CYBERLAW CLINIC
Harvard Law School | Berkman Center for Internet & Society

BEFORE THE UNITED STATES COPYRIGHT OFFICE
LIBRARY OF CONGRESS

PETITION OF A COALITION OF MEDICAL DEVICE RESEARCHERS FOR EXEMPTION TO PROHIBITION ON CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS FOR ACCESS CONTROL TECHNOLOGIES

Docket No. 2014-07

Submitted by:
Andrew F. Sellars
Cyberlaw Clinic
Berkman Center for Internet & Society
Harvard Law School
23 Everett Street, Second Floor
Cambridge, MA 02138
asellars@cyber.law.harvard.edu

A coalition of medical device patients and researchers (the "Medical Device Research Coalition")[1] submits this petition in response to the Notice of Inquiry on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 79 Fed. Reg. 55,687 (Sept. 17, 2014).

Brief Overview of the Exemption

The members of the Medical Device Research Coalition study the safety, security, and effectiveness of networked medical devices that are either implanted or attached to the body. This Coalition includes researchers who study device security at the design level, as well as those who study the safety and effectiveness of devices they personally use. Such research often requires the researcher to access the underlying source code and outputs from these devices, and device manufacturers are increasingly employing technologies that courts may classify as technological protection measures under § 1201 of the Copyright Act. In order to make sure that this form of critical research continues, the Medical Device Research Coalition proposes the following 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

[1] This coalition includes Hugo Campos, Stanford Medicine X; Jerome Radcliffe, Rapid7; Karen Sandler, Software Freedom Conservancy; and Benjamin West, an independent device researcher. The institutional affiliations provided here are for identification purposes only.

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.

Works Sought to Be Accessed in Medical Device Security Research

This exemption seeks to allow researchers to access literary works, in particular, the software and firmware of medical devices and their corresponding monitoring systems, as well the outputs generated by such devices and monitoring systems,[2] when such devices are capable of transmitting or receiving information and are designed to be attached to or implanted in patients. Examples of such devices include pacemakers, implantable cardioverter defibrillators ("ICDs"), insulin pumps, and continuous glucose monitors ("CGMs").

Technological Protection Measures Governing Access to Medical Devices

Many medical device manufacturers use measures to control access that a court may conclude are technological protection measures for purposes of § 1201. The measures identified are wide-ranging, and include, *inter alia*, encryption on the outputs on medical devices or home monitoring systems,[3] password systems that control access to patient management software and devices,[4] and proprietary software and tools for extracting device information.[5]

There is strong reason to believe that adoption of such technologies will increase over the coming three years. The Food and Drug Administration ("FDA") published new guidelines last month for premarket submission of medical devices, which asks medical device manufacturers to implement and identify their technological security measures. [6] Such guidelines, while not

[2] Many outputs on medical devices are not protectable as copyrighted works, and circumvention of protection measures over such data outputs would not implicate anti-circumvention law. *See* 17 U.S.C. § 1201(a)(1)(A) (protecting only a "work protected under this title"). This petition therefore seeks an exemption to circumvent the outputs of devices to the extent that a court ever would find the readouts of such devices to be embodied in a protectable expression.

[3] *See, e.g.*, *VITALIO Pacemaker*, BOSTON SCIENTIFIC, http://www.bostonscientific.com/en-EU/products/pacemakers/vitalio.html (last visited Nov. 2, 2014); *BIOTRONIK: Home Monitoring Service Center*, BIOTRONIK, http://www.biotronik.com/wps/wcm/connect/en_us_web/biotronik/sub_top/patients/dianostics_and_therapies/home_montitoring (last visited Nov. 2, 2014).

[4] *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 Nov. 2, 2014).

[5] *See, e.g.*, BIOTRONIK, BIOTRONIK EHR DATASYNC FAQ 6 (2010), *available at* http://www.biotronik.com/files/DC516FE77528E5D7C12577F50034665E/$FILE/379082_faqs_EHR_overview_EN_03Dec2010.pdf.

[6] U.S. FOOD AND DRUG ADMINISTRATION, CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 3 (Oct. 2, 2014), *available at* http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocu

binding on medical device manufacturers, are highly likely to influence the development of these devices in the immediate future.

Access of Medical Device Source Code and Outputs for General and Patient-Specific Research Does Not Infringe Copyright

Members of the Medical Device Research Coalition and others in their fields use the computer programs and data outputs of medical devices to analyze the security and effectiveness of medical devices, both as patients analyzing devices they use for therapy and treatment and as general researchers.[7] The use of these works for purposes of researching and critiquing the safety and effectiveness of the devices that use them is clearly a lawful use, either as a fair use or as a use that only copies unprotectable elements from the underlying works.

Accessing the source code and outputs of medical devices usually entails a form of reverse engineering, where a researcher intercepts the internally or externally transmitted binary object code of the program, and then uses a mix of techniques to reveal the underlying source code or data.[8] The act of reverse engineering might include the creation of incidental copies of the underlying work, but some techniques do not copy the underlying software or outputs at all.

If a researcher only copies the data points from these devices, the user does not implicate the copyright owner's exclusive rights whatsoever.[9] Even if a researcher were to copy the full reports of data from a device, such reports may not have the necessary creativity in selection or arrangement of information to be protectable under the Copyright Act.[10] If a researcher does in fact copy protectable expression, it is usually only an interim copy made to access and examine the functional elements of the code for testing and analysis. Courts have held such interim copies to be a fair use.[11] A federal appellate court has also held the copying of a protectable database in order to extract the underlying unprotected data to be a fair use.[12]

ments/UCM356190.pdf ("Manufacturers should develop a set of cybersecurity controls to assure medical device cybersecurity and maintain medical device functionality and safety.").

[7] Examples of this sort of research and analysis include Wayne Burleson et al., *Design Challenges for Secure Implantable Medical Devices,* 49TH DESIGN AUTOMATION CONFERENCE 12, (June 2012); Hugo Campos, *Hugo Campos Fights for the Right to Open His Heart's Data*, TEDXCAMBRIDGE (Jan 20, 2012), http://tedxtalks.ted.com/video/TEDxCambridge-Hugo-Campos-fight.

[8] ELDAD EILAM, REVERSING: SECRETS OF REVERSE ENGINEERING 109-38 (2005). The term "reverse engineering" is meant in the more general way it is used in the computer science community, instead of the specific interoperability context used in the statute. *See* § 1201(f). For a specific application of these techniques in an implantable medical device context, see Daniel Halperin et al., *Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses*, IEEE SYMPOSIUM ON SECURITY & PRIVACY 129, 133–35 (2008).

[9] *See, e.g.*, N.Y. Mercantile Exch., Inc. v. IntercontinentalExchange, Inc., 497 F.3d 109, 113-16 (2d Cir. 2007).

[10] *See id*.

[11] *See, e.g.*, Sony Comp. Ent. v. Connectix Corp., 203 F.3d 596, 599 (9th Cir. 2000); Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1526 (9th Cir. 1992).

[12] Assessment Techs. of WI, LLC v. WIREdata, LLC, 350 F.3d 640, 644-45 (7th Cir. 2003).

The case for fair use is even stronger given that the uses here are so highly transformative.[13] The purpose of a medical device company's source code is to enable the function of a medical device; researchers like the members of this Coalition use the code in order to publish criticism on how safe, secure, and effective these products actually are. The use therefore resembles that of a book critic quoting excerpts of a book in her critique, a paradigm case of fair use.[14] The proposed uses also would never supplant the market for the original work. Only the original work (as embodied in a medical device) will administer therapy to a patient. To the extent research and criticism diminishes the market for the original work, it is only due to the effectiveness of such criticism, which is rightly excluded from a fair use analysis.[15]

Allowing Anti-Circumvention Claims in this Area would Adversely Affect Critical Medical Research

Developing safe, secure, and effective medical devices is a national priority. 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.[16] The FDA, in turn, has sought "broad input from the Healthcare and Public Health . . . Sector on medical device and healthcare cybersecurity."[17]

While the injuries resulting from device flaws to date have been due to design and programming errors rather than malicious attacks, medical device security is a pressing concern. According to recent reports, the Department of Homeland Security is currently conducting confidential investigations into some two dozen cases of cyber-security flaws in medical devices.[18] Hundreds of recalls of software-based medical devices have been issued previously, affecting over a million devices. More than 11% of all medical device recalls between 1999 and 2005 were attributed to software failures.[19]

Medical device companies actively research these vulnerabilities, but it is often independent researchers, and not the manufacturers, that discover flaws, identify solutions, and inform the

[13] *See generally* Neil Weinstock Netanel, *Making Sense of Fair Use*, 15 LEWIS & CLARK L. REV. 715, 734-44 (2011) (noting that findings of "transformativeness," while neither necessary nor dispositive, drive judicial analysis of fair use today).

[14] Wainwright Securities, Inc. v. Wall St. Transcript Copr.,558 F.2d 91, 94 (2d Cir. 1977).

[15] *See, e.g.*, New Era Publ'ns Int'l v. Carol Publ'g Grp., 904 F.2d 152, 160 (2d Cir. 1990).

[16] *See* Exec. Order 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013); WHITE HOUSE OFFICE OF THE PRESS SEC'Y, PRESIDENTIAL POLICY DIRECTIVE 21 – CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

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

[18] Jim Finkle, *U.S. Government Probes Medical Devices for Possible Cyber Flaws*, RECODE (Oct. 22, 2014), http://recode.net/2014/10/22/u-s-government-probes-medical-devices-for-possible-cyber-flaws/.

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

government and public about safety hazards in devices. For example, a group of university researchers in 2008 demonstrated for the first time that radio signals could be used to intercept communications from an ICD and reprogram the device, potentially with lethal effects.[20] Similar independent research showed potentially lethal vulnerabilities in insulin pumps.[21] These and other studies were cited in the Government Accountability Office's subsequent report to Congress on medical device security, which encouraged the FDA to expand its consideration of information security in its approval process.[22] On the individual monitoring level, a growing number of patients and medical professionals are demonstrating how patients can improve the effectiveness of their treatment outcomes by actively monitoring their own information.[23]

Such research is rarely if ever done with manufacturer consent or authorization, no doubt in part due to the fact that discovery of flaws could lead to costly recalls, FDA investigations, and class action lawsuits.[24] Indeed, some companies have been shown to actively hide known vulnerabilities from patients and doctors.[25] Allowing independent research into this space is essential for public health and safety, and should be allowed to extend to those devices that employ technological measures to obfuscate their code or data outputs.

Conclusion

For the above reasons, the Medical Device Research Coalition requests that the Copyright Office include the exemption described above as part of its notice of proposed rulemaking.

Respectfully submitted,

Andrew F. Sellars
Cyberlaw Clinic

On behalf of Hugo Campos, Jerome Radcliffe, Karen Sandler, and Benjamin West[26]

[20] *See* Halperin, *supra* note 8.

[21] Jordan Robertson, *The Trials of a Diabetic Hacker*, BUSINESSWEEK.COM (Feb. 23, 2012), http://www.businessweek.com/articles/2012-02-23/the-trials-of-a-diabetic-hacker.

[22] U.S. GOV'T ACCOUNTABILITY OFFICE, MEDICAL DEVICES: FDA SHOULD EXPAND ITS CONSIDERATION OF INFORMATION SECURITY FOR CERTAIN TYPES OF DEVICES (Aug. 2012), *available at* http://www.gao.gov/assets/650/647767.pdf.

[23] *See* Campos, *supra* note 7.

[24] For example, a 2005 investigation into device errors on infusion pumps made by Baxter Healthcare Corp. lead to massive recalls and fees for the company. *See FDA Issues Statement on Baxter's Recall of Colleague Infusion Pumps,* U.S. FOOD AND DRUG ADMINISTRATION (May 3, 2010), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm210664.htm.

[25] For tragic examples of this, see 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.

[26] The Coalition with to thank Cyberlaw Clinic students Evita Grant and Megan Michaels for their invaluable contributions to this petition.