *Cybersecurity*, FDA, http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth/ucm373213.htm (last updated Oct. 23, 2014) [hereinafter *Cybersecurity*].
[19] *See infra* notes 78–89 and accompanying text.
[20] U.S. COPYRIGHT OFFICE, RECOMMENDATION OF THE REGISTER OF COPYRIGHTS IN RM 2008-08; RULEMAKING ON EXEMPTIONS FROM PROHIBITION ON CIRCUMVENTION OF COPYRIGHT

numerous cases where device manufacturers knew of vulnerabilities but failed to disclose or remedy them until public attention was brought to the issue, including an incident less than a month ago.[21]

The opposition commenters further argue that the FDA, and not the Copyright Office, should take the lead in regulating the safety of medical devices.[22] The Coalition agrees, but this argument favors granting this exemption. The FDA has long accepted the role played by independent researchers in testing the safety and security of medical devices, and its regulatory role has been enhanced by such efforts.[23] It is only because manufacturers have begun to employ TPMs that the Copyright Office has some overlapping authority in this space. As is best practice in all areas of overlapping agency authority, the Copyright Office should focus its inquiry its domain of expertise – that is, matters of copyright and piracy – and leave the greater health and safety tradeoffs and considerations to the FDA or Congress.[24] And as to piracy, as noted above, the opposition commenters provide little if any evidence to suggest that circumventing the TPMs actually risks enabling copyright infringement by researchers, patients, or anyone else.[25] This is because, as noted in the Coalition's prior comment, the types of uses considered in this exemption would never supplant the need for the original device in any conceivable use case.[26] No cardiac patient would look at a device's source code in lieu of getting a pacemaker; no patient with diabetes would look at the data readout from an insulin pump instead of getting one.

The Coalition and the opposition commenters agree that the source code of devices is protectable under copyright, that data outputs may in some cases may be protectable, and that TPMs exist in some of these devices.[27] There also seems to be agreement that existing statutory protections do not supplant the need for the exemption,[28] and that patients and researchers are the full owners of these devices, instead of mere licensees.[29] As to other objections expressed by opposition

---

PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES 189 (2010) [hereinafter 2010 RECOMMENDATION].

[21] *See infra* notes 111–116 and accompanying text; Kim Zetter, *Drug Pump's Security Flaw Lets Hackers Raise Dose Limits*, WIRED (Apr. 9, 2015), http://www.wired.com/2015/04/drug-pumps-security-flaw-lets-hackers-raise-dose-limits/.

[22] *See, e.g.*, ADVAMED COMMENT, *supra* note 3, at 3-4; NAM COMMENT, *supra* note 3, at 7.

[23] *See infra* notes 123–129 and accompanying text.

[24] *See infra* notes 120–122 and accompanying text.

[25] *See supra* notes 11–12 and accompanying text.

[26] COALITION COMMENT, *supra* note 2, at 14; *see also* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 75 Fed. Reg. 43,825, 43,833 (July 27, 2010) (the Librarian of Congress noting in the 2010 rulemaking that "[t]he socially productive purpose of investigating computer security and informing the public . . . [is] unlikely to have an adverse effect on the market for or value of the copyrighted work itself").

[27] *See, e.g.*, ADVAMED COMMENT, *supra* note 3, at 5.

[28] *See* COALITION COMMENT, *supra* note 2, at 15–17.

[29] *See* PUBLIC KNOWLEDGE, LONG COMMENT REGARDING A PROPOSED EXEMPTION 4–6 (Feb. 6, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_longform_PK_Class27.pdf.

commenters, this Office should treat these as no more than the self-serving conjecture of an industry that, like most, abhors scrutiny it cannot control, especially when the costs of correcting a misconfigured or vulnerable device can be so high.[30] The Coalition accordingly requests that the Register recommend this exemption.

II. The Medical Device Research Discussed Here Is Crucial to Improving the Safety and Security of Devices and Patients, Does Not Present Greater Risks, and is Directly Affected by Section 1201.

As discussed previously by the Coalition, independent research plays a critical role in informing doctors, patients, regulators, policymakers, manufacturers, and the general public about the nature and effectiveness of medical devices, both in general and as they relate to individual care.

A. Independent Medical Device Research Greatly Benefits Industry

Independent researchers are in a continuous dialogue with industry on how they can improve the safety, security, and effectiveness of its devices. As opposition commenters themselves note, there are now numerous conferences and other gatherings between independent researchers and manufacturers, including those convened by the FDA and universities.[31] As near as the Coalition can tell, the industry does not approve the guest list, nor does it grant individual permission to each piece of research discussed in these conferences. Anticircumvention law should not grant them such authority over researchers of devices that use TPMs.

The opposition commenters themselves concede how important and effective independent research can be to improving the quality of these devices. In the words of AdvaMed, "[a]fter the initial demonstration of a patient getting access to an insulin pump, the industry responded robustly."[32] Similarly, the Intellectual Property Organization noted that one company "hired three separate security firms to conduct research after an initial demonstration" of a vulnerability.[33] The key word in both sentences is *after*. It was only after security researcher Barnaby Jack – building upon research done by Coalition members Jerome Radcliffe and Karen Sandler – demonstrated this vulnerability at a large security conference that the industry responded.[34] And it was only after Radcliffe released his research findings that the Department of Homeland Security issued bulletins warning the industry of the vulnerabilities his research

---

[30] SCHULMAN COMMENT, *supra* note 3, at 1 (noting that devices may have to "go through recertification with the FDA" if vulnerabilities are found); *see also* LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 4 (noting that research could "expose the manufacturer to unforeseeable liability").
[31] NAM COMMENT, *supra* note 3, at 6; LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 3; IPO COMMENT, *supra* note 3, at 2; ADVAMED COMMENT, *supra* note 3, at 2; *see also* COALITION COMMENT, *supra* note 2, at 3 n.17.
[32] ADVAMED COMMENT, *supra* note 3, at 3.
[33] IPO COMMENT, *supra* note 3, at 2.
[34] *See* ADVAMED COMMENT, *supra* note 3, at 3.

revealed.[35] Medical device companies may wish to be proactive on matters of software reliability and security, but they are in fact often reactive.

B. Independent Medical Device Research Greatly Benefits Policymakers

Independent research has a similar influence in the policy and government space. As was noted in the Coalition's previous comment, President Obama has asked for broad input into vulnerability information in the healthcare sector.[36] Since the Coalition filed this comment, the President again stressed that "[o]rganizations engaged in the sharing of information related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States."[37] On the personal health information side, the President announced an initiative during the State of the Union address that seeks to develop the state of "Precision Medicine," or the greater personalization of treatment based on a greater understanding of one's own medical data and the empowerment of individuals to "invest and manage their health."[38]

In the specific area of medical devices, the Coalition has already discussed how independent research informs the policy decisions of the FDA, the Government Accountability Office ("GAO"), and the Department of Homeland Security ("DHS").[39] Coalition member Jerome Radcliffe specifically collaborated with DHS and the FDA after discovering security vulnerabilities in insulin pumps.[40] That the FDA has invited members of this Coalition to participate in workshops and private–public research only demonstrates how valuable the FDA considers independent research to be.[41] Independent research permeates and informs nearly every public statement made by regulatory bodies in the medical and cybersecurity space.

This fact is not always apparent at first glance, which perhaps explains why the opposition commenters here mistakenly relied on independent research when arguing that such research should not be allowed. For example, the National Association of Manufacturers uses a GAO study repeatedly in its opposition comment to describe the sensitive nature of medical devices, as

---

[35] *See* DHS NAT'L CYBERSECURITY & COMMS. INTEGRATION CTR., ATTACK SURFACE: HEALTHCARE AND PUBLIC HEALTH SECTOR (2012), *available at* https://info.publicintelligence.net/NCCIC-MedicalDevices.pdf.
[36] *See* COALITION COMMENT, *supra* note 2, at 18 (citing Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,739, 11,739 (Feb. 12, 2013)).
[37] Executive Order 13,691, Promoting Private Sector Cybersecurity Information Sharing, 80 Fed. Reg. 9349, 9349 (Feb. 13, 2015).
[38] *Fact Sheet: President Obama's Precision Medicine Initiative*, WHITE HOUSE OFFICE OF THE PRESS SECRETARY (Jan. 30, 2015), https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative; *see also* Robert Pear, *U.S. to Collect Genetic Data to Hone Care*, NEW YORK TIMES (Jan. 30, 2015), http://www.nytimes.com/2015/01/31/us/obama-to-unveil-research-initiative-aiming-to-develop-tailored-medical-treatments.html.
[39] COALITION COMMENT, *supra* note 2, at 18–19.
[40] *Id.* at App'x D ¶ 1.
[41] *See* ADVAMED COMMENT, *supra* note 3, at 2–3.

an argument to deter this form of research.[42] Yet the GAO report they reference relied heavily on the very same research they seek to deter – including studies by a member of this Coalition.[43] LifeScience Alley mentions the DHS's Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT") as an example of public regulation of vulnerability information that obviates the need for independent research.[44] They fail to mention, however, that ICS-CERT routinely relies on numerous independent researchers as part of their activities, as evidenced by repeated thanks to them in the *ICS-CERT Monitor* newsletter.[45] LifeScience Alley further notes that the House Energy and Commerce Committee has been holding hearings on cybersecurity, but it omits that the witness list includes numerous independent researchers.[46] They also reference the National Institute of Standards and Technology's National Cybersecurity Center of Excellence ("NCCoE"), which actively solicits comments and ideas from the public on how to secure medical devices.[47] Were the arguments made by the opposition commenters true, the FDA, DHS, and NIST would never make such public inquiries; they would only ask AdvaMed what AdvaMed thinks. Should TPMs be allowed to prevent this form of research, however, this critical, independent voice will be lost in discussions of an ever-growing number of medical devices.

C. *Independent Research on Safety and Security and Improved Access to Device Data Benefits Patients and Doctors.*

This research benefits patients as well. On a general level, fully understanding the risks of medical devices can help patients and doctors make more informed choices about treatment options. Doctors should be able to know the facts, probabilities, and magnitudes of various medical device concerns, as well as the solutions that are routinely included in the reports of independent researchers.[48] They should know that software bugs and design flaws in medical devices have killed hundreds of patients and have resulted in over a thousand recalls, whereas to date there has not been a single reported case of a malicious attack on a device outside of

[42] *See* NAM COMMENT, *supra* note 3, at 1, 5, 7.
[43] *See* GAO REPORT, *supra* note 6, at 2 n.5 (citing Jerome Radcliffe's work on insulin pump vulnerabilities and other independent scholarship).
[44] LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 3.
[45] *See, e.g.*, DHS, ICS-CERT MONITOR 12–13 (Feb. 2015), https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf (citing 20 different independent researchers that assisted ICS-CERT in their review).
[46] LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 3; *see Understanding the Cyber Threat and Implications for the 21st Century Economy*, U.S. HOUSE ENERGY & COMMERCE COMMITTEE, http://energycommerce.house.gov/hearing/understanding-cyber-threat-and-implications-21st-century-economy (last viewed April 28, 2015) (mentioned witnesses from Stanford University, Carnegie Mellon University, and independent security firm FireEye, Inc.).
[47] LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 3 (noting the importance of the NIST in this space); *see Cybersecurity Center Invites Feedback on Securing Medical Devices*, NIST (Dec. 22, 2014), http://www.nist.gov/itl/pumps-122214.cfm.
[48] *See* COALITION COMMENT, *supra* note 2, at 22.

research settings.[49] They should also know that certain safety features on devices, such as the alarm systems on many pacemakers, have failed in the past, and thus patients cannot rely solely on the devices themselves to alert them to problems.[50] All of this is relevant to their assessment, and patients and doctors should be empowered to assess this information together.[51] This equally is true of research that finds no vulnerabilities. As Register Peters noted in an earlier rulemaking, "[t]here is a social benefit in objective analysis that dispels rumors and speculation about the vulnerabilities caused" by technological measures.[52] And as noted by Coalition member Karen Sandler, companies currently do not provide this specific information to patients or doctors.[53] Only independent research brings this to light.

On an individual level, greater access to data is increasingly shown to improve patient care.[54] In some cases, this greater access is a necessity, because getting the data every few months will lead patients to miss critical health information that they need. In other cases, such data provides new affordances for improving the overall quality of care, and thus ensures greater overall safety and security.

Despite their considerable lip service to the notion that patients should have a right to access data,[55] the opposition commenters nevertheless argue that direct patient access is unnecessary because patients can already get this information in checkups with their doctor.[56] But as the Coalition has already shown, getting data a few times a year during periodic checkups is simply not adequate in many cases.[57] The Coalition's initial comment noted, for instance, that devices

---

[49] *See id.* at 2, 22 (citing Homa Alemzadeh et al., *Analysis of Safety-Critical Computer Failures in Medical Devices*, 11 IEEE SECURITY & PRIVACY 14, 14 (2013)).
[50] Alemzadeh, *supra* note 49, at 22.
[51] In this vein, it is curious why one commenter suggests that having "the risk-benefit calculation . . . made between a doctor and patient . . . changed by the security researcher" would be a bad thing. SCHULMAN COMMENT, *supra* note 3, at 1. If the researcher's discoveries can help patients and doctors make better choices, this can only be a positive development.
[52] 2010 RECOMMENDATION, *supra* note 20, at 186.
[53] *See* COALITION COMMENT, *supra* note 2, at App'x E ¶¶ 2, 5.
[54] *Id.* at 2–3, 18–19, App'x C ¶ 7; JACK DINTRUFF, SHORT COMMENT REGARDING PROPOSED EXEMPTION (Feb. 6, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/EFF_merged_shortform_comments_class27.pdf (page 679 of the aggregated PDF of individual comments) ("I almost died 2 years ago and I still retain digital copies of the imaging and laboratory studies that were conducted. It's my right as a patient to obtain this information, and restricting patient access to this information encroaches upon my right to informed consent.").
[55] *See, e.g.*, ADVAMED COMMENT, *supra* note 3, at 2 ("We believe that patients have the inherent right to access their own medical data . . . ."); MDISS COMMENT, *supra* note 4, at 1 ("MDISS supports the need of patients to have access to, and ultimate control of, their healthcare data . . . .").
[56] NAM COMMENT, *supra* note 3, at 5–6; LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 4.
[57] Exactly how often device data can be obtained is subject to some conflicting information. Patients generally can get this information about every six months. *See* TEDx Talks, *Hugo Campos Fights for the Right to Open His Heart's Data*, TEDX CAMBRIDGE, at 2:40–3:10 (Jan. 20, 2012), http://tedxtalks.ted.com/video/TEDxCambridge-Hugo-Campos-fight. Medtronic and

can detect time-sensitive anomalies that patients may not feel, including changes in heart rhythm or blood flow.[58] Such anomalies can be triggered by patient activity or diet, but because device information is often only made available months later, patients have to resort to extremely burdensome manual logging of their activities in order to correlate them with machine-detected anomalies.[59] As Coalition member Hugo Campos has also shown, the internal clocks of devices can also derivate from actual time, making post hoc correlation of activity and episodes all the more difficult.[60] The FDA seems to agree that more timely access to data should be allowed; it has recently approved a device that will notify patients about atrial fibrillation through their smartphone.[61]

On the insulin pump side, while the nature of these devices often means that more data is readily accessible than with a pacemaker, even very basic device functioning data, such as how much insulin is actually discharged from the device, may be hidden from a patient.[62] Allowing patients to obtain this information helps them become better custodians for their own care, a value recognized in diabetes treatment for decades.[63]

A growing number of studies have demonstrated that this inherent right, when exercised, can also radically transform patient care. For example, last month the *New York Times* published a profile on an MIT doctoral student named Steven Keating, who became interested in collecting

---

Biotronik publications indicate that insurance can cover device evaluations every 90 days or 30 days, depending on the particular device. *See* MEDTRONIC, MEDTRONIC CARELINK NETWORK REIMBURSEMENT GUIDE 1–2 (2009), *available at* http://www.medtronic.com.hk/wcm/groups/mdtcom_sg/@mdt/@crdm/documents/documents/carelink-reimb-guide-09.pdf; BIOTRONIK, PACEMAKER, ICD, AND ICM EVALUATIONS 2014 REIMBURSEMENT OVERVIEW 7 (2013), *available at* http://www.biotronik.com/files/D8881BEC82BE38B5C1257CFA00262658/$FILE/BR249r3sc.pdf. Medtronic's patient handbook mentions that more regular monitoring may be available through a home monitoring service, but does not indicate how often that would be allowed. *See* MEDTRONIC, PATIENT HANDBOOK: IMPLANTABLE CARDIOVERTER DEFIBRILLATOR 97–98 (2006).

[58] COALITION COMMENT, *supra* note 2, at 19.

[59] *Id.* at App'x C ¶ 9. Literature from the device manufacturers indicates that activities and symptoms that occur before and after an adverse heart event can be very important for patients and doctors to identify. *See* BOSTON SCIENTIFIC, IMPLANTABLE CARDIOVERTER DEFIBRILLATOR THERAPY 52 (2007).

[60] COALITION COMMENT, *supra* note 2, at App'x C ¶ 11.

[61] *See id.* at 19.

[62] *Id.* at App'x F ¶¶ 2, 4; *see also* Dana Lewis, *Context–Give Me Data (On My Device)*, DIYPS.ORG (Apr.13, 2015), http://diyps.org/2015/04/13/context-give-me-my-data-on-my-device/ (noting several pieces basic operational information that an insulin pump knows but does not share with a patient); JAN JAKUB OBER, SHORT COMMENT REGARDING A PROPOSED EXEMPTION (Feb. 6, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/EFF_merged_shortform_comments_class27.pdf (page 726 of the aggregated PDF) ("[A]ccess to the medical data gathered by this device will allow me to verify that the device operates as intended, and that the data is accurate.").

[63] COALITION COMMENT, *supra* note 2, at 19.

data about his own health, and with that information he was able to self-diagnose and detect a brain tumor, which doctors then successfully removed.[64] The Coalition noted similar research in its appendix to the initial comment, including studies showing that granting patients greater access to doctors' notes can improve overall outcomes.[65]

Despite these immediate benefits and potential new affordances, the opposition commenters here provide a series of objections to giving patients better access to their data. Multiple commenters expressed concerns about battery life of devices, and suggested that repeated access (referred to as "interrogation" in the industry) would drain devices' batteries.[66] As noted above and in the Coalition's initial comment, however, the exemption here is not asking for continuous interrogation of devices.[67] These devices already periodically dispatch data,[68] and most researchers seek only to be able to intercept and read that data as it goes by.

AdvaMed also suggests that even though "patients have the inherent right to access their own medical data," patients "may not understand the format of data or may misinterpret the data."[69] This is an insult to the intelligence of patients. Some patients may defer to doctors, but many instead opt to become experts in their own conditions. Coalition member Hugo Campos's story is a familiar one to anyone who has had a friend of family member go through an unexpected disease or ailment. After he was diagnosed with hypertrophic cardiomyopathy, he attended cardiology conferences, took classes on how pacemakers work, and did all he could to try and understand what his body was going through and what he could do to help.[70] Every member of this Coalition can tell a similar story.[71] Ownership of one's health information is exactly what the President is supporting with his new initiative on "Precision Medicine."[72] Patients working to

[64] Steve Lohr, *The Healing Power of Your Own Medical Records*, NEW YORK TIMES (March 31, 2015), http://www.nytimes.com/2015/04/01/technology/the-healing-power-of-your-own-medical-data.html?ref=technology&_r=0.
[65] COALITION COMMENT, *supra* note 2, at App'x B ¶¶ 9, 10, 14, 23.
[66] This objection does not appear to relate to insulin pumps, which tend to run on standard, replaceable batteries. *See, e.g.*, *Changing Your Battery*, MEDTRONIC, http://www.medtronicdiabetes.com/customer-support/device-settings-and-features/utility-settings/battery (last viewed Apr. 30, 2015).
[67] COALITION COMMENT, *supra* note 2, at 10.
[68] *See* TEDx Talks, *supra* note 57, at 2:30–3:00 ("Doctors . . . have full, 24/7, unrestricted access to this information. . . . Compare this to the patient experience: patients have no access to this information."); BIOTRONIK, *supra* note 57, at 97–98 (noting that with its CareLink service data can be uploaded for analysis on a regular schedule); Sherwin Siy, *Copyright Law and My Mother's Heart*, PUBLIC KNOWLEDGE (Jan. 20, 2015), https://www.publicknowledge.org/news-blog/blogs/copyright-law-and-my-mothers-heart/ (noting that pacemakers often transmit data whenever device patients walk within range of a monitoring base station, which then gets analyzed by diagnosticians).
[69] ADVAMED COMMENT, *supra* note 3, at 2; *see also* MDISS COMMENT, *supra* note 4, at 1.
[70] TEDx Talks, *supra* note 57, at 4:30–5:00.
[71] *See generally* COALITION COMMENT, *supra* note 2, at App'x C–F.
[72] *See* WHITE HOUSE OFFICE OF THE PRESS SECRETARY, *supra* note 38.

learn about their own health with a team of experts, including their doctor, can only benefit patient outcomes.[73]

When individual patients work with researchers to understand their data, the benefits can extend well beyond just the individual patient and improve the efficacy of treatment as a whole. Steven Keating, who discovered a brain tumor using his own medical data, now has made much of his data publicly available so others may use it to conduct further research.[74] The organization Sage Bionetworks has worked extensively to improve medical research by creating open and collaborative research frameworks, and to actively solicit meaningful input and participation from patients themselves.[75] Apple recently launched a program called ResearchKit in collaboration with Sage Bionetworks and other organizations to facilitate the use of individualized patient data in making medical discoveries.[76] The website PatientsLikeMe boasts hundreds of thousands of members who sign up to share their data in order to understand more about their own health and allow the website to use patient data in aggregate studies.[77] The potential of greater access to data is profound, from providing patients to critical information at the right time, to informing the public at large about medical issues, to possibly even transforming the way we think of tailoring medical care today.

D. Research Does Not Enable Malicious Actors

As was noted in the Coalition's initial comment, the nature of research considered here does not jeopardize the security of these devices for numerous reasons. First, pragmatically speaking, researchers do not publish all of the steps in creating a vulnerability, and to date there is not a single instance of a malicious intrusion on a device outside of a research setting.[78] Researchers also frequently work with manufacturers or the government, so that if vulnerabilities were ever found that realistically could be exploited, responses will be ready.[79]

More generally, authorities in computer science have long rejected the suggestion that medical device companies can better protect their products by keeping information about vulnerabilities secret.[80] As Prof. Eugene Volokh noted in a law review article deeply exploring the social

---

[73] *Cf.* COALITION COMMENT, *supra* note 2, at App'x E ¶ 6 (Coalition member Karen Sandler, noting that if she was allowed better access to the source code of her device, she could "organize a team of colleagues" who could analyze the information). Contrary to what LifeScience Alley hypothesizes, such information does not replace the need for a doctor, no do they produce any evidence to suggest that it would. *See* LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 6.
[74] *See* STEVEN KEATING, http://stevenkeating.info/main.html (last viewed Apr. 28, 2015).
[75] *See Philosophy*, SAGE BIONETWORKS, http://sagebase.org/philosophy/ (last viewed April 28, 2015).
[76] *See ResearchKit*, APPLE, https://www.apple.com/researchkit/ (last viewed April 28, 2015).
[77] *See* PATIENTSLIKEME, http://www.patientslikeme.com/ (last viewed April 28, 2015).
[78] COALITION COMMENT, *supra* note 2, at 22.
[79] *Id.*
[80] *Id.* at 23; *see also* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 7 (1996) ("If the strength of your new cryptosystem relies on the fact that the attacker does not know the algorithm's inner workings, you're sunk. If you believe that keeping the algorithm's insides secret improves the

benefits and harms of disclosing how to commit crimes, "[p]ublishing detailed information about a computer program's security vulnerabilities may help security experts figure out how to fix the vulnerabilities, persuade apathetic users that there really is a serious problem, persuade the media and the public that some software manufacturer isn't doing its job, and support calls for legislation requiring manufacturers to do better."[81] Examples of all of these can be found in the medical device world. Prof. Kevin Fu's groundbreaking research into pacemaker vulnerabilities also led to the proposal and development of numerous corrective technologies.[82] As recently as last month, independent research published in *Wired* was used to inform the public about vulnerabilities in Hospira infusion pumps used to deliver computer-controlled doses of drugs in hospitals, including information about the likelihood that such vulnerabilities could be exploited and what the industry could do and has done to improve their systems.[83] And as was already noted above, policymakers routinely rely on this information when crafting rules and legislation.[84]

The opposition commenters offer nothing but empty fearmongering in response. "[T]he consequences of placing the wrong information in the wrong hands are too grave to ignore," says the National Association of Manufacturers.[85] They apparently are too grave to substantiate, too: no commenter provides any evidence of the risk presented by this type of research, and they would not have found any had they tried. The National Association of Manufacturers also quotes this Coalition as asserting that "malicious attacks on devices are rare."[86] The Coalition did not say they were rare. It said they were nonexistent. "[T]o date, there has been no recorded incident of a malicious attack on a medical device."[87] And, this is not for lack of vulnerabilities, either. This is instead, in part, a credit to the excellent independent research that has already been done, and continues to be done, for all devices except those that employ encryption.[88] As the Register Peters noted in an earlier rulemaking, good faith research plays an important role in the "security ecosystem."[89] The well-established benefits of more open and understood security information radically outweigh the conjectural harms.

---

security of your cryptosystem more than letting the academic community analyze it, you're wrong.").

[81] Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1118 (2005).

[82] *See* Shyamnath Gollakota et al, *They Can Hear Your Heartbeats: Non-Invasive Security for Implantable Medical Devices*, 41.4 ACM SIGCOMM COMPUTER COMM. REV. 2 (2011).

[83] Zetter, *supra* note 21.

[84] *See supra* notes 36–47 and accompanying text.

[85] NAM COMMENT, *supra* note 3, at 8.

[86] *Id.*

[87] COALITION COMMENT, *supra* note 2, at 22.

[88] And as was noted previously, the presence of encryption alone does not obviate the need for this research, as many vulnerabilities and software bugs are not resolved through encryption technologies. *See id.* at 20 n.138.

[89] 2010 RECOMMENDATION, *supra* note 20, at 202.

E. The Coalition Has Adequately Demonstrated How This Research is Jeopardized by Section 1201.

The National Association of Manufacturers asks the Copyright Office to find that the Coalition did not adequately demonstrate enough of a need for the exemption, suggesting that only the statement from Jerome Radcliffe demonstrated a need for this exemption.[90] In so doing, the NAM glosses over the bibliography of dozens of published papers and studies in the field of independent medical device research that the Coalition provided with its comment, all of which now could not be repeated if the devices they studied employed TPMs.[91] For the increasing number of devices that, quite rightly, encrypt communications or source code, a researcher would have to circumvent the encryption to conduct the various forms of life-saving research described above.[92] This necessitates this exemption.

The NAM also argues that the chill to research should be considered *de minimis*, because the Coalition did not provide any evidence of research being done on TPM-enabled devices today.[93] The absence of illegal research does not obviate the need to make the research legal.[94] No existing system allows for the inspection of source code of medical devices, and AdvaMed's comment in this proceeding suggests they would never give it if asked.[95] As to research that may

[90] NAM COMMENT, *supra* note 3, at 4; *see* COALITION COMMENT, *supra* note 2, at App'x D ¶ 3. In its discussion, NAM tries to tweak the standard of proof here by reading a sentence about hypothetical harms out of context. NAM COMMENT, *supra* note 3, at 5. The standard for showing a need for an exemption is a preponderance of the evidence. *See* Notice of Inquiry, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 79 Fed. Reg. 55,687, 55,689 (Sept. 17, 2014). Here, the Coalition has shown that research on devices that now have TPMs was done before, that it is currently adversely affecting research, and that adoption of TPMs will only continue over the next few years, which neither NAM nor any other commenter disputes. The only difference between the research that has been done before and today is the presence of TPMs.

[91] COALITION COMMENT, *supra* note 2, at App'x B.

[92] The NAM seems to fundamentally misapprehend this point, by suggesting that "there is little reason to believe that the use of TPMs will substantially restrict the use of works for noninfringing uses." NAM COMMENT, *supra* note 3, at 3. Unless the researchers obtain permission or qualify under one of the statutory exemptions, which the Coalition's initial comment noted is not likely in many cases, see COALITION COMMENT, *supra* note 2, at 15–17, circumvention alone would implicate the DMCA.

[93] NAM COMMENT, *supra* note 3, at 4–5.

[94] 2010 RECOMMENDATION, *supra* note 20, at 187.

[95] ADVAMED COMMENT, *supra* note 3, at 3. AdvaMed suggests that the "FDA has recognized that access to the proprietary source code is not necessary for the evaluation of safety and efficacy." Once again, AdvaMed cites no authority for this point, and this time this is both incomplete and incorrect. In fact, the FDA *insists* that source code be maintained in many areas and made available for inspection, precisely because it can present risks. *See CPG Sec. 425.300 Computerized Drug Control Processing; Source Code for Process Control Application Programs*, FDA, http://www.fda.gov/ICECI/ComplianceManuals/

be occurring with permission, or occurring but not currently subject to a legal threat, this too should not be used to justify withholding an exemption. As the Register stated in the 2010 recommendation, "[t]he mere fact that legal action has not been brought against legitimate security researchers, or that permission may be available to some researchers from some companies, does not diminish the fact that legitimate researchers seeking to obey the law may understandably feel compelled to refrain from research that involves circumvention."[96] To do the research described in the Coalition's initial comment now often requires circumvention, and the opposition commenters offer no evidence to the contrary, only the suggestion that the industry can take care of it. And for reasons noted in the next section, it is clear that they cannot.

III. Independent Research Is Needed Notwithstanding The Existence of Some Collaboration Between Manufacturers and Researchers.

AdvaMed suggests that research into devices with TPMs should only be allowed to take place when the researchers enter into "formal agreements" with the device manufacturers.[97] The Coalition does not dispute that manufacturers should be encouraging and funding this form of research, but there is no area of health science or product safety where the lawful owner of an item would have to wait and obtain permission from its creator in order to research it.[98] This is largely for the same reason that fair use doctrine does not require a parodist to get permission from her subject; to do so would create an exclusive license to criticize, to the detriment of society.[99] Relying only on industry-funded research would also leave doctors, medical regulators, and the public with a skewed view of the world; it has been repeatedly demonstrated that industry-sponsored research tends to bias towards the industry's perspective and be less trustworthy.[100] Only truly independent research can correct that bias.

CompliancePolicyGuidanceManual/ucm074374.htm (last updated March 20, 2015); *see also* COALITION COMMENT, *supra* note 2, at App'x E ¶ 2.

[96] 2010 RECOMMENDATION, *supra* note 20, at 195.

[97] ADVAMED COMMENT, *supra* note 3, at 2; *see also* NAM COMMENT, *supra* note 3, at 6 (noting that "collaborative approaches" already exist to deal with these issues).

[98] *See* MATTHEW D. GREEN, SHORT COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. 1201 1 (Feb. 6, 2015), *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_shortform_MGreen_Class27.pdf (a professor in computer science, noting that it is "extremely important that security researchers are able to undertake good faith studies of networked medical devices with an aim at finding, disclosing, and fixing such vulnerabilities without fear of prosecution"). Independent research in the sciences is so fundamental to societal development that courts at times grant it constitutional significance. *See* ROBERT C. POST, DEMOCRACY, EXPERTISE, AND ACADEMIC FREEDOM 30–31 (2012) (gathering cases where courts spoke of scientific freedom of research in First Amendment terms).

[99] *See* Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 592 (1994) ("[T]here is no protectable derivative market for criticism.").

[100] *See, e.g.*, Ben Goldacre, *Trial Sans Error: How Pharma-Funded Research Cherry-Picks Positive Results*, SCIENTIFIC AMERICAN (Feb. 12, 2013), http://www.scientificamerican.com/article/trial-sans-error-how-pharma-funded-research-cherry-picks-positive-results/; Exxon Shipping Co. v. Baker, 554 U.S. 471, 501 n.17 (2008) (declining to rely on studies in deciding a case against Exxon "[b]ecause this research was funded in part by

Opponents to exemptions in earlier rulemakings have taken similar positions as the opponents here, and the Register has correctly rejected them. In 2010, Prof. J. Alex Halderman sought (and in a modified version, obtained) an exemption to study video game vulnerabilities, noting in particular the need to study such systems because of a recent issue with the Macrovision SafeDisc program, which was found to contain an exploit for malware by an antivirus company.[101] Opposition commenters in part argued that the current "security ecosystem" was adequate to handle those concerns.[102] Register Peters rejected that contention, noting that the opponents had failed to show that the ecosystem adequately responded to the problems with SafeDisc on their own, and that independent research had a role to play in this "security ecosystem."[103] Here, no opponent has disputed the social significance of the medical device safety, nor have they produced any evidence to rebut the existence of numerous recalls and deaths that have been attributed to software problems in medical devices,[104] nor do they dispute that independent research has played a role in improving device security.[105]

Opposition commenters also cite to existing research happening at university-affiliated research centers, including the Archimedes Research Center for Medical Device Security at the University of Michigan, as evidence that the exemption is not necessary.[106] Not only does this fail to address the concerns the Coalition has raised about the continuing presence of flaws in devices, but such university-affiliated research institutions would actually be direct beneficiaries of this exemption. The commenters here seem to imply that the Archimedes Center conducts research exclusively with the consent of the relevant manufacturers, when instead it actively solicits donations from the public of explanted devices that are no longer used in human care.[107] The Center's website explicitly states that "[i]ndependent, boundary-pushing research can improve the trustworthiness of software-controlled medical devices."[108] If this exemption were denied, centers like Archimedes may not be able to conduct research on such devices if they contained encryption without the express prior consent of the manufacturer. This will necessarily foreclose considerable amounts of valuable research.

Exxon"). In the world of medical devices specifically, a group of independent scientists in 2011 published an extensive criticism of Medtronic's "Infuse" spinal growth product, noting that the company had funded "misleading and biased" studies of the device. Barry Meier & Duff Wilson, *Spine Experts Repudiate Medtronic Studies*, NEW YORK TIMES (June 28, 2011), http://www.nytimes.com/2011/06/29/business/29spine.html.

[101] *See* 2010 RECOMMENDATION, *supra* note 20, at 189–203.

[102] *Id.* at 202.

[103] *Id.* at 202–03

[104] COALITION COMMENT, *supra* note 2, at 21.

[105] *See supra* notes 31–35 and accompanying text.

[106] ADVAMED COMMENT, *supra* note 3, at 3; NAM COMMENT, *supra* note 3, at 6; IPO COMMENT, *supra* note 3, at 2.

[107] *See Donate Medical Devices to Our Library*, ARCHIMEDES RESEARCH CTR. FOR MEDICAL DEVICE SECURITY, http://secure-medicine.org/library/donate (last viewed April 28, 2015).

[108] *Id.*

Finally, several opponents argue that they simply should be trusted to do this research themselves, noting that they have the "incentive" to ensure the safety and security of their products.[109] But as Register Peters noted in an earlier rulemaking, "[t]he incentives of a company to fix its own problems . . . are not necessarily sufficient to publicize, investigate or remedially address flaws or vulnerabilities found to exist" and that companies do not always "have good reason to discover, publicize and repair" their flaws.[110]

The history of medical device research tragically bears this out. The Coalition noted in its original comment several examples where manufacturers knew of defects but did not disclose them until they caused patient deaths.[111] No death has yet been attributed to last month's discovery of vulnerabilities in Hospira drug pumps, but the order of events to remedy the issue is an all-too familiar one.[112] It was independent researcher Billy Rios – and not Hospira – that discovered a vulnerability in the drug pump in question by analyzing a decommissioned device he obtained online. Rios notified DHS of the vulnerability, and DHS subsequently notified Hospira and the FDA. When Hospira was notified, however, it refused to fix the vulnerability, or investigate whether other devices in the same product line suffered from similar flaws.[113] It was only after DHS published a warning about the vulnerability, and *Wired* magazine published a story on the same, that Hospira released an update to the software.[114] As noted by the Coalition before, and by the opposition commenters themselves,[115] fixing a problem can be quite expensive, and thus companies may avoid doing so if they feel that they can get away without.[116]

In its conclusion to its opposition, AdvaMed states that "publicity related to" security research can "cause[] the public to believe that these life-saving medical devices are not safe or secure."[117] But history teaches us that the public often has a good reason for this conclusion.[118]

---

[109] NAM COMMENT, *supra* note 3, at 3.
[110] 2010 RECOMMENDATION, *supra* note 20, at 189. Notably, Jay Schulman, an opponent to the exemption here, has written separately that companies should rely on independent researchers to avoid issues like corporate groupthink. *See* Jay Schulman, *Why Your Strategy Needs a Consultant*, BUILDING A CAREER IN LIFE AND SECURITY (Jan. 29, 2015), https://www.jayschulman.com/strategy-needs-consultant/.
[111] COALITION COMMENT, *supra* note 2, at 21.
[112] *See* Zetter, *supra* note 21.
[113] *See id.*
[114] *See id.*; *Hospira MedNet Vulnerabilites*, DHS ICS-CERT (March 31, 2015), https://ics-cert.us-cert.gov/advisories/ICSA-15-090-03.
[115] SCHULMAN COMMENT, *supra* note 3, at 1.
[116] The NAM suggests that flaws should be disclosed to the manufacturer, so that they can coordinate a response with the FDA. NAM COMMENT, *supra* note 3, at 7. That may be true in some cases, but given the tragic stories noted above and the example of Hospira here, one could certainly sympathize with a researcher who opts instead to go directly to the FDA, DHS, or the press to raise the issue.
[117] ADVAMED COMMENT, *supra* note 3, at 7.
[118] The opposition comments themselves give even more cause to be concerned. In its opposition here, AdvaMed suggests that access one's own base station could reveal personal medical information of other patients. ADVAMED COMMENT, *supra* note 3, at 2 ("Where unauthorized

Time and again, medical devices have been proven not to be as safe as manufacturers and their contractors claim them to be. Manufacturer-funded research may be a necessary ingredient to the security ecosystem, but it is not sufficient. Independent research is essential.

IV. The FDA and Other Safety and Security Agencies Actively Rely on Independent Research, and Denying This Prohibition Will Supplant the FDA's Authority for that of the Copyright Office

The commenters state repeatedly that the FDA is the agency responsible for ensuring the safety, efficacy, and security of medical devices, and that, in the words of the AdvaMed Comment, it "should retain regulatory supremacy" in this domain.[119] The Coalition agrees that the FDA should be the lead agency on matters of health and safety, just as the Copyright Office should be the lead agency on matters of copyright and digital piracy. This best effectuates the will of Congress in delegating power to both agencies. But this is an argument in favor of granting this exemption, rather than denying it.

As noted above, independent research on medical devices has been taking place for decades prior to this rulemaking. It is only now that manufacturers are implementing encryption and other TPMs that such research has begun to raise DMCA issues.[120] This means that, for the first time, the Copyright Office is put in the position of determining whether the presence of TPMs should stop this field of medical research. The overlapping authority of the FDA and the Copyright Office in this space is not itself a reason to grant this exemption, but as in all areas of regulatory overlap, the most effective response is for each agency to regulate according to its expertise, and avoid duplicative efforts.[121] This is the model that the FDA currently takes with other agencies that overlap its activities, including the Federal Communications Commission and the Office of the National Coordinator for Health Information Technology.[122]

---

circumvention activity is utilized to access the corresponding monitoring system of an implanted or attached device . . . [information] of other patients may be compromised."); *id.* at 7 ("[N]etworked devices could be used to access information which third parties should not be able to access."). The implication that third-party patient data is being stored or can be retrieved on a different patient's at-home monitoring system suggests shockingly careless patient data handling practices on the part of medical device manufacturers. Like the overwhelming majority of comments they made, however, AdvaMed does not offer any substantiation on this point, and so it is not clear how seriously one should take this confession. In any event, the Coalition has not discovered any evidence to indicate that patient data is being mismanaged in this way.

[119] ADVAMED COMMENT, *supra* note 3, at 1; *see also* NAM COMMENT, *supra* note 3, at 7; LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 3.

[120] *See supra* notes 5–7 and accompanying text.

[121] *See* Todd S. Aagaard, *Regulatory Overlap, Overlapping Legal Fields, and Statutory Discontinuities*, 29 VA. ENV. L.J. 237, 289 (2011).

[122] *See* FDASIA HEALTH IT REPORT: PROPOSED STRATEGY AND RECOMMENDATIONS FOR A RISK-BASED FRAMEWORK 28 (Apr. 2014), *available at* http://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf (noting that the three agencies "intend to establish a tri-Agency MOU to clarify how we will exchange information with each other, discuss safety issues

On the health and safety side, the FDA already actively regulates medical devices, and it does so with independent research as a key part of its system.[123] As noted above, the FDA's approach has been to treat device research as a "shared responsibility" between numerous stakeholders.[124] Thus, even though the FDA imposes requirements on medical device manufacturers and a few other entities to report adverse events from medical devices, it also encourages other healthcare professionals, patients, and consumers to monitor medical device performance and voluntarily report adverse events or product problems.[125] It invites independent researchers to many of the workshops and conferences it convenes, including the ones cited by the opposition commenters.[126] Contrary to what LifeScience Alley suggests, allowing researchers to participate in this system is not acting in "direct opposition" to this shared responsibility;[127] it is recognizing the vital role already played by independent research.

Independent research also helps the FDA better do its job. A major point of contention in the realm of medical device regulation is when the FDA should subject a device to its full premarket approval procedure, as opposed to only requiring notification of a device's release because it is "substantially equivalent" to one already on the market (referred to as "510(k) notification").[128] A critical question in this determination is when new software should be treated as "substantially equivalent" to existing software. On this point, independent research has been published to enlighten the FDA of the consequences of the decision one way or another, and thus inform the FDA on how it addresses such issues.[129]

On the copyright side, this Office has repeatedly stated that the focus of this rulemaking is to determine whether the presence of TPMs is "diminishing the ability of individuals to use . . .

---

that may involve more than one agency, coordinate activities, and consider how the three Agencies will address new technologies . . . .").

[123] *See supra* notes 36–47 and accompanying text.

[124] *See* COALITION COMMENT, *supra* note 2, at 19 (citing FDA CYBERSECURITY GUIDANCE, *supra* note 6, at 3); LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 2.

[125] *See Medical Device Reporting (MDR)*, FDA, http://www.fda.gov/MedicalDevices/Safety/ReportaProblem/default.htm#voluntary (last updated February 3, 2015); COALITION COMMENT, *supra* note 2, at 20–21.

[126] *See supra* note 31 and accompanying text.

[127] LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 2. The Intellectual Property Owners Association comment that "[t]he FDA agrees that access should be limited" is similarly incorrect and misleading. *See* IPO COMMENT, *supra* note 3, at 1. Nowhere on the FDA website cited by IPO does it state that researchers and patients should not be allowed to access devices – in fact, it cites numerous conferences, workshops, and mechanisms where independent researchers have been actively involved. *See Cybersecurity*, *supra* note 18.

[128] JUDITH A. JOHNSON, FDA REGULATION OF MEDICAL DEVICES, CONGRESSIONAL RESEARCH SERV. NO. R42130 (June 25, 2012), *available at* https://www.fas.org/sgp/crs/misc/R42130.pdf.

[129] *See* Kevin Fu, *Trustworthy Medical Device Software*, *in* PUBLIC HEALTH EFFECTIVENESS OF THE FDA 510(K) CLEARANCE PROCESS (2011).

works in ways that are otherwise lawful."[130] This is, at its heart, a concern about the tradeoff between allowing noninfringing uses of works and enabling digital piracy. Register Pallante stressed in the last rulemaking that when the evidence suggests, "at best, only a tenuous relationship between [the exempted activity] and piracy," granting the exemption is favored.[131] As already stated, no copy of a device's software or data made in the process of conducting security research or extracting one's own medical information could ever replace the need for a medical device in the first place, as the copy cannot possibly provide the patient with the therapy that the physical device does.[132] The other factors this Office must consider, including whether prohibitions on circumvention negatively impact criticism and what effect the TPMs have on the market for or value of copyright works, undoubtedly favor the Coalition as well.[133]

To the extent that the Copyright Office is concerned about the health and safety of medical device users, the Coalition feels this concern even more acutely, as each of its members both researches and uses a medical device for life-sustaining treatment.[134] The research is done to ensure that these devices are safe for themselves and others. The FDA also undoubtedly wants to keep patients healthy and safe, and it relies extensively on independent research of the kind discussed here in order to do so. To the extent that the FDA would ever change their mind, nothing the Copyright Office does here would prevent them from exercising their own regulatory powers in this space.[135] On the other hand, declining this exemption would mean that, for the first time, there would be a type of medical device that would not be subject to the independent research favored by the FDA.

V. The Proposed Uses Here are Non-Infringing Uses, and Do Not Implicate Other Laws

All of the commenters focused mainly on the factual question of whether this research should be allowed to continue, but a few raised legal concerns as well. With respect to copyright law, AdvaMed very briefly raises some objections to the Coalition's fair use argument as it relates to reverse engineering (though not as it relates to patients accessing their own data).[136] Rather than cite any cases that rebut the many precedents discussed at length by this Coalition in its original comment, AdvaMed instead asks a series of rhetorical questions that appear to raise two main objections. First, AdvaMed suggests that the fact that Jerome Radcliffe, one of the Coalition members, later found work in the security research space should mean that his research was not

---

[130] U.S. COPYRIGHT OFFICE, SECTION 1201 RULEMAKING: FIFTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION 5 (2012) (quoting H.R. REP. NO. 105-551, pt. 2, at 37).
[131] *Id.* at 77.
[132] COALITION COMMENT, *supra* note 2, at 25.
[133] 17 U.S.C. § 1201(a)(1)(C); *see* COALITION COMMENT, *supra* note 2, at 23-25.
[134] COALITION COMMENT, *supra* note 2, at App'x C ¶ 1, App'x D ¶ 2, App'x E ¶ 2, App'x F ¶ 1.
[135] *See* PUBLIC KNOWLEDGE, LONG COMMENT REGARDING A PROPOSED EXEMPTION 4 (Feb. 6, 2015), http://copyright.gov/1201/2015/comments-020615/InitialComments_LongForm_PublicKnowledge.pdf ("To the extent that the purpose would violate other rules, nothing in section 1201 supersedes or obviates those rules.").
[136] ADVAMED COMMENT, *supra* note 3, at 5–6.

"non-commercial" under fair use law.[137] Second, AdvaMed halfheartedly suggests that "[c]ourts have typically required small portions of the copyrighted work to be used in order for the use to be considered a fair use."[138] (The Coalition uses the term "halfheartedly" advisedly; the only case they cite in this discussion is a case that found the appropriation of an entire work to be a fair use.[139])

On the commerciality side, Register Peters noted in the 2010 rulemaking that "[a]lthough researchers may receive indirect benefits from scholarship (e.g., tenure and publicity), the same may be said for any scholarly research."[140] The research conducted by Jerome Radcliffe was independently developed and published,[141] but even if it were done as a commissioned or funded study, the mere fact that an activity is conducted for profit does presumptively foreclose a finding of fair use, and the Coalition cited numerous cases where research of the kind considered here was fair even when done commercially.[142] If that were the case, then nearly all the illustrative uses listed in Section 107 would be "swallowed up" by the presumption, since those activities are "generally conducted for profit in this country."[143] A more important question, especially to courts today, is whether a use is transformative.[144] The Coalition has already demonstrated that this use is transformative,[145] the discussion of the Register in an earlier rulemaking seems to agree,[146] and the opposition commenters offer no rebuttal.

Opposition commenters also argue that because researchers seek to make an internal copy of most or all of the software in analyzing it, their use is unlikely to be fair.[147] This is wrong. Numerous courts have ruled in recent years that copies of an entire work can be fair, particularly

[137] *Id.*
[138] *Id.* at 6.
[139] *Id.* at 6 n.8 (citing Swatch Grp. Mgmt. Servs. Ltd. v. Bloomberg L.P., 756 F.3d 73 (2d Cir. 2014)); *see Swatch*, 756 F.3d at 90 (noting that the district court found that copying all of a work favored neither party and the use was ultimately fair, and that this analysis is "entirely consistent with our case law").
[140] 2010 RECOMMENDATION, *supra* note 20, at 184.
[141] *See generally* COALITION COMMENT, *supra* note 2, at App'x D ¶ 2–3.
[142] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 584 (1994); *see* COALITION COMMENT, *supra* note 2, at 12–14 (citing, e.g, A.V. v. iParadigms, LLC, 562 F.3d 630 (4th Cir. 2009); Sony Computer Entm't Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000)).
[143] *Campbell*, 510 U.S. at 584.
[144] Neil Weinstock Netanel, *Making Sense of Fair Use*, 15 LEWIS & CLARK L. REV. 715, 734–44 (2011) (noting the rise in prominence of the transformativeness in recent court decisions).
[145] *See* COALITION COMMENT, *supra* note 2, at 11–15.
[146] *See* 2010 RECOMMENDATION, *supra* note 20, at 184 (noting that "security research is transformative because it serves an entirely different purpose " and the copies made are "analogous to reverse engineering" because they are copies made "as a means to another end, that is, to understand the functioning of the [technology] in order to assess potential vulnerabilities").
[147] ADVAMED COMMENT, *supra* note 3, at 6.

when the use is transformative and does not impact markets for the original.[148] AdvaMed cited one such case, *Swatch Group Management v. Bloomberg L.P.*, where the Second Circuit ruled that Bloomberg's use and distribution of an entire copy of a protected recording of a conference call was fair.[149] The critical question is whether the amount taken is reasonably necessary in light of the use, and the Coalition has already demonstrated why it is here.[150] There can be no real doubt that the uses contemplated here are fair.

LifeScience Alley also suggests that trade secret law could be implicated by this exemption, but do not explain how this would be so.[151] Trade secret law tends to only be imposed where there is some breach of a duty to keep information secret, and reverse engineering or independent discovery have always been thought to be outside the doctrine.[152] LifeScience Alley provides no reasons as to why the circumstances here would warrant a different result.

Additionally, and once again without any substantiation, AdvaMed and the Intellectual Property Owners Association suggest that triggering transmissions of data to manufacturers' servers could implicate the Computer Fraud and Abuse Act or Health Insurance Portability and Accountability Act ("HIPAA").[153] As to HIPAA, the opposition commenters do not explain how HIPAA would preclude this research, only that, in the words of AdvaMed, it "rais[es] HIPAA concerns."[154] To suggest that this statute prevents patients from accessing their own data would be to read this statute in exactly the opposite way than it was intended. HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act ("HITECH"), specifically provides mechanisms by which patients have a right to obtain copies of their own health information.[155] More to the point, it only restricts the actions of "covered entities" and their associates,[156] of whom independent researchers would not qualify, and it only applies as to individually identifiable health information, which excludes entirely all research done on devices not used in patient care.[157]

Claims related to the Computer Fraud and Abuse Act and state analogues similarly merit little discussion. Such laws tend only to apply when a person obtains information from a computer

---

[148] *See, e.g.*, *Swatch*, 756 F.3d at 90; Authors Guild, Inc. v. HathiTrust, 755 F.3d 87, 98–99 (2d Cir. 2014); *iParadigms*, 562 F.3d at 642; Ty, Inc. v. Publication Int'l Ltd., 292 F.3d 512, 522 (7th Cir. 2002).
[149] *Swatch*, 756 F.3d at 90.
[150] *See* COALITION COMMENT, *supra* note 2, at 12.
[151] LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 5.
[152] *See generally* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine In Search of Justification*, 86 CAL. L. REV. 269–70 (1998).
[153] ADVAMED COMMENT, *supra* note 3, at 4; IPO COMMENT, *supra* note 3, at 3.
[154] ADVAMED COMMENT, *supra* note 3, at 4; *see also* MDISS COMMENT, *supra* note 4, at 1 ("It's not clear that HIPAA supports access to PHI proposed").
[155] *See* 45 C.F.R. § 164.524; C. STEPHEN REDHEAD, THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH (HITECH) ACT, CONGRESSIONAL RESEARCH SERV. NO. R40161 at 4 (2009).
[156] *See* 45 C.F.R. § 160.103.
[157] § 160.103.

without authorization, or cause damage to a computer system without authorization.[158] Based on the absence of contracts to the contrary, patients or researches own their respective medical device, and thus any access to them would be authorized.[159] The opposition commenters provide no exceptions to this general rule, or any argument to the contrary.[160]

In sum, there is no area of law that precludes the research and patient access to data contemplated in this exemption. The only legal hurdle is anticircumvention, which, for the reasons noted above, should be exempted in this case.

VI. The Proposed Exemption is Sufficiently Narrow, and the Coalition Accepts a Clarification to Specify That Patient Devices May Only Be Used With Permission From the Patient.

Finally, the opposition commenters raised some objections to the possible scope of the exemption. First, LifeScience Alley proposes a clarification that attempts to resolve a potential ambiguity in the exemption, by specifying that access to devices that are currently used in patient care should be allowed only if the patient consents.[161] The Coalition has no objection to that clarification. The Coalition proposes the following modification in light of that concern (emphasis added to highlight the difference between versions):

> Computer programs, in the form of firmware or software, including the outputs generated by those programs, that are contained within or generated by medical devices and their corresponding monitoring systems, when such devices are designed for attachment to or implantation in patients, and where such circumvention is
>
> (1) at the direction of a patient seeking access to information generated by his or her own device, or
>
> (2) at the direction of those conducting research into the safety, security, and effectiveness of such devices, *provided that such research does not involve devices that are currently used in patient care unless the researcher obtains the patient's informed consent*.

Second, the National Association of Manufacturers objected to the general term "those conducting research," as containing a "potentially limitless class."[162] The NAM does not offer a limiting construction, or any evidence as to why a broad definition of researcher would be inappropriate here (other than general objections on safety grounds, which have been addressed

---

[158] 18 U.S.C. §§ 1030(a)(2), (a)(5).

[159] As noted already, the commenters here do not dispute that patients and researchers are the owners of their devices, and not mere licensees. *See supra* notes 29–30 and accompanying text.

[160] AdvaMed briefly attempts to flip this concept, and argues that triggering a device to send data to a manufacturer's system would be an unauthorized access of the system, instead of the device. ADVAMED COMMENT, *supra* note 3, at 4. Even if true, such delivery of data *to* a system does not violate the Computer Fraud and Abuse Act, only obtaining information *from* the system does. *See* 18 U.S.C. § 1030(a)(2)(C).

[161] LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 6.

[162] NAM COMMENT, *supra* note 3, at 2.

above). The Coalition opposes this modification. Keeping a broad definition of a researcher here is reflective of the state of the medical device research field itself, and essential to ensuring that the current state of medical device research is allowed to continue.[163] As the Coalition demonstrated, many forms of critical device research comes from those acting entirely outside of universities, trade associations, or professional security firms.[164]

Third, opposition commenters allege that the requested exemption category is too broad, arguing that software-enabled "medical devices and their corresponding monitoring systems, when such devices are designed for attachment to or implantation in patients" is overly broad, and could extend beyond cardiac and diabetes devices to include neurostimulators, ambulatory monitoring devices, and cochlear implants.[165] The Coalition believes that limiting medical devices to those designed for personal attachment or implantation already provides a sufficiently narrow class. As to each of the devices mentioned here, the exact same concerns to patient life and safety due to software mismanagement or vulnerabilities are present, and independent medical research helps rectify these harms. Much of the research already cited by the Coalition applies generally to all software-enable personal medical devices,[166] and separate independent research has specifically addressed security concerns with neural devices and cochlear implants.[167] There is no reason why the same logic would not extend to research already being conducted in those areas.

VII. Conclusion

In response to the Coalition's detailed initial comment, the opposition commenters here offered little beyond conjecture, rhetorical questions, and hypothetical concerns. As detailed above, such generalized objections are contrary to the requirements of the NPRM, and completely unfounded on the facts. Independent medical device research plays a critical role in ensuring the well being of device users, both individually and in the aggregate. There is no reason why it should be stopped simply because manufacturers now employ TPMs in these devices. Accordingly, the Coalition here requests that the Register recommend the exemption for Class 27.

---

[163] *See* COALITION COMMENT, *supra* note 2, at 21–22.
[164] *See supra* notes 31–47 and accompanying text.
[165] See IPO COMMENT, *supra* note 3, at 2; LIFESCIENCE ALLEY COMMENT, *supra* note 3, at 4; ADVAMED COMMENT, *supra* note 3, at 4.
[166] *See* COALITION COMMENT, *supra* note 2, at App'x B ¶¶ 1–3, 6–7, 9–15, 17, 19–22, 24, 29, 31–36.
[167] *See* Tamara Denning et al., *Neurosecurity: Security and Privacy for Neural Devices*, 27 NEUROSURG FOCUS 1 (2009); Jeremy A. Hansen & Nicole M. Hansen, *A Taxonomy of Vulnerabilities in Implantable Medical Devices*, *in* PROCEEDINGS OF THE 2ND USENIX WORKSHOP ON HEALTH SECURITY AND PRIVACY (2011) (discussing, *inter alia*, specific interference risks with cochlear implants).

Respectfully submitted,

Andrew F. Sellars
Clinical Fellow, Cyberlaw Clinic
Berkman Center for Internet & Society
Harvard Law School
23 Everett Street, Second Floor
Cambridge, MA 02138
(617) 384-9125
asellars@cyber.law.harvard.edu[168]

[168] The Coalition wishes to thank Cyberlaw Clinic students Jonathan Diaz and Shudan Shen for their valuable contributions to this comment.