BEFORE THE UNITED STATES COPYRIGHT OFFICE
LIBRARY OF CONGRESS

LONG COMMENT REGARDING A PROPOSED EXEMPTION UNDER 17 U.S.C. § 1201
Docket No. 2014-07

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 Systems for Access Control Technologies[1] ("NPRM"), a Coalition of Medical Device Researchers[2] (the "Coalition") submits the following comment and respectfully requests the Copyright Office to recommend Proposed Class 27 for exemption pursuant to 17 U.S.C. § 1201(a)(1)(C).

I. Commenter Information

These 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

II. Proposed Class Addressed

These comments relate to Proposed Class #27: Software—Networked Medical Devices.[3] In its initial petition, the Coalition proposed the following language for the exemption:

> 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.

---

[1] 79 Fed. Reg. 73,856 (Dec. 12, 2014) [hereinafter NPRM].
[2] The members of this Coalition are listed in Appendix A.
[3] *See* NPRM, *supra* note 1, at 73,871.

III. Overview

The members of the Coalition are patients and researchers who study the safety, security, and effectiveness of networked medical devices. They, and researchers like them, seek to access the computer code and data outputs of medical devices,[4] and use this information to analyze the safety and performance of these devices, both in general and as they apply to particular patients.

This independent research is essential to public health. Millions of Americans rely on implantable devices to monitor and treat medical issues, including diabetes, cardiac arrhythmia, cardiomyopathy, and numerous others.[5] The past several years have seen a tremendous increase in the adoption of computerized medical devices.[6] This increase, however, has heightened concerns around medical device safety, security, and effectiveness.[7] Computerized medical devices can fail in many ways, including through programming errors, incorrect calibration, and exposure to malicious intrusions, as well as physical or medical errors.[8] Over a thousand recalls were issued on software-based medical devices from 1999 to 2005.[9] Hundreds of deaths have been attributed to software failure in medical devices.[10]

The threat of medical device "hacking" by malicious actors tends to captivate popular media,[11] but latent software bugs and design defects present the greatest ongoing threats to patient

---

[4] The term "medical device" is meant to encompass devices that are physically implanted in whole or in part to the body and are used as part of the delivery of therapy and medical care to a patient. This can be distinguished from consumer health devices, such as digital pedometers and other devices that gather data and report their results directly to the patient. "Medical devices" are meant to include devices such as pacemakers, implantable cardioverter defibrillators, insulin pumps, and continuous glucose monitors. For an illustration of how a networked pacemaker works, see Daniel Halperin et al., *Security and Privacy for Implantable Medical Devices*, 7 IEEE: PERVASIVE COMPUTING 30, 32 (2008) [hereinafter Halperin, *Security and Privacy*]. For an illustration of an insulin pump, see U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-816, FDA SHOULD EXPAND ITS CONSIDERATION OF INFORMATION SECURITY FOR CERTAIN TYPES OF DEVICES 7 (2012) [hereinafter GAO REPORT].

[5] *See* discussion in section VI., *infra*.

[6] Homa Alemzadeh et al., *Analysis of Safety-Critical Computer Failures in Medical Devices*, 11 IEEE SECURITY & PRIVACY 14, 14 (2013).

[7] *See, e.g.*, David Talbot, *Computer Viruses are "Rampant" on Medical Devices in Hospitals*, MIT TECH. REV. (Oct. 17, 2012), http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/.

[8] RICHARD C. FRIES, RELIABLE DESIGN OF MEDICAL DEVICES 18–21 (3d ed. 2013).

[9] Alemzadeh, *supra* note 6, at 14.

[10] *Id.* at 22.

[11] *See, e.g.*, Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASHINGTON POST (Oct. 21, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/; *Homeland: Broken Hearts* (Showtime television broadcast Dec. 2, 2012) (an episode of a popular television series where pacemaker device hacking plays prominently).

safety.[12] Medical devices also pose risks for patients by what they withhold – namely, the actual data measured within the patient's body, which a patient is unable to access except through periodic checkups with a doctor.[13] This arrangement means that patients are not put in a position to detect errors in devices, or use the information from these devices to determine whether a medical emergency is occurring.[14] Because patients are isolated from their own data, serious health risks could go completely unnoticed.[15]

Independent research and analysis, done at the direction of patients and scholars, effectively addresses these problems. Numerous publications and presentations by independent researchers have identified design flaws, software bugs, and possible points of malicious intrusion.[16] The Government Accountability Office ("GAO") and Food and Drug Administration ("FDA") specifically cite this research as a basis for devoting additional resources to improving the cybersecurity of medical devices.[17] On the access to data side, a growing body of research is developing to show how greater patient access to data can improve patient health and detect developing medical issues.[18]

Such work often requires researchers and patients to access the underlying computer code and outputs from these devices.[19] Previously, this did not implicate anticircumvention law at all, because medical device companies were leaving the data outputs and computer code unprotected. Medical device manufacturers, however, are increasingly adopting technologies around the computer code and data outputs of devices that may be classified as technological protection measures ("TPMs") under 17 U.S.C. § 1201(a)(1). While this is a welcome development for patient safety,[20] it puts continuing research at risk of violating anticircumvention law. In order to ensure that this life-saving research is allowed to continue, the

---

[12] *See* MIIA VUONTISJÄRVI & KARI HYTÖNEN, CODENOMICON, MEDICAL DEVICES IN MODERN DAY WORLD 3 (2014); Kevin Fu, *Stop the Insanity. Stop Sensationalism of Medical Device Security.*, ARCHIMEDES RESEARCH CTR. FOR MEDICAL DEVICE SECURITY (Oct. 30, 2012), http://blog.secure-medicine.org/2012/10/stop-insanity-stop-sensationalism-of.html.
[13] Statement of Hugo Campos, Appendix C, ¶¶ 7-9.
[14] TEDX Talks, *Hugo Campos Fights for the Right to Open His Heart's Data*, TEDX CAMBRIDGE (Jan 20, 2012), http://tedxtalks.ted.com/video/TEDxCambridge-Hugo-Campos-fight; Emily Singer, *Getting Health Data from Inside Your Body*, MIT TECH. REV. (Nov. 22, 2011), http://www.technologyreview.com/news/426171/getting-health-data-from-inside-your-body/.
[15] Statement of Hugo Campos, Appendix C, ¶ 8 (detailing numerous risks that devices currently can detect, but do not share with patients).
[16] A sample bibliography of research is attached as Appendix B.
[17] GAO REPORT, *supra* note 4, at 2 (citing third-party research by Coalition member Jerome Radcliffe, and others, as a basis for recommending FDA reforms); *Public Workshop – Collaborative Approaches for Medical Device and Healthcare Cybersecurity*, FDA, http://www.fda.gov/ MedicalDevices/NewsEvents/WorkshopsConferences/ucm412979.htm (discussing a recent multistakeholder conference on medical device security that included independent researchers).
[18] *See* Appendix B.
[19] *See* Section IV.C., *infra*.
[20] *See* Statement of Karen Sandler, Appendix E, ¶ 6.

Coalition respectfully requests that the Register recommend the above exemption.

IV. Technological Protection Measures and Methods of Circumvention.

This exemption seeks to allow researchers to access the computer code operating in medical devices and their corresponding monitoring systems, as well the outputs generated by such devices. The following section details the copyrighted works at issue, the TPMs that protect those works, and how they would be circumvented while conducting this research.

A. Works in Question: Computer Code and Data Outputs of Medical Devices

The members of this Coalition, and researchers like them, seek to access the computer code and data outputs of medical devices. The presence of computer code in devices like these is ubiquitous and essential to their operation. Computerized software inherently embodies the "object code," or the long strings of binary ones and zeroes that a computer actually uses to execute instructions.[21] Depending on the specific form of research, researchers may wish to access this code alone, or they may wish to decompile the object code to reveal the underlying source code, or the programming language used by developers when coding the device.[22] In either case, computer code is treated as a literary work under copyright law.[23]

The members of this Coalition also seek to access the data outputs of these devices. In the NPRM, the Copyright Office asked specifically whether these outputs should be considered a protectable work under copyright law.[24] There is no universal answer to that question, but based on current caselaw, it is likely that many of the outputs in question here are not protectable. As to these outputs, researchers are free to circumvent any TPMs that may govern access, notwithstanding section 1201.[25] Some outputs, however, may have the necessary original

---

[21] Andrew Johnson-Laird, *Software Reverse Engineering in the Real World*, 19 U. DAYTONA L. REV. 843, 858–60 (1994); *see* Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1243 (3d Cir. 1983).

[22] *See* Section IV.C., *infra*.

[23] 17 U.S.C. § 101 (defining "computer programs"); U.S COPYRIGHT OFFICE, COMPENDIUM OF U.S. COPYRIGHT OFFICE PRACTICES §§ 721.3, 721.4 (3d ed. 2014) [hereinafter COMPENDIUM III]. While this Office has indicated that it will defer to courts on interpreting questions of law during this proceeding, references to the Compendium are instructive because they are so persuasive to courts. *See, e.g.*, Muench Photography, Inc. v. Houghton Mifflin Harcourt Publ'g Co., 712 F. Supp. 2d 84, 91–92 (S.D.N.Y. 2010) (according *Skidmore* deference, from Skidmore v. Swift & Co., 323 U.S. 134 (1944), to Copyright Office Circulars and the Compendium).

[24] NPRM, *supra* note 1, at 73,781 (asking commenters to address "[w]hether the outputs generated by the medical device programs constitute copyright-protected materials").

[25] 17 U.S.C. § 1201(a)(1)(A) (protecting "a work protected under this title"); U.S. COPYRIGHT OFFICE, SECTION 1201 RULEMAKING: FIFTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION 14 n.66 (2012) [hereinafter 2012 RECOMMENDATION].

selection and arrangement to be protectable expressions, although their protection is quite thin.[26] Accessing protectable outputs may raise anticircumvention issues.

Data outputs on devices can vary from streams of real-time data to batch "reports" transmitted from the device either on a set schedule or when prompted by a wired or wireless connection to device reader.[27] In most cases the data consists principally of the readouts of sensors gathering information on the physical characteristics of the patient and records of device activity, but the device may also transmit other information, including the patient's name, the treating physician's name, information about the date of installation, and other facts that may be relevant to the patient's care.[28]

Streamed data is highly unlikely to be a protectable work under copyright law for several reasons. A constant readout of data from a device reveals nothing more than a fact of nature, which, like an idea, is not protectable unless embodied in an original expression.[29] A comprehensive readout also shows no selection of information, a requirement for protection of a compilation of data.[30] Furthermore, real-time transmissions of instrument measurements may not be sufficiently "fixed" to be a protectable work if they are not being saved simultaneously with their transmission.[31]

---

[26] *See infra* notes 27–36 and accompanying text; Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 349 (1991) (noting that rights in factual compilations is "thin," as "a subsequent compiler remains free to use the facts contained in another's publication to aid in preparing a competing work").

[27] Statement of Hugo Campos, Appendix C, ¶ 12 (describing the "PDD" file his device generates when dispatching a report); Pedro Pereira Rodrigues et al., *Learning from Medical Data Streams*, AIME 2011 WORKSHOP REPORT 2 (2011), *available at* http://www.kdd.org/sites/default/files/lemedsKDD2011_Report_Submitted.pdf.

[28] Daniel Halperin et al., *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*, IEEE SYMPOSIUM ON SECURITY & PRIVACY 129, 135 (2008) [hereinafter Halperin, *Pacemakers*].

[29] *Feist*, 499 U.S. at 347–48; Triange Publ'ns, Inc. v. Sports Eye, Inc., 415 F. Supp. 682, 685 n.9 (E.D. Pa. 1976) ("For the purposes of copyright infringement, data and ideas are treated as equivalents."). This logic extends whether the data is expressed in numbers or as a medical graph. *See* COMPENDIUM III, *supra* note 23, § 924.3(D) (Copyright Office will generally deny registration of medical imaging as a useful article, including "electrocardiography" and "magnetic resonance imaging").

[30] *See* Matthew Bender & Co., Inc. v. West Publ'g Co., 158 F.3d 674, 687 (2d Cir. 1998) (West's inclusion of every Supreme Court opinion in its database made no "selection" for copyright purposes); *Feist*, 499 U.S. at 363 (the fact that company did not "select" what to include was alternative grounds for rejecting infringement claim).

[31] *See* 17 U.S.C. § 102(a) ("Copyright protection subsists . . . in original works of authorship fixed in any tangible medium of expression."); § 101 (transmitted expressions are fixed if a fixation is made simultaneously with transmission). This may or may not apply if a temporary copy of a selection of the data is made in preparation for transmission, *compare* MAI Sys. Corp. v. Computer, Inc., 991 F.2d 511, 518 (9th Cir. 1993), *with* Cartoon Network LP, LLLP v. CSC

Similarly, dispatches from devices that solely contain the comprehensive readouts of the device's sensors are not likely to be protectable works, as no originality would be shown on the part of the programmer of the device to select particular elements.[32] The Copyright Office has previously indicated that it will refuse registration on an arrangement of data when such arrangement is "practically inevitable," "mechanical or routine," or "an exhaustive selection of information," as all of these would lack originality.[33] Courts may also use the "blank form doctrine" to decline to extend protection to a device output, if all the device programmer is contributing is the template to organize the data.[34]

By the same token, a collection of data sent as a batch report could be protectable, if it can be shown that it was assembled with a degree of originality in the selection and arrangement of the information.[35] Courts have held that information databases the employ creative choices in selection and arrangement are protectable, even if that arrangement is designed solely to present the most relevant or logical information to the user.[36] The question of whether data outputs are protectable under copyright law will therefore turn largely on the exact content of particular data outputs.[37]

Even though many outputs may not be protectable, the Copyright Office should use the potential existence of some protectable outputs to consider this exemption on the merits. In addition to providing support to this critical field of research, it avoids the paradoxical situation researchers would face if they were forced to only circumvent unprotectable data outputs. By the way this research is conducted, it is often not possible for a researcher to know whether a dispatch report contains protectable expression or not until after the researcher circumvents any TPM over that

---

Holdings, Inc., 536 F.3d 121, 127 (2d Cir. 2008), though the output may still be unprotectable for the reasons noted above.

[32] *See Matthew Bender*, 158 F.3d at 687.

[33] COMPENDIUM III, *supra* note 23, § 312.2; *see also* Assessment Techs. of Wisconsin, LLC v. WIREdata, Inc., 350 F.3d 640, 643 (7th Cir. 2003) (selecting a particular class of fields and categories in a database was protectable because "this structure is not so obvious or inevitable as to lack the minimal originality required"); Key Publ'ns, Inc. v. Chinatown Today Publ'g Enters., Inc., 945 F.2d 509, 513–14 (2d Cir. 1991) (finding protection when listing was not a "mechanical grouping of data," citing Copyright Office guidance).

[34] *See* Utopia Provider Sys., Inc. v. Pro-Med Clinical Sys., Inc., 596 F.3d 1313, 1323 (11th Cir. 2010); Kregos v. Associated Press, 937 F.2d 700, 708 (2d Cir. 1991).

[35] *Feist*, 499 U.S. at 358; COMPENDIUM III, *supra* note 23, §§ 312.2, 618.6, 727.2. These batch reports are distinct from the reports a physician may receive from the device companies, which aggregate device data with several other sources and format them into a stylized document. *See Mainspring Data Express*, MEDTRONIC, http://www.medtronic.com/for-healthcare-professionals/products-therapies/cardiac-rhythm/patient-management-carelink/mainspring-data-express/index.htm (last updated Sept. 22, 2010).

[36] CCC Info. Sys., Inc. v. Maclean Hunter Market Reports, Inc., 44 F.3d 61, 67 (2d Cir. 1994).

[37] For an example of an arranged output in the medical device context, *see* Halperin, *Security and Privacy*, *supra* note 4, at 33.

data.[38] To analogize to the paradigm case on copyright originality, a researcher will not know if they are looking at a copy of the white pages or a copy of the yellow pages until they open the phonebook.[39]

B. Technological Protection Measures Governing Access to Works

Although there is no single uniform standard, many medical device manufacturers use TPMs to control access to the code of a device or its outputs, and this use is almost certainly going to increase over the next three years due to new regulations from the FDA.[40] The measures currently used are wide-ranging, and include:

- *Access to data or source code information through a proprietary reader*. Most devices, including those by Biotronik and Boston Scientific, use a proprietary reader to access device information and the functional elements of the computer code.[41] Such proprietary readers are programmed to engage in a bidirectional "conversation" with implanted devices, whereby the reader will send a transmission "asking" for information and the device will "reply" with certain information.[42] At least one early case interpreting the DMCA allowed a back-and-forth transmission between programs to serve as a TPM, and found that another company's emulation of that "handshake" to access a protected transmission circumvented a technological protection measure.[43]
- *Access to data through password systems.* Some devices only allow access to data outputs through a password-authentication system, often operated in concert with a

[38] *See* Halperin, *Pacemakers*, *supra* note 28, at 134–35 (showing the process of intercepting, decoding, and reading data from a device).
[39] *Feist*, 499 U.S. at 361.
[40] *See* notes 53–60 *infra* and accompanying text.
[41] *See, e.g.*, BIOTRONIK, EHR DATASYNC FAQ 6 (2010), *available at* http://www.biotronik.com/files/DC516FE77528E5D7C12577F50034665E/$FILE/379082_faqs_EHR_overview_EN_03Dec2010.pdf; BOSTON SCIENTIFIC, ZOOM LATITUDE PROGRAMMING SYSTEM (2010), *available at* http://www.bostonscientific.com/content/dam/Manuals/us/current-rev-en/358471-001_S.pdf.
[42] Halperin, *Pacemakers*, *supra* note 28, at 133–35.
[43] RealNetworks, Inc. v. Streambox, Inc., No. 99-cv-2070, 2000 WL 127311, at **2, 4, 7 (W.D. Wash. 2000) (granting preliminary injunction over software the "mimics" a "secret handshake" technological measure); *see also* Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1191 (Fed. Cir. 2004) (both parties assumed a "rolling code" communication between two devices was a TPM). Many "secret handshake" protocols involve a degree of cryptographic protection and require the receiving device to solve an algorithmic problem with a randomly generated variable in order to verify its authenticity. *See* Ryan Iwahashi, *How to Circumvent Technological Protection Measures Without Violating the DMCA: An Examination of Technological Protection Measures Under Current Legal Standards*, 26 BERKELEY TECH. L. J. 491, 507 (2011). It is not clear whether the court in *Streambox* was faced with that sophisticated of a program, or whether it is needed to meet the definition of a TPM.

proprietary device reader.[44] Courts have split as to whether a password system imposes a TPM, but some have allowed a password to be sufficient.[45] As this is a nationwide rulemaking, the Copyright Office should therefore assume the presence of a TPM in these cases, and proceed to examine the exemption on its merits.[46]

- *Encryption on the outputs of devices or home monitoring systems.* Some systems, including the VITALIO pacemaker by Boston Scientific, encrypt the outputs of their devices.[47] Encryption is usually done by use of "key" that is kept private, which algorithmically alters the content of the transmission in a way that renders it indecipherable without use of a correspondent decryption key.[48] Courts have held that encrypting the transmission of the work imposes a TPM.[49]
- *Encryption on the computer code of devices.* While not yet widely employed, security researchers have recommended the adoption of encryption around access to the functional elements and computer code on devices.[50] This form of encryption works similarly to the encryption on data outputs, except that computer code encryption usually is done with a decryption key that is found or generated elsewhere on the

[44] *See, e.g.*, *Medtronic Paceart System: Technical Features*, MEDTRONIC, http://www.medtronic.com/for-healthcare-professionals/products-therapies/cardiac-rhythm/patient-management-carelink/medtronic-paceart-system/index.htm#tab3 (last visited Feb. 4, 2015); *Using Remote Patient Care Management*, ST. JUDE MEDICAL, http://health.sjm.com/heart-failure-answers/daily-life/everyday-concerns-with-an-implantable-device/using-remote-patient-care-management (last visited Feb. 4, 2015).
[45] *Compare* Pearl Investments, LLC v. Standard I/O, Inc., 257 F. Supp. 2d 326, 350 (D. Me. 2003) (circumvention of a password-protected VPN may be actionable), *with* I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532–33 (S.D.N.Y. 2004) (use of another's password does not circumvent a TPM). *See also* Iwahashi, *supra* note 43, at 510–12 (noting that password systems may or may not qualify as TPMs, depending on the test the court adopts and whether the password protects access to a particular file or an online service).
[46] *See* 2012 RECOMMENDATION, *supra* note 25, at 91–92 (noting that inconsistent authority on lawful uses "compels a finding" in favor of assuming a lawful use).
[47] *VITALIO Pacemaker*, BOSTON SCIENTIFIC, http://www.bostonscientific.com/en-EU/products/pacemakers/vitalio.html (last visited Jan. 27, 2015); Umashankar Lakshmanadoss et al., *Telemonitoring a Pacemaker*, *in* MODERN PACEMAKERS-PRESENT AND FUTURE 129, 131(Mithilesh R Das ed., 2011) (noting use of encryption when transmitting data from device to a company's data storage).
[48] ELDAD EILAM, REVERSING: THE SECRETS OF REVERSE ENGINEERING 6 (2005).
[49] Universal City Studios, Inc. v. Corley, 273 F.3d 429, 444 (2d Cir. 2001); Realnetworks, Inc. v. DVD Copy Control Ass'n, 641 F. Supp. 2d 913, 935 (N.D. Cal. 2009).
[50] *See, e.g.*, Chunxiao Li et al., *Hijacking an Insulin Pump: Security Attacks and Defenses for Diabetes Therapy Systems*, IEEE 13TH INT'L CONF. ON E-HEALTH NETWORKING 150, 154–55 (2011).

> device, because the code would need to be decrypted before it can be run.[51] Encrypting source code imposes a TPM.[52]

In addition to the TPMs that are already in place, the FDA is increasing pressure on medical device manufacturers to use TPMs in their devices for safety reasons.[53] In October 2014 the FDA issued new guidance for the management of cybersecurity in medical devices, which formally recommends that manufacturers "address cybersecurity during the design and development of [medical devices]."[54] The guidance specifically proposes limiting access to devices through passwords, code authentication, and encryption.[55] This follows earlier recommendations from the FDA that medical devices relying on wireless communication use encryption to control access to the device.[56]

It is highly likely that these recommendations will be adopted by the industry. The FDA requires manufacturers of medical devices to file either a premarket notification with the FDA when they plan to release a new device (often called a "510(k)" notification) or go through a full pre-market approval process if the device is especially risky or novel.[57] Whether a device goes through the notification process or the approval process, the device manufacturer is required to disclose the technological characteristics of the device to the FDA.[58] Guidance documents like these, while not legally binding,[59] are the usual means by which the FDA indicates its preferences when examining devices, and entities regulated by the FDA routinely treat these guidelines as rules in order to assure expediency in FDA approvals.[60]

---

[51] EILAM, *supra* note 48, at 330.
[52] § 1201(a)(3)(A); EyePartner, Inc. v. Kor Media Grp. LLC, No. 4:13-cv-10072, 2013 WL 3733434, at *4 (S.D. Fla. July 15, 2013).
[53] *Overview of Device Regulation*, FDA, http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ (last updated June 26, 2014).
[54] FDA, CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 4 (Oct. 2, 2014), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf [hereinafter FDA CYBERSECURITY GUIDANCE].
[55] *Id.* at 3–4.
[56] FDA, RADIO FREQUENCY WIRELESS TECHNOLOGY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 10–11 (Aug. 14, 2013), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf.
[57] *See Premarket Notification (510k)*, FDA, http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/HowtoMarketYourDevice/PremarketSubmissions/PremarketNotification510k/default.htm (last updated Aug. 19, 2014).
[58] *See* Content and Format of a 510(k) Summary, 21 C.F.R. § 807.92(a) (2014); Premarket Approval Application, 21 C.F.R. § 814.20(b) (2014); *see also* FRIES, *supra* note 8, at 73, 76 (noting devices that are "heavily software dependent" receive greater scrutiny).
[59] FDA CYBERSECURITY GUIDANCE, *supra* note 54, at 2.
[60] K.M. Lewis, *Informal Guidance and the FDA*, 66 FOOD & DRUG L.J. 507, 541–42 (2011). The FDA also recommends that device manufacturers consult this guidance when designing devices. *See* GAO REPORT, *supra* note 4, at 12.

C. Methods of Circumvention.

Accessing the computer code and outputs of medical devices usually requires a form of radio transmission interception, often combined with reverse engineering techniques. Medical devices communicate on a few specific radio frequencies, and to intercept the outputs of devices researchers monitor communications along those frequencies, and then work to decode those transmissions.[61] If the researcher wishes to access the code of the device, the researcher intercepts the transmitted binary object code of the program, and then uses educated guesses as to how the code was created and a mix of tools to test their assumptions, which if successful will reveal the underlying source code.[62] This often requires significant experimentation – done on devices not used in patient care[63] – with intercepting radio communications between the device and a reader and manipulating their contents to observe how it changes the other outputs of the device.[64]

When testing for defects and vulnerabilities, researchers may also use "fuzzing," a technique where a researcher will input malformed data into a device in order to find its defects.[65] Malformed inputs can expose errors, trigger vulnerabilities in software, or degrade the device's performance.[66] Observing how such malformed data affects a device will likely also require using some of the interception techniques noted above. For obvious reasons, this analysis is done with devices that are not being used for patient care.[67]

V. Asserted Noninfringing Uses.

As noted previously, members of this Coalition and others in their field use the computer programs and data outputs of medical devices to analyze their security and effectiveness, both as patients trying to detect issues with their devices, and as general researchers. An illustrative collection of papers and presentations to illustrate this type of security and effectiveness research

---

[61] Statement of Hugo Campos, Appendix C, ¶ 6; Halperin, *Pacemakers*, *supra* note 28, at 131–32; Li, *supra* note 50, at 152.

[62] *See* Halperin, *Pacemakers*, *supra* note 28, at 135–36; Johnson-Laird, *supra* note 50, at 858–59; JEROME RADCLIFFE, HACKING MEDICAL DEVICES FOR FUN AND INSULIN: BREAKING THE HUMAN SCADA SYSTEM 3–7 (2011). The act of reverse engineering computer is not, itself, a circumvention of a TPM. *See* Lexmark Int'l, Inc. v. Static Control Components, Inc. 387 F.3d 522, 548–49 (6th Cir. 2004) (accessing code that does not impose a TPM does not violate Section 1201); Dice Corp. v. Bold Techs., 913 F. Supp. 2d 389, 411 (E.D. Mich. 2012) (defendant did not violate DMCA because, in part, "Plaintiff does not encrypt its software").

[63] *See* Halperin, *Pacemakers*, *supra* note 28, at 130 (noting use of Medtronic Maximo pacemaker not used in a patient); Li, *supra* note 50, at 152 (noting use of an insulin pump not used in patient care).

[64] Wayne Burleson et al., *Design Challenges for Secure Implantable Medical Devices*, *in* IEEE DESIGN AUTOMATION CONFERENCE 12, 13 (2012); ANDREW HUANG, HACKING THE XBOX: AN INTRODUCTION TO REVERSE ENGINEERING 31 (2d ed. 2013).

[65] VUONTISJÄRVI & HYTÖNEN, *supra* note 12, at 5–6.

[66] *Id.*

[67] *See* note 63, *supra*.

has been included as Attachment B to this comment.

This analysis usually requires the researcher to access the outputs or source code of these devices, review the data they uncover, and then present their analysis of the device and its data. Depending on how they access, review, and present their discoveries, researchers may never implicate any of the enumerated rights of copyright. Reading the contents of a work and then writing a wholly original report does not implicate 17 U.S.C. § 106.[68]

To the extent that researchers do implicate these rights, it is usually in the context of short quotations from the code or data outputs of a device included in a final report analyzing the device, or through the creation of intermediate, in-house copies of the code or outputs while the researcher is in the process of analyzing the work. For reasons noted below, these are fair uses. Each is discussed in turn.

A. Quoting from Code or Outputs as Part of a Presentation or Report is a Fair Use

In some cases, researchers may quote from protectable portions of the computer code or data outputs of devices as part of the presentation of their research, often in a published periodical or presentation. Using short quotations from a work to analyze and criticize the work is as old as fair use itself.[69] The United States Court of Appeals for the Second Circuit has called it "a classic illustration of fair use."[70]

In a test very well known to this Office, courts deciding a question of fair use consider a list of four non-exclusive factors, along with other considerations at the court's discretion.[71] The Copyright Act instructs judges to consider (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit education purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.[72] To briefly follow the factors, the purpose here is clearly transformative;[73] when a researcher excerpts a portion of the code or data outputs in a research paper, they are taking expression that is meant to facilitate the function of a medical device and use it instead to explain how the device is performing, whether it has defects, and whether it

[68] *See* Severe Records, LLC v. Rich, 658 F.3d 571, 579 (6th Cir. 2011) (there is no "use" right in copyright); Venegas-Hernandez v. ACEMLA, 424 F.3d 50, 58–59 (1st Cir. 2005) (right to authorize use of a work is not protectable under copyright).
[69] Folsom v. Marsh, 9 F. Cas. 342, 348 (C.C.D. Mass. 1841) (citing Roworth v. Wilkes, 1 Camp. 94, 98 (K.B. 1807) (U.K.)).
[70] Wainwright Sec., Inc. v. Wall St. Transcript Corp., 558 F.2d 91, 94 (2d Cir. 1977).
[71] Beyond the statutory factors, judges also often consider the defendant's good faith, whether the defendant gave attribution to the original, and whether the plaintiff is misusing copyright to suppress unfavorable commentary. *See* WILLIAM PATRY, PATRY ON FAIR USE § 7:1 (2014).
[72] 17 U.S.C. § 107.
[73] That the use is transformative is especially relevant to the question of fair use, as transformative uses are considerably more likely to be found fair. *See* Neil Weinstock Netanel, *Making Sense of Fair Use*, 15 LEWIS & CLARK L. REV. 715, 734–44 (2011).

leaves open possibilities for intrusion. This undoubtedly adds to the original with a new meaning or message.[74] It is also often usually done for non-commercial, educational purposes, often at academic institutions, another consideration that favors fair use.[75]

The second and third factors similarly favor fair use. The software of medical devices is both published and highly utilitarian, both of which favor fair use.[76] It is also highly unlikely that scholarly article would ever take a qualitatively or quantitatively inappropriate portion from the original computer code, which can be tens of thousands of lines long, and without any identifiable "heart" of the work.[77] It is harder to categorically define the amount and substantiality of data taken from any given device's output, but examples from existing literature demonstrate that such taking is routinely appropriate given the nature of the use.[78]

Finally, in terms of the effect on the market, it is impossible to conceive of a circumstance where a quotation of the code or data output in a report would usurp the market for the pacemaker itself, or any correlated market.[79] Unlike nearly all other classes of works considered by the Copyright Office during this rulemaking, the physical copy of the work remains irreplaceable because of the personal nature of the information it gathers and, in many devices, the therapy it directly provides. No third-party publication of source code or data from a pacemaker replaces a patient's need for the pacemaker. To the extent that the research would diminish the demand for a particular device, it would only be due to the effectiveness of its criticism, which is not considered cognizable harm under the fourth factor.[80] Quite to the contrary, courts are more

[74] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569, 579 (1994).
[75] Maxtone-Graham v. Burtchaell, 803 F.2d 1253, 1262 (2d Cir. 1986).
[76] Sony Computer Entm't v. Connectix Corp., 203 F.3d 596, 603 (9th Cir. 2000) (operating software "lies at a distance from the core [of intended copyright protection] because it contains unprotected aspects that cannot be examined without copying"). The data outputs of devices are also highly utilitarian and factual, but are not likely to be considered published, as no public distribution would have occurred. This alone, however, is unlikely to impact fair use analysis for a work that is never planned for commercial dissemination. A.V. v. iParadigms, LLC, 562 F.3d 630, 641–42 (4th Cir. 2009); *see also* Pierre N. Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1118–19 (1990) ("The second factor should not turn solely, nor even primarily, on the published/unpublished dichotomy.").
[77] *Medical Device Software Validation*, MATHWORKS (http://www.mathworks.com/solutions/medical-devices/medical-software-validation.html (last viewed Feb. 4, 2015); *see* Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 565 (1985).
[78] *See* RADCLIFFE, *supra* note 62, at 5 (excerpting a very small string of object code); Halperin, *Security and Privacy*, *supra* note 4, at 33 (a small handful of lines from a device's data output to demonstrate a flaw in the data).
[79] Cariou v. Prince, 714 F.3d 694, 708–09 (2d Cir. 2013).
[80] New Era Publ'ns Int'l v. Carol Publ'g Grp., 904 F.2d 152, 160 (2d Cir. 1990); Wojnarowicz v. Am. Family Ass'n, 745 F. Supp. 130, 145–46 (S.D.N.Y. 1990); *see also* 2012 RECOMMENDATION, *supra* note 25, at 73 (harm to reputation is "not what the fourth fair use factor is intended to address").

likely to find fair use when circumstances suggest a copyright owner is using copyright to suppress criticism.[81]

As was said in the prior DMCA rulemaking, uses that excerpt segments of a work for criticism "fall within the favored purposes referenced in the preamble of Section 107 and, especially in light of the brevity of the excerpts used, are likely to be fair uses."[82]

B. Making In-House, Interim Copies When Developing a Report is a Fair Use

Many forms of research may require the researcher to make an interim copy of the work while in the process of analyzing the software or data, translating the object code of a program into source code, or writing up a report.[83] Such copies may also be used as a necessary step to extract the unprotectable data from a device report.[84]

Because courts consider any reproduction of a work to be potentially actionable, the legality of interim copies made in a researcher's workshop needs to be considered.[85] Few cases consider this question of in-house copies made in the process of noninfringing uses, and scholars express great skepticism toward pursuing infringement actions for those uses.[86] Outside of software, these in-house copies are regularly found to be fair when the user lawfully obtains the copy.[87] This specifically includes copying a work when done in the process of extracting underlying unprotectable data.[88] Cases concerning software have similarly held that making copies to access the unprotectable functional elements of software is a fair use.[89] Courts that have disagreed have

[81] *See* Ty, Inc. v. Publ'ns Int'l Ltd., 292 F.3d 512, 521 (7th Cir. 2002).
[82] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 77 Fed. Reg. 65,260, 65,268 (Oct. 26, 2012).
[83] *See, e.g.*, Li, *supra* note 50, at 152–53 (describing the process of intercepting the code by recording transmissions and then deciphering its contents).
[84] *See* Halperin, *Pacemakers*, *supra* note 28, at 131 (describing the process of extracting patient data from a device interrogation report).
[85] Walt Disney Prods. v. Filmation Assocs., 628 F. Supp. 871, 875–76 (C.D. Cal. 1986). Some incidental copies made during the research process may be too ephemeral to qualify for a *prima facie* case of infringement, but these are excluded from this analysis. *See* Cartoon Network LP, LLP v. CSC Holdings, Inc., 536 F.3d 121, 127–30 (2d Cir. 2008).
[86] *See* PATRY, *supra* note 71, § 3:50 ("Focusing on interim copying as the sole basis for infringement should be an embarrassment, the last refuge of those who do not have a legitimate claim.").
[87] Stone v. Perpetual Motion, LLC, 87 Fed. App'x 51, 52 n.1 (9th Cir. 2004); Duffy v. Penguin Books USA, Inc., 4 F. Supp. 2d 268, 274 (S.D.N.Y. 1998); *see also* Am. Geophysical Union v. Texaco Inc., 60 F.3d 913, 919 (2d Cir. 1994) (supposing in dicta that making a copy of a lawfully-obtained journal article to bring into a laboratory while working would be a fair use).
[88] Assessment Techs. of Wisconsin, LLC v. WIREdata, Inc., 350 F.3d 640, 645 (7th Cir. 2003).
[89] Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596, 608 (9th Cir. 2000); Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1522–23 (9th Cir. 1992); *see also* 2012 RECOMMENDATION, *supra* note 25, at 92 (noting Congress's endorsement of *Sega* and *Connectix* in defending interoperability within § 1201).

done so when the finished product infringed on the original or when other circumstances negated a finding of fair use.[90]

While the cases examining interim copies made in the process of reverse engineering software are most directly relevant to this inquiry, it is important to note that most of those cases concerned defendants who developed complementary or rival software.[91] Here, the use is even more transformative; as noted above, the users here are producing analysis into the safety and effectiveness of devices, both in general and personally. The works in question are highly utilitarian, and thus more likely to be fair uses under the second factor. At times whole copies of a work may be made, but courts acknowledge that even copying the whole of a work does not negate a finding of fair use, if it is necessary in light of the purpose.[92]

In terms of the fourth factor, and as noted above, it is profoundly unlikely that this copying will usurp the market for the original work. Interim copies made in the process of conducting research could not possibly supplant the need for an original device in a patient, and there is no licensing market to criticize a work.[93] Copies made to access underlying, unprotectable device data also do not supplant the need for the device in the first place, and do not supplant the need for the reports that medical device companies may generate with the same underlying data, which are combined with other information and presented in tandem with a consultation from a physician.[94] The uses of data advocated here instead concern time-sensitive access for safety and security reasons, including detecting anomalies and emergencies, or sharing time-sensitive medical information with family members as part of their care.[95]

Courts are empowered to consider other factors in a fair use determination, and in the particular case of accessing one's own data from a medical device, it is entirely possible that a court would take into account the highly personal and potentially lifesaving nature of the information in

[90] *See, e.g.*, Walt Disney Prods. v. Filmation Assocs., 628 F. Supp. 871, 876 (C.D. Cal. 1986) (allowing liability for near-complete work in circumstances where the final would likely infringe); Atari Games Corp. v. Nintendo of Am., Inc., No. 88-cv-4805, 1993 WL 214866, at *6–7 (N.D. Cal. April 15, 1993) (declining fair use when reverse engineering for future compatibility, and noting a bad faith tactic used to obtain the source code from the Copyright Office). Some courts have allowed claims to proceed when the parties enter into a contract that prohibits reverse engineering, *see* Bowers v. Baystate Techs., Inc., 320 F.3d 1317, 1325–26 (Fed. Cir. 2003), but here it does not appear that patients or researchers ever enter into such contracts. *See* Statement of Hugo Campos, Appendix C, ¶ 14.

[91] *Connectix*, 203 F.3d at 599; *Sega*, 977 F.2d at 1514–15.

[92] Sony Corp. of Am. v. Universal City Studios, 464 U.S. 417, 449–50 (1984); Authors Guild v. HathiTrust, 755 F.3d 87, 98–99 (2d Cir. 2014); Kelly v. Arriba Soft Corp., 336 F.3d 811, 816 (9th Cir. 2003); *Connectix*, 203 F.3d at 606.

[93] Mattel, Inc. v. Walking Mountain Prods., 353 F.3d 792, 806 (9th Cir. 2003).

[94] *See* MEDTRONIC, *supra* note 35 (describing the contents of a diagnostic report).

[95] Statement of Ben West, Appendix F, ¶ 5 (describing efforts to share insulin data with family members in order to afford a greater degree of personal freedom).

question.[96] The underlying data is indisputably fair to copy and use, and to the extent one must make a copy to reveal the underlying data, courts give that incidental copying latitude.[97]

C. The Statutory Exemptions in Section 1201 Do Not Apply

In the NPRM, the Copyright Office asked about the relevance of statutory exemptions 17 U.S.C. §§ 1201(f) and 1201(g), which grant exemptions for purposes of reverse engineering and encryption research.[98] A third section, § 1201(j), which concerns security testing, could also be considered as relevant to the proposed exemption. For reasons noted below, however, these exemptions either do not apply, or do not cover the full scope of research advocated here.

Section 1201(f) allows a person to circumvent a TPM when the person is "identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs."[99] It is therefore designed to apply when the researcher is developing interoperable software,[100] and not where, as here, researchers instead are reverse engineering to analyze existing software's vulnerabilities. There is no indication that Congress intended section 1201(f) to be the only permissible act of reverse engineering.[101] Indeed, Congress specifically desired that this rulemaking process respond to the changing circumstances of technology, a desire that would be frustrated if the Office were to treat the statutory exemptions as foreclosing an entire technique of discovery.[102]

Section 1201(g) also is inapposite due to its subject matter. The section allows for circumvention for "encryption research," which the statute defines as "activities necessary to identify and

---

[96] Time, Inc. v. Bernard Geis Assocs., 293 F. Supp. 130, 146 (noting the strong "public interest in having the fullest information available" as relevant to fair use inquiry); Whalen v. Roe, 429 U.S. 589, 605–06 (1977) (acknowledging a possible constitutional right to control over information, though not finding it in the case at bar). *See also* Statement of Hugo Campos, Appendix C, ¶ 14 ("When [implants] become an integral part of our organic body, they also become an intimate part of our identity."); Statement of Karen Sandler, Appendix E, ¶ 6 ("I believe patients should also have the fundamental right to assess the software in their own bodies . . . .").

[97] *Assessment Techs.*, 350 F.3d at 644–45; *see also* Golan v. Holder, 132 S. Ct. 873, 890 (2012).

[98] NPRM, *supra* note 1, at 73,871.

[99] 17 U.S.C. § 1201(f)(1).

[100] *See* H.R. REP. NO. 105-551(II), at 42 (1998) ("Section [1201(f)] is intended to promote reverse engineering by permitting the circumvention of access control technologies for the sole purpose of achieving software interoperability.")

[101] *See* 2012 RECOMMENDATION, *supra* note 25, at 71–72 (rejecting argument that 1201(f) clearly defines the contours of acceptable circumvention related to interoperability).

[102] H.R. REP. NO. 105-551(II), at 36 ("The Committee has chosen a regulatory, rather than a statutory, route for establishing this prohibition for only one reason: to provide greater flexibility in enforcement, through the rulemaking proceeding[.]"); *see also* 2012 RECOMMENDATION, *supra* note 25, at 72 n.358 (noting a lack of evidence that Congress intended 1201(f) to "occupy the field" with respect to reverse engineering).

analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works."[103] While some medical device research touches on this question, the overwhelming majority of research is more concerned with analyzing bugs and vulnerabilities with the software that powers the medical device itself, instead of the encryption on top of it.[104] Given this, reliance on Section 1201(g) would not be inappropriate in the vast majority of cases.

Section 1201(j) also does not cover all of the relevant activity here, though the exact scope of this section is unclear. This section allows for acts of "security testing" on a "computer, computer system, or computer network," provided that the testing does not violate other laws and is done with the authorization of the owner or operator of the device, and the tester is deemed legitimate in light of certain "qualifying factors," including whether the research promotes the security of the "owner or operator" of the object, and whether the researcher shared research with the manufacturer.[105]

Only two reported decisions discuss 1201(j), and neither gives any light to its scope.[106] This Office has considered the scope of section 1201(j) during two prior rulemakings. In her recommendation in 2006, the Register noted that it was unclear whether the section only exempted circumvention of a TPM controlling access to a "computer, computer system, or computer network," or of a copyrighted work on media accessed by a computer.[107] The Register allowed consideration of an exemption in light of this uncertainty.[108] In 2010, the Register noted that "Congress appeared to be addressing firewalls and antivirus software that were used on computers, computer systems, and networks" when they enacted section 1201(j).[109] The Register therefore was compelled to examine a proposed exemption on its merits when it concerned research outside of this scope.[110]

---

[103] 17 U.S.C. § 1201(g)(1)(A); *see also* S. REP. NO. 105-190, at 15-16 (1998) (illustrating "encryption research" as developing, testing, and decrypting cryptographic algorithms).
[104] *See generally* Jeremy A. Hansen & Nicole M. Hansen, *A Taxonomy of Vulnerabilities in Implantable Medical Devices*, SPIMACS 2010 PROCEEDINGS ON SECURITY & PRIVACY 13 (2010).
[105] 17 U.S.C. § 1201(j).
[106] *See* Univ. City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 321 (S.D.N.Y. 2000); Univ. City Studios, Inc. v. Reimerdes, 82 F. Supp. 2d 211, 219 (S.D.N.Y. 2000).
[107] U.S. COPYRIGHT OFFICE, RECOMMENDATION OF THE REGISTER OF COPYRIGHTS IN RM 2005-11; RULEMAKING ON EXEMPTIONS FROM PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES 57–59 (2006) [hereinafter 2006 RECOMMENDATION].
[108] *Id.* at 59.
[109] U.S. COPYRIGHT OFFICE, RECOMMENDATION OF THE REGISTER OF COPYRIGHTS IN RM 2008-8; RULEMAKING ON EXEMPTIONS FROM PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES 196–97 (2010) [hereinafter 2010 RECOMMENDATION] (citing H.R. REP. NO. 105-796, at 66-67 (1998); H.R. REP. NO. 105-551(II), at 44-45 (1998)).
[110] *Id.* at 200–201.

Similar concerns over the scope of section 1201(j) suggest that the Register should not rely on this section here. First, as was the case in the 2006 rulemaking, some of the uses proposed here are not seeking to access the computer code, but instead the data outputs of the devices, and to conduct research into device safety and effectiveness using that information specifically.[111] Second, the uses do not limit their scope of research to computer security in the sense that "firewalls and antivirus software" do.[112] Research in this field also addresses individual patient safety, as well as other design defects and unintended consequences of design choices. This may include the use of secure technology that nevertheless is hazardous to a patient.[113] More fundamentally, it is unclear whether Congress would have considered pacemakers, cardioverter defibrillators, insulin pumps, or other personal medical devices a "computer, computer system, or computer network" for purposes of section 1201(j).[114]

It is similarly unclear how strictly a court will interpret the "qualifying factors" listed in section 1201(j)(3)(A). Section 1201(j)(3)(A) asks courts to consider whether the research is done "solely to promote the security of the owner or operator" of the device.[115] At times medical device research is more macroscopic, highlighting defects in design and implementation that are common to all devices of that type, or even all devices in general.[116] The statute also asks courts to consider whether the researcher shared research with the developer of the device directly.[117] There are times where a researcher may better serve the interests of safety or security of devices by sharing information with persons other than the developer of the medical device. For example, the FDA runs a program called MedWatch that encourages all those affected by FDA-regulated products to report adverse impacts of these devices.[118] The Department of Homeland Security runs a similar reporting program.[119] Courts adopting a strict interpretation of the qualifying factors may not extend them to this conduct. The Register should instead examine this exemption on its merits.

---

[111] *See, e.g.* Statement of Hugo Campos, Appendix C, ¶ 8.
[112] *See* Section VI.C., *infra*.
[113] Halperin, *Security and Privacy*, *supra* note 4, at 35–36 (noting that resource-intensive security can drain a device's battery and jeopardize a patient).
[114] The legislative record on this question is contradictory. On the one hand, as the Register noted during the 2010 rulemaking, Congress seemed concerned about personal computers and webservers when developing the statutory exemptions discussed above, referencing firewalls, network management tools, and antivirus software as paradigm targets for analysis. 2010 RECOMMENDATION, *supra* note 109, at 196–98. At the same time, the Conference Committee indicated that the term "computer system" should share a definition with Computer Security Act, which extends to any machine that transmits or stores data. *See* H.R. CONF. REP. 105-796, at 66 (1998) (citing 15 U.S.C. § 278g-3(d)(1) (1997)). To further complicate matter, this definition was mentioned specifically in a discussion of the law enforcement exemption, and it is not clear whether this definition was meant to apply generally, or only to this section.
[115] 17 U.S.C. § 1201(j)(3)(A).
[116] *See, e.g.*, Hansen & Hansen, *supra* note 104.
[117] 17 U.S.C. § 1201(j)(3)(A).
[118] *MedWatch: the FDA Safety Information and Adverse Event Reporting Program*, FDA, http://www.fda.gov/Safety/MedWatch/ (last updated Jan. 27, 2015).
[119] GAO REPORT, *supra* note 4, at 11.

VI. Adverse Effects on Noninfringing Uses.

A. Research Into the Safety, Security, and Effectiveness of Devices is Vital

As noted in Section III above, medical device errors and vulnerabilities are a major concern, affecting the lives of millions of Americans.[120] Hundreds of deaths have been attributed to software failure in medical devices, resulting from errors including software lockups, premature shutdown, failure to restart, unexpected depletion in battery life, faulty detection of patient events, and miscalculated safety alarms.[121] As the software on devices becomes more complicated, the odds increase that errors will be present.[122] An internal report from the Food and Drug Administration ("FDA") concluded that between 2005 and 2009, 18% of recalls on all medical devices were related to a software problem.[123] The economic costs of such errors are enormous as well; a 2002 study by the National Institute of Standards & Technology estimated that inadequate software testing and resultant bugs cost the economy $59.5 billion per year.[124] This figure has no doubt increased since then.

President Obama has declared it the policy of the United States "to increase the volume, timeliness, and quality of cyber threat information," and has identified the Healthcare and Public Health sector as an industry of specific emphasis.[125] The FDA, in turn, has sought "broad input from the Healthcare and Public Health . . . Sector on medical device and healthcare cybersecurity."[126]

As was noted in a prior section 1201 rulemaking, independent researchers operating in good faith play a role in this "security ecosystem."[127] Independent research is critical to analyzing the design flaws and vulnerabilities of medical devices, and personal access to data outputs of devices ensures patients receive safe and effective treatment on a personal level. Examples of

---

[120] A 2001 report estimated that 25 million Americans had some form of implantable medical device INNOVATION AND INVENTION IN MEDICAL DEVICES: WORKSHOP SUMMARY 21 (Kaith e. Hanna et al. eds., National Academic Press 2001), http://www.nap.edu/openbook.php?record_id=10225&page=21.

[121] Alemzadeh, *supra* note 6, at 22; KAREN SANDLER ET AL., KILLED BY CODE: SOFTWARE TRANSPARENCY IN IMPLANTABLE MEDICAL DEVICES, SOFTWARE FREEDOM LAW CTR. 4 (2010), https://www.softwarefreedom.org/resources/2010/transparent-medical-devices.html.

[122] *See* FRIES, *supra* note 8, at 279 ("Software development is very labor intensive and is, therefore, prone to human error.").

[123] FDR CTR. FOR DEVICES AND RADIOLOGICAL HEALTH: 510(K) WORKING GROUP, PRELIMINARY REPORT AND RECOMMENDATIONS (2010), *available at* http://www.fda.gov/downloads/AboutFDA/CentersOffices/CDRH/CDRHReports/UCM220784.pdf

[124] NAT'L INST. OF STANDARDS & TECH., THE ECONOMIC IMPACTS OF INADEQUATE INFRASTRUCTURE FOR SOFTWARE TESTING at ES-11 (2002), *available at* http://www.nist.gov/director/planning/upload/report02-3.pdf.

[125] Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11,739, 11,739 (Feb. 12, 2013).

[126] Collaborative Approaches for Medical Device and Healthcare Cybersecurity; Public Workshop; Request for Comments, 79 Fed. Reg. 56,814, 58,814 (Sept. 23, 2014).

[127] 2010 RECOMMENDATION, *supra* note 109, at 202.

this are numerous, ranging from research exposing design flaws in pacemakers, demonstrating a particular risk with insulin pumps, and *ex post* analysis of critical failures to understand how these devices can be improved in the future.[128] Even basic software auditing could detect many of the failures that occur in medical devices today.[129] Agencies in the United States actively rely on this independent research when developing technology policy.[130]

At the individual level, physiological events that could be critical to a patient's well being may be missed if the device detects the event, but does not inform the patient. Changes to heart rhythm, blood flow, or chest impedance may not be physically experienced by the patient, or may only manifest in generalized symptoms such as faintness or dizziness.[131] Patients like Coalition member Hugo Campos have demonstrated how greater access to device data can lead to changes in lifestyle that improve overall health.[132] Signaling a growing trend toward personal access to medical information, the FDA has already approved a mobile device that will inform patients about incidents of atrial fibrillation through their smartphone.[133] In diabetes treatment the benefits of self-monitoring of blood sugar levels have been known for decades.[134]

In light of the risks of security vulnerabilities in networked medical devices, it is necessary that security researchers are free to perform various tests and experiments to determine the efficacy of these devices. As the FDA has noted, "medical device security is a shared responsibility between stakeholders."[135] Anticircumvention law should not exclude patients and independent investigators from conducting this research.

B. The Growing Proliferation of TPMs in Devices Presents a Substantial Risk to this Critical Form of Research

Prior to the adoption of the TPMs identified above, researchers were able to conduct this analysis without fear of anticircumvention liability. Medical devices, however, are increasingly employing TPMs as part of their design security, and the FDA's statements last October ensure

[128] See collected research in Appendix B.
[129] SANDLER, *supra* note 121, at 4.
[130] GAO REPORT, *supra* note 4, at 19 (in an investigation into FDA medical device cybersecurity practices, the GAO extensively cited independent research); *see* Statement of Jerome Radcliffe, Appendix D, ¶ 1 (after his presentation about insulin pumps, Mr. Radcliffe collaborated with the Department of Homeland Security and FDA on vulnerability research).
[131] Statement of Hugo Campos, Appendix C, ¶ 8; Singer, *supra* note 14.
[132] Statement of Hugo Campos, Appendix C, ¶¶ 8–10.
[133] Varun Saxena, *FDA Clears First Smartphone-Based Device to Detect Atrial Fibrillation*, FIERCE MED. DEVICES (Aug. 22, 2014), http://www.fiercemedicaldevices.com/story/fda-clears-alivecor-smartphone-plug-heart-monitor-detect-atrial-fibrillatio/2014-08-22.
[134] Jenna H. Frost, *Innovations in Participatory Medicine: the Advent of Do-It-Yourself Blood Glucose Monitoring*, J. PARTICIPATORY MED. (Sept. 14, 2010), http://www.jopm.org/columns/innovations/2010/09/14/innovations-in-participatory-medicine-the-advent-of-do-it-yourself-blood-glucose-monitoring/.
[135] FDA CYBERSECURITY GUIDANCE, *supra* note 54, at 3

this practice will grow over the following three years.[136] In general, this is a very good thing, as it improves device privacy and security.[137] The unintended consequence of this development, however, is that the research that has been conducted previously may become prohibited under section 1201. The TPMs do not solve all device safety problems, and defects and shortcomings in devices will be obscured instead of identified and remedied.[138]

The risk of the DMCA chilling this form of medical device research is present and substantial. At least one researcher has specifically reported that he is limiting his research in light of anti-circumvention concerns. Jerome Radcliffe, a member of this Coalition, studies vulnerabilities in insulin pumps. Given the presence of TPMs on some of these devices, he sought counsel to analyze whether his research would present a risk under the DMCA. Ultimately, he was forced to limit his inquiry to the portions of the device that were not protected by the TPM, thus substantially limiting the scope of his possible inquiry.[139] Beyond their formal liability, researchers like Mr. Radcliffe are understandably concerned about the possibility their research will lead to legal threats.[140] In another context, legal ambiguity and the lack of clear exemptions lead a major technology publisher to cancel release of a significant computer science book on hardware reverse engineering.[141]

Even worse, companies that do not wish to be identified with defective devices may attempt to use section 1201 to silence critical device research. There is great incentive for the medical device manufacturers to deter independent discovery of vulnerabilities, because there is such a profound economic disincentive for manufacturers to have these vulnerabilities come to light.[142] Device manufacturers have an obligation to investigate any report of a serious defect in a device,

---

[136] *See* discussion in Section IV.B., *supra*.
[137] *See, e.g.*, Statement of Karen Sandler, Appendix E, ¶ 6.
[138] Statement of Karen Sandler, Appendix E, ¶ 6 ("[A]dding such security measures will not guarantee that [devices] are safe from attack and certainly does not impact the likelihood of malfunction due to bugs in the software."); Burleson, *supra* note 64, at 15 ("Unfortunately, encryption is not a panacea for IMD security and privacy vulnerabilities; many questions remain[.]").
[139] Statement by Jerome Radcliffe, Appendix D, ¶¶ 3–4 (noting that he could not research a substantial part of the "risk area" due to section 1201 concerns, and that "[t]here are still large areas of technology that have not been researched, specifically because of the limitations of the DMCA").
[140] Thomas Fox-Brewster, *Pro Hackers Petition White House for DMCA and Computer Crimes Law Reform*, FORBES (Oct. 9, 2014), http://www.forbes.com/sites/thomasbrewster/2014/10/09/pro-hackers-want-the-us-goverment-to-fix-dmca-cfaa/ (quoting Mr. Radcliffe, "I want to make sure this stuff is safe . . . I don't want to get sued into oblivion." (abbreviation in original)).
[141] *See* HUANG, *supra* note 64, at 9 (noting that Huang's leading book on reverse engineering hardware was pulled by John Wiley & Sons following fears of liability under Section 1201).
[142] Kevin Fu, *NIST Explores Economic Incentives for Medical Device Cybersecurity*, ARCHIMEDES RESEARCH CTR. FOR MEDICAL DEVICE SECURITY (Feb. 2, 2012), http://blog.secure-medicine.org/2012/02/nist-explores-economic-incentives-for.html.

and then disclose the report and investigation to the FDA.[143] Discovered vulnerabilities can lead to recalls, suspension of FDA approval, seizure of devices, referrals for prosecution, and tort liability lawsuits.[144]

Despite mechanisms for mandatory reporting of incidents, there remains a tragic history of failures to disclose defects in devices. An early case of software failure in the 1980s took nearly a year to lead to FDA action, following numerous serious injuries and deaths from radiation overdose.[145] In 2005 an investigation into deaths related to defects in infusion pumps lead to a massive recall.[146] That same year, a company's design error in a defibrillator was shown to cause a death of a 21-year old patient, and subsequent investigation by the New York Times revealed the company was aware of the flaw for three years before telling doctors and patients.[147] To help prevent future incidents like these, medical device researches need an exemption to ensure their research will not stop simply because companies now encrypt their medical devices.

C. The Diversity of this Research Requires that the Copyright Office Not Distinguish Between Types Users and Accessing the Source Code or the Outputs of Devices

In the NPRM, the Copyright Office inquired specifically whether the exemption should distinguish between different types of uses under the greater umbrella of medical device security research, and whether third parties should be allowed to be involved in such research.[148] The Coalition urges the Copyright Office to consider the exemption broadly, and allow for the owners and operators of medical devices to solicit the help of others in conducting this research. As described above, understanding design security and effectiveness requires consideration of several different fields, including medicine, computer science, electrical engineering, systems design, and even patient behavior.[149] Because these systems are so complex, it is usually impossible to attribute a failure to a single cause in a single domain, and thus research is usually

---

[143] *See* 21 C.F.R. § 803.50 (2014).
[144] *See generally* DEP'T HEALTH & HUMAN SERVICES OFFICE OF THE INSPECTOR GENERAL, OEI-01-08-00110, ADVERSE EVENT REPORTING FOR MEDICAL DEVICES 7 (Oct. 2009) *available at* http://oig.hhs.gov/oei/reports/oei-01-08-00110.pdf; Robin Miller, *Products Liability: Cardiac Pacemakers*, 23 A.L.R.6th 223 (2007). Federal law preempts state tort liability that imposes different or greater obligations than federal law, but the legal risk remains substantial. *See* Riegel v. Medtronic, Inc., 552 U.S. 312, 330 (2008).
[145] Nancy G. Leveson & Clark S. Turner, *An Investigation of the Therac-25 Accidents*, 26 COMPUTER 18, 22 (1993).
[146] *See FDA Issues Statement on Baxter's Recall of Colleague Infusion Pumps,* FDA (May 3, 2010), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm210664.htm.
[147] Barry Meier, *Maker of Heart Device Kept Flaw from Doctors*, NEW YORK TIMES (May 24, 2005), http://www.nytimes.com/2005/05/24/business/24heart.html.
[148] NPRM, *supra* note 1, at 73,871.
[149] *See, e.g.*, Halperin, *Pacemakers*, supra note 28, at 129 (noting a mix of computer scientists and a Doctor of Medicine as participants in the research); Burleson, *supra* note 64, at 12 (noting the combined efforts of a computer scientist and electrical engineer in the research); Statement of Hugo Campos, Appendix C, ¶ 13 (noting his efforts to coordinate with other researchers in understanding the outputs of his own device).

conducted in teams.[150] This mirrors how the FDA approaches the pre-market approval process for devices, where they employ multidisciplinary teams for analysis.[151]

Because of this, while the researchers should be agents of the owner or operator of a device (either a patient or the owner of a unused device), an owner or operator should be able to coordinate with others when conducting this critical research.

D. The Proposed Exemption Would Not Negatively Impact the Security of these Devices

In the NPRM, the Copyright Office asked whether there would be negative repercussions in enabling this form of research, including by "making it easier for wrongdoers to access such medical devices' software or outputs."[152] To what extent there may be, they are slight and vastly superseded by the benefits such research provides to device security. To begin with, as a factual matter, many researchers take care not to explicitly provide fully detailed or enabled set of steps for reproducing the attack; instead, they provide the minimal evidence for a security expert to verify results.[153] Providing incomplete instructions on how to conduct an intrusion into a system is an effective way to balance the desire to deter bad actors with the numerous social benefits from explaining these intrusions, including greater public understanding of the nature of these threats and helping device manufacturers solve these problems.[154] It is noteworthy that nearly all publications reviewed in this comment that identify a problem also propose a corresponding solution.[155] It is also important to note that, to date, there is no recorded incident of a malicious attack on a medical device.[156]

More generally, the demonstrated history of cybersecurity research suggests that it helps good actors far more than it enables bad actors. The idea that insecure systems can overcome their shortcomings by keeping security-related details secret is sometimes called the "security through obscurity" theory. The concept has intuitive appeal, but professionals have rejected this as an

[150] Leveson & Turner, *supra* note 145, at 18 ("Most accidents are system accidents; that is, they stem from complex interactions between various components and activities. To attribute a single cause to an accident is usually a serious mistake."); *see also* Statement of Karen Sandler, Appendix E, ¶ 6 ("Were I able to review the source code on my own device, I could organize a team of colleagues who are programming experts to test for potential vulnerabilities and flaws.").
[151] *See* GAO REPORT, *supra* note 4, at 9.
[152] NPRM, *supra* note 1, at 73,871.
[153] Steven Hanna, *Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations in Medical Devices*, 2ND USENIX WORKSHOP ON HEALTH SECURITY & PRIVACY 2 (2011); Halperin, *Pacemakers*, *supra* note 28, at 130; Statement of Jerome Radcliffe, Appendix D, ¶ 1.
[154] *See generally* Eugene Volokh, *Crime-Facilitating Speech*, 57 STAN. L. REV. 1095, 1114–26 (2005).
[155] RADCLIFFE, *supra* note 62, at 7–9; Li, *supra* note 50, at 154–56; Halperin, *Pacemakers*, *supra* note 28, at 138–42.
[156] Halperin, *Pacemakers*, *supra* note 28, at 130.

effective element of security design since the late 1800s.[157] Quite the opposite, most of the critical agencies dedicated to safety and security actively solicit the input of the greater research community. The Department of Homeland Security, which is actively investigating incidents of medical device vulnerability, has a program whereby individuals who are aware of vulnerabilities can approach the agency, who will then coordinate a response with all relevant stakeholders.[158] The Department of Defense has rejected the theory of "security through obscurity" directly, and noted the benefits of free and open source software for detecting vulnerabilities.[159] The FDA has gone beyond the computer code access advocated here and openly experimented with developing free and open source software for infusion pumps, in part due to the added security open code provides.[160]

Given the consensus around these agencies, and the fact that researchers are demonstrably careful about the nature of their publications, the Copyright Office should not let the fear of assisting bad actors – who, to date, do not even exist – prevent this critical research.

VII. Statutory Factors.

To summarize, the statutory factors laid out in 17 U.S.C. § 1201(a)(1)(C) are reviewed in turn.

A. The Availability for Use of Copyrighted Works.

The statute instructs the Copyright Office to consider the "availability for use of copyrighted works," which the Office has interpreted to include "whether the availability of the work in a protected format enhances or inhibits public use of the work, whether the protected work is available in other formats, and, if so, whether such formats are sufficient to accommodate noninfringing uses."[161]

As was noted in the discussion of the market harm under fair use, the general public use of the works in question is solely as patients receiving therapy from devices. This use of the work does not turn on the presence or absence of TPMs; if a person needs an insulin pump, they get an insulin pump. There do not appear to be competing versions of devices with or without TPMs, and the device and the copyrighted work are inseparable. The circumstance for device researchers is quite different, and is discussed in the next section.

---

[157] Burleson, *supra* note 64, at 15 (describing the fallacy of security through obscurity, and noting its criticism security design since Auguste Kerckhoff's research in 1883).
[158] GAO REPORT, *supra* note 4, at 11; *see* Jim Finkle, *U.S. Government Probes Medical Devices for Possible Flaws*, REUTERS (Oct. 22, 2014), http://www.reuters.com/article/2014/ 10/22/us-cybersecurity-medicaldevices-insight-idUSKCN0IB0DQ20141022.
[159] *Frequently Asked Questions Regarding Open Source Software and the Department of Defense*, DEP'T OF DEFENSE, http://dodcio.defense.gov/OpenSourceSoftwareFAQ.aspx ("In general, 'Security by Obscurity' is widely denigrated."); SANDLER, *supra* note 121, at 5.
[160] *When Code can Kill or Cure*, THE ECONOMIST (June 2, 2012), http://www.economist.com/node/21556098
[161] 2012 RECOMMENDATION, *supra* note 25, at 97.

B. The Availability for Use of Works for Nonprofit, Archival, Preservation, and Education Purposes.

As the Copyright Office has noted, the second factor emphasizes the "special consideration" the exemption process gives "for certain identified socially productive uses."[162] Here, it is especially important to emphasize again that each device is distinct, and either does or does not include TPMs as part of its design. Each device also has the potential to present unique risks and security concerns. Failures are not isolated to a particular brand or particular software; deaths have been attributed to devices ranging from infusion pumps to monitors to radiology and imaging machines, and across various brands.[163] For devices that employ a TPM, there is no alternative for accessing the source code of the device.[164] The use of a work for the educational purpose advocated here is entirely unavailable for a device employing a TPM unless this exemption is granted.

Similarly, there are no alternatives for time-sensitive access to a patient's data for purposes of detecting device flaws or life-threatening events. As researcher Hugo Campos notes in his attached statement, in order to compensate for the fact that he is unable to get more immediate data from his medical device, he has had to obtain a number of various devices and keep a mobile-enabled database on his smartphone to track incidents by hand.[165] This is impractical in many cases, and does not fully replace having access to the device. As the Copyright Office has previously noted, requiring recreation of data through purchasing numerous other devices is not a reasonable alternative.[166]

C. The Impact on Criticism, Comment, News Reporting, Scholarship or Research.

As reviewed extensively above, the improvement of scholarship and research around the safety of medical devices, both in general and as applied to particular patients, is the essence of the exemption requested here. Granting Coalition members researchers like them permission to circumvent the access controls to medical device software and firmware will lead to advances in the medical research field. The public regulatory agencies depend upon this research as one of a series of critical stakeholders in the security ecosystem.[167] Granting this exemption will ensure that devices that employ TPMs are subject to the same critical scrutiny in the future.

---

[162] 2006 RECOMMENDATION, *supra* note 107, at 22.
[163] Alemzadeh, *supra* note 6, at 22 (noting seven different categories of devices where software deaths have been attributed); SANDLER, *supra* note 121, at 3 (noting five different brands of ICDs have been responsible for deaths).
[164] Statement of Karen Sandler, Appendix E, ¶ 2 (detailing how Ms. Sandler contacted all of the major manufacturers to review the source code around medical devices, but was unable to get a company to agree to turn over the source code for inspection); Statement of Ben West, Appendix F, ¶¶ 2–3 (same).
[165] Statement of Hugo Campos, Appendix C, ¶¶ 10–11; TEDX CAMBRIDGE, *supra* note 14.
[166] 2012 RECOMMENDATION, *supra* note 25, at 21.
[167] FDA CYBERSECURITY GUIDANCE, *supra* note 54, at 3.

D. The Effect on the Market for, or Value of, Copyrighted Works.

This critical research and analysis can only improve the market for these devices. As the Register noted in the 2006 rulemaking, "research into and correction of security flaws in access controls ultimately will have a positive impact on the market for or value of copyrighted works."[168] Conducting this research does not usurp the demand for the original devices, as no copy that is made in the process of developing this research could ever replace the need for a medical device.[169] As this research continued, the public will become more confident in the safety of these devices, and thus increase demand in the market, if they know that researchers are actively testing these medical appliances and showing ways that patients can leverage the data gathered on these devices to prevent adverse incidents and improve their health.

VIII. Conclusion.

For the enumerated reasons above, the Coalition respectfully requests that the Copyright Office recommend that the Librarian adopt Proposed Class 27 as part of this triennial rulemaking.

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[170]

Appendicies:
Appendix A – Medical Device Research Coalition members
Appendix B – Bibliography of Independent Research on Device Security
Appendix C – Statement of Hugo Campos
Appendix D – Statement of Jerome Radcliffe
Appendix E – Statement of Karen Sandler
Appendix F – Statement of Ben West

---

[168] 2006 RECOMMENDATION, *supra* note 107, at 64.
[169] *See* 2012 RECOMMENDATION, *supra* note 25, at 77 (favoring a finding of an exemption when "the evidence on the record demonstrates, at best, only a tenuous relationship between [the activity] and piracy").
[170] The Coalition wish to thank Cyberlaw Clinic students Sarah Baugh, Evita Grant, Megan Michaels, Joo-Young Rognile, and Shudan Shen for their invaluable contributions to this comment.

Appendix A

Medical Device Research Coalition Members

The Medical Device Research Coalition consists of the following members:

Hugo Campos
Oakland, CA
Hugo Campos is a person living with a cardiac implantable electronic device and a passionate advocate for the rights of patients to have full access and control over their health data.

Jay Radcliffe
Boise, ID
jay.radcliffe@gmail.com
Jay is a Cyber-Security expert that works for Rapid7. He has been a Type I diabetic since age 22. His goal in life is making the cyberworld a safer place for people.

Karen Sandler
Brooklyn, NY
karen@sfconservacy.org
Karen is the Executive Director of the Software Freedom Conservacy. She is also on the board of directors of the GNOME Foundation, pro bono counsel to the Free Software Foundation, the GNOME Foundation, and QuestionCopyright.org, and co-hose of the audcast *Free as in Freedom*.

Ben West
San Francisco, CA
bewest@gmail.com
Ben is an author of free and open source software. He has committed code to hundreds of software projects, many related to Type 1 diabetes, in an effort to restore fidelity to healthcare.

Appendix B

Bibliography Independent Research into Device Safety

The following is a select list of publications that have addressed the safety, security, and effectiveness of medical devices. This is not an exhaustive collection of publications on this subject.

1. Homa Alemzadeh et al., *Analysis of Safety-Critical Computer Failures in Medical Devices*, 11.4 IEEE SECURITY & PRIVACY 14 (2013) (reviewing recalls for computer-related failures in medical devices, outlining the causes of those failures, and discussing future challenges in device safety).

2. Haitham Al-Hassanieh, Encryption on the Air: Non-invasive Security for Implantable Medical Devices (2011), *available at* http://dspace.mit.edu/handle/ 1721.1/66020 (discussing how a lack of cryptographic mechanisms in devices can lead to privacy breaches and malicious intrusion, and proposing an external device that could assist in protecting already-implanted medical devices).

3. Wayne Burleson et al., Design Challenges for Secure Implantable Medical Devices, Proceedings of the 49th Annual Design Automation Conference (2012) (summarizing prior tests into computerized medical device security and safety, and reviewing possible solutions and trade-offs).

4. Paul Chan et al., *Automated External Defibrillators and Survival After In-Hospital Cardiac Arrest*, 304.19 JAMA 2129 (2010) (reviewing cases where a software-enabled defibrillator was used as part of hospital care, and finding that the use of the system was not associated with improved survival).

5. Shane Clark & Kevin Fu, *Recent Results in Computer Security for Medical Devices*, WIRELESS MOBILE COMM. AND HEALTHCARE 111 (2012) (reviewing examples where devices have been reverse engineered, and proposing ways to better simulate device implantation with *in vitro* testing).

6. Monika Darji & Bhushan Trivedi, *Detection of Active Attacks on Wireless IMDs Using Proxy Device and Localization Information,* SECURITY IN COMPUTING AND COMMS. 353 (2014) (proposing ways to use radio frequency-based localization to distinguish authorized from unauthorized signals to medical devices).

7. Tamara Denning et al., Absence Makes the Heart Grow Fonder: New Directions for Implantable Medical Device Security, Proceedings of USENIX Workshop on Hot Topics in Security (July 2008) (proposing "communication cloakers" around implantable medical devices" as a way of balancing security and accessibility).

8. Tamara Denning et al., Patients, Pacemakers, and Implantable Defibrillators: Human Values and Security for Wireless Implantable Medical Devices, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (2010) (analyzing many different approaches to device security, including implantable devices that change their security settings based on adverse events).

9. Tom Delbanco et al., *Inviting Patients to Read their Doctors' Notes: a Quasi-Experimental Study and a Look Ahead*, 157 ANNALS OF INTERNAL MEDICINE 461 (2012) (studying how enabling patients to access additional information about their care, in the form of doctors' notes, changed the doctor–patient relationship).

10. Esther Dyson, *Why Participatory Medicine?*, J. PARTICIPATORY MED. (2009) (discussing the research agenda for analysis into whether greater patient access to data improves patient care).

11. Kevin Fu & James Blum, *Inside Risks Controlling for Cybersecurity Risks of Medical Device Software*, 56.10 COMM. ACM 35 (Oct. 2013) *available at* http://www.csl.sri.com/users/neumann/cacm231.pdf (describing a series of specific events where software on medical devices lead to errors, and noting increasing pressure by FDA to adopt technological security measures).

12. Kevin Fu, *Trustworthy Medical Device Software*. PUBLIC HEALTH EFFECTIVENESS OF THE FDA 510(K) CLEARANCE PROCESS: MEASURING POSTMARKET PERFORMANCE AND OTHER SELECT TOPICS: WORKSHOP REPORT (2011) (reviewing software failures in medical devices, and specifically proposing greater public scrutiny as a policy proposal).

13. 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) (extensively reviewing a proposed "shield" system to block unwanted transmissions, including experimentation on multiple implantable medical devices and a device reader).

14. David Gurwitz & Jeantine Lunshof, *Personalized Participatory Medicine: Sharing Knowledge and Uncertainty*, 3.10 GENOME MED. 69 (2011) (addressing how greater information sharing with patients impacts patient decision-making as personalization of medical information increases).

15. J. Halamka et al., The Security Implications of VeriChip Cloning, 13.6 J. AM. MED. INFORMATICS ASS'N 601 (2006) (detailing an interception of outputs from a radio frequency medical identification chip, and its vulnerability to "spoofing").

16. Daniel Halperin et al., Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-power Defenses, Security and Privacy IEEE Symposium (2008) (a landmark study into the vulnerability of pacemakers and defibrillators, including a reverse engineering of a device, analysis of its outputs and inputs, a series of possible threats, and proposed solutions for those threats).

17. Daniel Halperin et al., *Security and Privacy for Implantable Medical Devices*, 7.1 IEEE PERVASIVE COMPUTING 30 (2008) (proposing a framework for evaluating threats to implantable medical devices, and describing the tradeoffs and considerations confronted when proposing solutions).

18. Steven Hanna et al., Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices, Proceedings of the 2nd USENIX Workshop on Health Security and Privacy (2011) (reverse engineering an automated defibrillator, noting several vulnerabilities, and proposing solutions).

19. Jeremy Hansen & Nicole Hansen, A Taxonomy of Vulnerabilities in Implantable Medical Devices, Proceedings of the Second Annual Workshop on Security and Privacy in Medical and Home-Care Systems (2010) (proposing a general framework for classifying various vulnerabilities in medical devices, and noting possible responses).

20. Xiali Hei et al., Defending Resource Depletion Attacks on Implantable Medical Devices, Global Telecommunications Conference (2010) (research focusing specifically on attacks that drain the battery life of devices, and proposing a response).

21. Kari Hytönen & Miia Vuontisjärvi, *Medical Devices in Modern Day World*, CODENOMICON (Dec. 2012) (reviewing software security challenges in medical devices, and discussing particular methods for testing the security of devices).

22. Daniel Kramer et al., *Security and Privacy Qualities of Medical Devices: An Analysis of FDA Postmarket Surveillance*, PLOS ONE 7.7: e40200 (2012), *available at* http://journals.plos.org/plosone/article?id=10.1371/journal. pone.0040200 (detailing oversight shortcomings in software-based medical devices, and proposing greater postmarket review of devices).

23. Izabella Lejbkowicz et al., *Internet Usage by Patients with Multiple Sclerosis: Implications to Participatory Medicine and Personalized Healthcare*, MULTIPLE SCLEROSIS INT'L (2010) (studying how increases in patient online research of a disease changed experience and outcomes with the disease).

24. Nancy G. Leveson & Clark S. Turner, *An Investigation of the Therac-25 Accidents*, 26 COMPUTER 18 (1993) (reviewing a particular device's failure due to a software error, and the subsequent delay in identifying and responding to the issue).

25. Chunxiao Li et al., Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System, 13th IEEE International Conference on E-Health Networking Applications and Services (2011) (demonstrating intrusions into a glucose monitoring and insulin delivery system, including a full reverse engineering of the radio protocol of the devices, and outlining possible defenses).

26. William Maisel, *Safety Issues Involving Medical Devices: Implications of Recent Implantable Cardioverter-Defibrillator Malfunctions*, 294.8 JAMA 955 (2005) (reviewing a particular event where a software failure in a device killed a patient, and highlighting ways in which the industry can help prevent future failures)

27. Nathanael Paul & Tadayoshi Kohno, Security Risks, Low-Tech User Interfaces, and Implantable Medical Devices: A Case Study with Insulin Pump Infusion Systems, Proceedings of the 3rd USENIX conference on Health Security and Privacy (2012) (detailing security risks with control interfaces on insulin pump systems).

28. Jerome Radcliffe, Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System, Black Hat Conference (2011), *available at* https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf (detailing a reverse engineering and analysis of an insulin system, noting vulnerabilities, and discussing factors that can limit intrusions).

29. Masoud Rostami et al., Balancing Security and Utility in Medical Devices?, Proceedings of the 50th Annual Design Automation Conference (2013) (reviewing existing proposals for adding security to implanted medical devices, and noting their strengths and shortcomings).

30. Dong Woo Ryu et al., *Generating Knowledge for the Identification of Device Failure Causes and the Prediction of the Times-to-Failure in u-Healthcare Environments*, 17.7 PERSONAL AND UBIQUITOUS COMPUTING 1383 (2013) (extensively analyzing several external medical devices that reported device failures to see what may have attributed to those failures).

31. Karen Sandler et al., Killed by Code: Software Transparency in Implantable Medical Devices, SOFTWARE FREEDOM LAW CENTER (2010) (reviewing numerous cases of software failure on medical devices, and noting system flaws, regulatory gaps, and a lack of transparency as contributing factors).

32. Krishna Venkatasubramanian et al., *PSKA: Usable and Secure Key Agreement Scheme for Body Area Networks*, 14.1 IEEE TRANSACTIONS INFO. TECH. BIOMEDICINE 60 (2010) (analyzing a particular form of cryptography for securing body area networks).

33. D. R. Wallace & D. R. Kuhn, *Failure Modes in Medical Device Software: An Analysis of 15 Years of Recall Data*, 8 INT'L J. RELIABILITY QUALITY & SAFETY ENGINEERING 351 (2001) (taxonomizing numerous ways devices can fail, based on data from prior device recalls).

34. Mark Weitzel et al., *Participatory Medicine: Leveraging Social Networks in Telehealth Solutions*, AMBIENT ASSISTIVE HEALTH & WELLNESS MGMT. 40 (2009) (discussing opportunities and affordances with sharing health data with patients and allowing patients to further share with family or friends).

35. Katherine Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA COMPUTER & HIGH TECH. L.J. 139 (2014) (a legal analysis of cyberattacks on devices and the liabilities that may follow).

36. Ziggy Yoediono & Ralph Snyderman, *Proposal for a New Health Record to Support Personalized, Predictive, Preventative, and Participatory Medicine*, 5.1 FUTURE MED. 47 (2008), *available at* http://www.futuremedicine.com/ doi/abs/10.2217/17410541.5.1.47 (proposing a more prospective form of health record which incorporates greater patient involvement with their own data).

Appendix C

Statement of Hugo Campos
ICD Patient

January 31, 2015

1. I am a cyborg of sorts. My every heartbeat is monitored by a built-in computer running proprietary software. But the data it records via sensors in my heart is beyond my reach. It is wirelessly transmitted to a bedside monitor and sent via telephone lines to a monitoring company, bypassing me altogether. I am a cardiac patient living with an implantable cardioverter-defibrillator (ICD).

2. In addition to being an ICD patient, I am a vocal advocate for the rights of patients with pacemakers and ICDs to gain electronic access to the data collected by their devices. I am an Emeritus Member of the Stanford Medicine X ePatient Advisory Board[1]; member of the Stakeholder Advisory Board (SAB), National Steering Committee for pSCANNER (Patient-Centered SCAlable National Network for Effectiveness Research)[2]; former advisory board member for the UC San Diego Calit2 Health Data Exploration Project: Personal Data for the Public Good; former member-at large for the Executive Committee of the Society for Participatory Medicine; and the founder of the ICD User Group, an online group of ICD patients with over 1,300 followers.

3. In 2011, I successfully completed a 2-week intensive course in cardiac rhythm management (CRM) at the Arrhythmia Technologies Institute, Greenville, SC. The course gave me an excellent understanding of the basic principles of cardiac device technology and the technical applications of cardiac pacing therapy. In the same year I shared my story at TedX Cambridge[3].

4. I have spoken on this topic to numerous U.S. and international publications, including NPR[4], the Wall Street Journal[5], the San Francisco Chronicle[6], the San Jose Mercury News[7], MIT Technology Review[8], Slate[9], O Estado de S. Paulo[10] and MedGadget Español[11].

---

[1] Stanford Medicine X | 2015, *2015 Stanford Medicine X ePatient Advisory Board*, http://medicinex.stanford.edu/2014-stanford-medicine-x-epatient-advisory-board (last visited Jan. 31, 2015).
[2] pSCANNER, *Stakeholder Boards*, http://pscanner.ucsd.edu/people/stakeholder-boards (last visited Jan. 31, 2015).
[3] TEDx Talks, *TEDxCambridge - Hugo Campos fights for the right to open his heart's data* (Jan. 20, 2011). http://tedxtalks.ted.com/video/TEDxCambridge-Hugo-Campos-fight
[4] Amy Standen, KQED, NPR, *Patients Crusade For Access To Their Medical Device Data* (May. 28, 2012). http://www npr.org/blogs/health/2012/05/28/153706099/patients-crusade-for-access-to-their-medical-device-data
[5] Amy Dockser Marcus and Christopher Weaver, The Wall Street Journal, *Heart Gadgets Test Privacy-Law Limits* (Nov. 28, 2012). http://www.wsj.com/articles/SB10001424052970203937004578078820874744076
[6] Victoria Colliver, SF Gate, *Patient's fear of being 'difficult' may hurt care* (May 7, 2012). http://www.sfgate.com/health/article/Patient-s-fear-of-being-difficult-may-hurt-care-3539612.php
[7] Lisa M. Krieger, San Jose Mercury News, *Man with defibrillator wants to know what his heart is saying*, (Jan. 29, 2012). http://www mercurynews.com/ci_19847981

5. My ICD was implanted in 2007 after I was diagnosed with a genetic heart condition that increases my risk for a sudden cardiac arrest. The device regulates the beating of my heart and delivers shocks to treat life-threatening ventricular arrhythmias[12]. ICDs are in a class of cardiac implantable electronic medical devices that also include pacemakers and implantable loop recorders. There are about 800,000 ICDs in the United States, with 10,000 new devices implanted every month[13].

6. The ICD is primarily designed to protect against deadly arrhythmias, but in the process of monitoring the heart it also collects great amounts of data about its own function and a patient's clinical status. Data about cardiac events is recorded in the ICD's memory and later transmitted to a base station at the medical implant-reserved frequency (402–405 MHz)[14]. The data is then sent via a standard telephone line to the device manufacturer for evaluation[15]. Finally, the manufacturer generates a report and makes it available to the clinic who may, for a fee, share it with the patient during a scheduled visit.

7. Remote patient monitoring has shown to be helpful to doctors by providing them with information needed for therapeutic interventions[16]. The data it collects, however, is unavailable to patients who are motivated to care for themselves and take responsibility for their health. Furthermore, locking patients out of access to potentially actionable information about their health illustrates an antiquated system where patients remain tethered to the clinic and the manufacturer of their implanted devices.

8. As helpful as it is to doctors, I believe access to information stored in the ICD is mostly beneficial to patients who live with the condition, not to doctors who care for them. The type of information collected by the ICD includes changes in the patient's cardiac status, programming settings and device integrity information. For example: (1) an abrupt

---

[8] Emily Singer, MIT Technology Review, *Getting Health Data from Inside Your Body* (Nov. 22, 2011). http://www.technologyreview.com/news/426171/getting-health-data-from-inside-your-body

[9] Torie Bosch, Slate, *Why Don't You Have the Right To Access Your Own Biometric Data?* (Feb. 27, 2012). http://www.slate.com/blogs/future_tense/2012/02/27/biometric_data_tedxcambridge_talk_by_hugo_campos_video_.html

[10] Agência Estado, O Estado de S. Paulo, *'E-Patients' se envolvem no próprio tratamento* (Jun. 6, 2011). http://veja.abril.com.br/agencias/ae/ciencia-saude/detail/2011-06-06-2014582.shtml

[11] Tilo Febres-Cordero, MedGadget Español, *Defensor del paciente en la búsqueda para obtener los datos de su desfibrilador implantable* (Feb. 1, 2012). http://medgadget.es/2012/02/defensor-del-paciente-en-la-busqueda-para-obtener-los-datos-de-su-desfibrilador-implantable.html

[12] National Institutes of Health, *What Is an Implantable Cardioverter Defibrillator*, http://www nhlbi nih.gov/health/health-topics/topics/icd (last visited Jan. 31, 2015).

[13] Medtronic Ask The ICD, *How many people have ICDs*, http://asktheicd.com/tile/106/english-implantable-cardioverter-defibrillator-icd/how-many-people-have-icds (last visited Jan. 31, 2015).

[14] *See, page 6*, Charles S. Farlow, *An Overview of the Medical Device Radiocommunications Service (MedRadio) and Future Telemetry Considerations* (Jun. 20, 2011). http://www.cwins.wpi.edu/workshop11/ppt/business_Charles.pdf

[15] Medtronic, *How the CareLink Network Works* (Mar. 26, 2014). http://www medtronic.com/patients/sudden-cardiac-arrest/living-with/carelink/how-it-works (last visited Jan. 31, 2015).

[16] Saxon LA, Boehmer JP, Neuman S, Mullin CM. *Remote Active Monitoring in Patients with Heart Failure (RAPID-RF): design and rationale*. J Card Fail. 2007;13:241–246. http://www.innovationsincrm.com/images/pdf/crm-05-03-1551.pdf

change in chest impedance could indicate excessive water retention and worsening of heart failure with increased mortality risk[17]; (2) an automatic switch in pacing mode may indicate the onset of atrial fibrillation, a common arrhythmia that increases a person's risk of having an ischemic stroke[18]; and (3) a sudden change in lead impedance may indicate a serious device malfunction that can lead to inappropriate shocks to the heart[19]. Patient access to this information would allow for early identification of adverse events and enable swift corrective action to be taken by the patient.

9. More importantly, understanding this data in the context of other patient-generated health data can lead to better adherence to medication and changes in lifestyle, improving the patient's health. In my experience, the tedious process of manually logging symptomatic cardiac episodes led me to identify the consumption of Scotch whisky as a trigger for atrial arrhythmias, and of caffeine as seemingly not harmful, in my particular case.

10. I achieved this by creating a mobile-enabled Google form that I used to capture on-the-go information about cardiac events. Once submitted, the form entered the data into a spreadsheet. In the event of a symptomatic arrhythmia, I would use the form to log my observations about the episode. The data I chose to collect included the presumed type of cardiac arrhythmia (atrial, ventricular, or unknown), its intensity, estimated duration in seconds, and my mood and activity at the time the episode occurred. Upon submission a time stamp was automatically added to each entry. At a later follow-up visit to the clinic, I would then obtain a copy of the data download from the ICD and attempt to reconcile the events recorded by the device with the ones logged by me.

11. This method was limited in part by my ability to record only the events that were symptomatic and that occurred during the course of the day when I was able to safely use my mobile phone. Cardiac events that occurred during sleep, and during activities such as driving went unrecorded. Another limitation was the synchronization of the ICD's internal clock with the actual time of the cardiac event. I found that the ICD's internal clock gradually veered off of the actual time. In addition, the ICD is not equipped with automatic conversion to Daylight Savings Time (DST)[20], and so the time-stamp differences were difficult to reconcile. Access to my device data would have allowed me to close the loop sooner and get valuable biofeedback within hours instead of months.

12. When the ICD is interrogated, a file containing patient session data is generated and may be saved to a diskette or USB flash drive[21]. With my brand of ICD, the data is stored in a

[17] Tang WH, Warman EN, Johnson JW, et al. *Threshold crossing of device-based intrathoracic impedance trends identifies relatively increased mortality risk.* Eur Heart J. 2012;33(17):2189-2196. http://www ncbi.nlm.nih.gov/pmc/articles/PMC3432233/pdf/ehs121.pdf

[18] Swerdlow CD, Schsls W, Eijkman B, et al. *Detection of Atrial Fibrillation and Flutter by a Dual-Chamber Implantable Cardioverter-Defibrillator. For the Worldwide Jewel AF Investigators.* Circulation 2000;101(8):878-885. http://circ.ahajournals.org/content/101/8/878 full.pdf

[19] Schoenfeld MH. *Contemporary pacemaker and defibrillator device therapy: challenges confronting the general cardiologist.* Circulation 2007; 115(5):638-653. http://circ.ahajournals.org/content/115/5/638 full.pdf

[20] Medtronic, *Medtronic CRDM Devices and Daylight Saving Time*, http://www.medtronic.com/crm/dst html (last visited Jan. 31, 2015).

[21] Medtronic. *Medtronic CareLink 2090 Programmer Reference Manual*. Minneapolis, MN U.S.A. (2014), p. 78, chapter 6.1,

proprietary file format known as PDD[22]. PDD is the extension for the manufacturer's data file, which can only be read by a custom desktop application or by the manufacturer's pacemaker Programmer, a computer running the operating system software Microsoft Windows XP[23]. The Programmer is a medical device not usually available to consumers. Each PDD contains the download of a patient's session information or all of the information from the patient's ICD[24], including device model, serial numbers, programming parameters, device settings, and arrhythmic episodes.

13. So far, I have been unable to obtain technical help in decoding PDD data files from my ICD. The likelihood that this would infringe on copyright law adds a hurdle to an already bewildering task and discourages trustworthy software experts from trying. Having the ability to legally circumvent the technological measures put in place by the manufacturer would allow me to find reputable help to liberate my cardiac data from its base station and decode my PDD files.

14. Implants are the most personal among personal chattel. When they become an integral part of our organic body, they also become an intimate part of our identity. To the best of my knowledge, I have never signed a document indicating that I am not the owner of the defibrillator embedded in my chest. It was implanted by a physician, billed by the hospital and paid for, on my behalf, by my health insurance provider.

15. Obtaining an anti-circumvention exemption would be a fundamental step toward allowing me to pursue expert technical help in obtaining access to data from my device. Implanted devices should answer first to us, then to our doctor, and finally, maybe, to a manufacturer. Right now that sequence is reversed.

---

http://manuals.medtronic.com/wcm/groups/mdtcom_sg/@emanuals/@era/@crdm/documents/documents/contrib_205974.pdf (last visited Jan. 31, 2015).

[22] Medtronic. *Virtuoso DR/VR D154AWG/D154VWC Implantable cardioverter defibrillator systems with OptiVol Fluid Monitoring, and Conexus Telemetry Reference Manual*. Minneapolis, MN U.S.A. (2013), p. 272, section 9.14.1.2, http://manuals.medtronic.com/wcm/groups/mdtcom_sg/@emanuals/@era/@crdm/documents/documents/contrib_172184.pdf (last visited Jan. 31, 2015).

[23] Medtronic. *Medtronic CareLink 2090 Programmer for Medtronic and Vitatron Devices, Programmer Reference Guide*. Minneapolis, MN U.S.A. (2011), p. 16, chapter 1, http://www.bewusstlosigkeit.de/wcm/groups/mdtcom_sg/@emanuals/@era/@crdm/documents/documents/contrib_086653.pdf (last visited Jan. 31, 2015).

[24] Medtronic. V*irtuoso DR/VR D154AWG/D154VWC Implantable cardioverter defibrillator systems with OptiVol Fluid Monitoring, and Conexus Telemetry Reference Manual*. Minneapolis, MN U.S.A. (2013), p. 271, section 9.14.1, http://manuals.medtronic.com/wcm/groups/mdtcom_sg/@emanuals/@era/@crdm/documents/documents/contrib_172184.pdf (last visited Jan. 31, 2015).

Appendix D

Statement of Jerome Radcliffe
Senior Security Consultant and Researcher, Rapid7

January 28, 2015

1. My name is Jerome Radcliffe and I currently work as a senior security consultant and researcher for Rapid7. I have been working in information and computer security for over 16 years. My interest in computers and technology goes back much further. I had a computer in my bedroom at the early age of 3 and went on to get my FCC Amateur Radio license when I was 12 years old. I have given presentations at numerous leading security, technology, and healthcare industry conferences, including Black Hat, DEF CON, B-Sides, MD&M, Design West. Most notably, I presented research on the wireless security for my personal insulin pump at Black Hat in 2011, which gained international attention and led to collaboration with the Department of Homeland Security and the Food and Drug Administration. The specific technical details of that research have never been published in order to protect patients using those devices.

2. Medical device research is something that I am very passionate about. This stems not only from my love of technology, but also from the effect on me as a patient. I was diagnosed with Type I diabetes on my 22nd birthday and that experience and perspective shapes my research. Depending on technology to maintain your health is a scary feeling. These life-giving technologies are immensely helpful in managing dangerous health conditions, but also have the ability to bring a different set of risks to the patient. I continue to research these devices so that they can be used safely while managing the risks associated with being connected to other computers and devices.

3. When I conducted my insulin pump research, my starting point was not the technology, it was a discussion with the Electronic Frontier Foundation (EFF). Having been in the security industry for a long time, I knew there were legal risks associated with research. I also studied law and have my undergraduate degree in Criminal Justice with a focus on Pre-Law. Most in the security industry do the research first and hope that they were on the right side of the law and don't get in trouble. I wanted to make sure that I was on solid legal ground before starting my research. I specifically asked the EFF to help me define what I could, and more importantly could NOT research. This distinction is not clearly defined. There is little-to-no case law to provide guidance on these issues. One area that was exceptionally risky under the DMCA was firmware-related research. This comprises a large area of research and risk for most technology. My rough guess is that for the insulin pump research I was looking at, the firmware area comprised about 40% of the potential risk area. I chose not to do any firmware related research because of the legal risk related to the DMCA. Even without looking at the firmware, I found substantial security risks in the insulin pump, allowing me to change all the setting on the insulin pump and even remotely turn it off. In the wild, this kind of attack would send a diabetic to hospital at a minimum and could result in death.

4. This insulin pump research has led to improvements in the technology, and increased awareness in the industry, but I feel that this is just the tip of the iceberg. There are still large areas of technology that have not been researched, specifically because of the limitations of the DMCA. In this way, the "bad guys" have an advantage from the security prospective. They do not have limitations to their areas of research and exploitation. In 1998 when the DMCA was enacted, the internet was in its infancy. We couldn't imagine that these networks and computers would be the foundation for something as large as the global financial system or control something as precious as a child's health and life. For these reasons, I think it is incredibly important for an exemption to be made in the DMCA for security research.

Appendix E

Statement of Karen Sandler
Free and Open Source Software Expert and Lawyer

February 4, 2015

1. I am a lawyer admitted to practice law in the State of New York and an expert in issues related to free and open source software (simply referred to herein as free software or software freedom). Prior to going to law school, I studied mechanical and electrical engineering, which involved programming primarily in FORTRAN and c. In the course of my legal practice, I was General Counsel of the Software Freedom Law Center and am now Executive Director of the Software Freedom Conservancy, both 501(c)(3) charitable nonprofits. I also have hypertrophic cardiomyopathy and have an implanted cardiac defibrillator (ICD) due to my high risk of sudden death.

2. Because of my expertise in free software, when prescribed my ICD I asked the major manufacturers to review the source code on the proposed devices but was unable to get any real response. I spoke to sales representatives of more than one company and called three of the manufacturers multiple times only to be given a run around in a phone tree. The one time I was able to get a person willing to speak to me, the representative told me that everything she could tell me was on the FDA's website. One manufacturer gave me a number for an "engineering team" but no one ever returned my voice mails.

3. Due to the nature of my need and the relatively high likelihood of sudden death, I opted to get a device and conduct research on the FDA mechanisms for the review of software as well as surveying security research around software freedom and software safety, summarizing the results for publication.[1] This paper demonstrated a few simple propositions: that all software is extremely likely to have flaws ("bugs"), that security experts agree that free software is generally safer over time, that in the field of medical devices free software that can be audited and reviewed will have fewer bugs and vulnerabilities and that when there are bugs in free software they can be fixed more readily.

4. Not only does my life rely on the proper functioning of the software but there are a number of ways in which malfunction would be more than inconvenient. An unnecessary shock, improper pacing, or software settings that run down the battery (thus requiring the whole device to be replaced by surgery) are all scary outcomes. Knowing that software in my own body surely has some flaws and not being able to take a look at it is extremely frustrating, to say the least. On top of that, if there is a problem with the software, I have to wait for the manufacturer to first admit that there is a problem and then to fix it on their own. If a problem that impacts me is not important enough for the company to

[1] Karen Sandler, Lysandra Ohrstrom, Laura Moy, Robert McVay "Killed by Code: Software Transparency in Implantable Medical Devices"
https://www.softwarefreedom.org/resources/2010/transparent-medical-devices.html

spend resources on I have no ability to work with my medical professionals to find a solution that works with the device I have already had implanted.

5. ICDs broadcast wirelessly so that medical practitioners can deliver treatment quickly in the case of emergency. The side effect of this is that anyone can attempt to interact with these devices. Currently ICDs have no encryption preventing access by anyone who is sophisticated enough to do so. Multiple researchers have demonstrated their ability to access ICDs and cause unwanted (and even fatal) shocks, pace inappropriately and run down the devices batteries.[2] The way ICDs are used now, there is no way for patients to look at the source code on their devices to test them for safety purposes (or to fix a bug in the event that an agent of the manufacturer is unavailable or unwilling to) and yet any determined and savvy malicious actor could take control of the ICDs remotely. On an extremely personal note, as a woman in my 30s it is somewhat likely that my needs are different than the majority of people who get ICDs. For example, my device has been recalibrated on multiple occasions, one of which was after my device inappropriately shocked me twice while I was pregnant.

6. These devices would be less vulnerable with some encryption or other mechanism to prevent unwanted access by attackers but adding such security measures will not guarantee that they are safe from attack and certainly does not impact the likelihood of malfunction due to bugs in the software. The need to allow medical professionals and software experts[3] to assess the safety and stability of these devices remains. Were I able to review the source code on my own device, I could organize a team of colleagues who are programming experts to test for potential vulnerabilities and flaws. Most importantly, I would at least have the tools necessary to deal with any problems down the road, rather than hoping that the manufacturer stays in business and continues to find financial incentive to prioritize my needs.

[2] Daniel Halperin, Thomas S. Heydt-Benjamin, Benjamin Ransford et al "Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses" 2008 IEEE Symposium on Security and Privacy and "Pacemaker hack can deliver deadly 830-volt jolt: Pacemakers and implantable cardioverter-defibrillators could be manipulated for an anonymous assassination" article by Jeremy Kirk in ComputerWorld, Oct 17, 2012.

[3] I believe patients should also have the fundamental right to assess the software in their own bodies, or work with experts of their choice in doing so. Indeed, experts who are patients may even want to consider having another expert review the safety and efficacy of their device.

Appendix F

Statement of Ben West
Independent Researcher

February 5, 2015

1. I am software engineer who writes network based applications and libraries to inspect and develop technology to help people. I also suffer from type 1 diabetes. In 2009 I discovered the devices I use had potential to audit and better understand my own therapy through the use of vendor-specific networking protocols.

2. As I began to investigate the USB and wireless protocols, I discovered that the insulin pump and continuous glucose monitoring devices offered features that could be used to better control my therapy. After contacting the vendors to confirm the presence of system design flaws but having my request to documentation of the network protocols denied, I realized that FDA reviews the documentation I wanted as part of their review, and began contacting them in 2012.

3. The FDA explained that while my data technically belonged to me, that the documentation explaining the protocols to test and audit the safety of my life-critical device were confidential, protected by the vendor's copyright assertion that the method used to audit my therapy was their sole intellecutal property. In repeated attempts to contact insulin pump and continuous glucose monitoring vendors, use of copyright to obscure these protocols and the behavior, safety, and efficacy of these devices from public review.

4. Despite the obscurity of the protocols, independent researchers such as myself through methodical, manual analysis were able to reverse engineer how these protocols work. Using open source tools, we were able to develop some investigatory tools using a mixture of open source software that allowed us to communicate with insulin pumps and continuous glucose meters.

5. Due to our unique relationship and dependence on these devices to survive, we used this knowledge to then build tools to better understand how therapy works. A popular application called Nightscout/cgm- in-the-cloud[1] was created, the ability for people to independently review and understand their therapy has anecdotally increased freedom – allowing first sleepovers, first trips too public school, first walks with grandparents – as well as increasing fidelity, allowing people predict and obtain measurably better therapeutic results.

[1] http://www.wsj.com/articles/citizen-hackers-concoct-upgrades-for-medical-devices-1411762843#livefyre-comment

6. With hypoglycemia – a side-effect of therapy – becoming more common,[2] it is critical for the public to review every detail. In Nightscout's case, we were able to overcome system design limitations to achieve better therapy and avoid common injuries.

[2] http://newoldage.blogs.nytimes.com/2014/06/19/hypoglycemia-rising-in-older-people-with-diabetes/?_r=0