Before the
Copyright Office
Library of Congress
Washington, D.C. 20024

In the Matter of	Docket No. 2014-07
Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies	Proposed Class 25: Software – Security Research Proposed Class 27: Software – Networked Medical Devices

New America's Open Technology Institute ("OTI") respectfully files these third-round comments in response to the Notice of Proposed Rulemaking published in the above-referenced proceeding on December 12, 2014, and in response to other comments published in response to that notice.[1] OTI urges the Copyright Office and Library of Congress to disregard arguments, made by opponents of proposed Classes 25 and 27, that exemptions for software and/or medical device security research would create or exacerbate consumer privacy risks.

The Advanced Medical Technology Association and Medical Imaging and Technology Alliance argue, "where unauthorized circumvention activity is utilized to access the corresponding monitoring system of an implanted or attached device, or networked patient imaging and health record systems, the privacy and personal health information of other patients may be compromised."[2] LifeScience Alley

[1] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, *Notice of Proposed Rulemaking*, 79 Fed. Reg 73,856 (Dec. 12, 2014), *available at* http://copyright.gov/fedreg/2014/79fr73856.pdf [hereinafter 2013 NPRM].

[2] Class 25 Comments of Advanced Medical Technology Association and Medical Imaging and Technology Alliance at 3, *available at* http://copyright.gov/1201/

argues that if circumvention of TPMs in medical devices is allowed, "patient data may be compromised. The privacy and personal health information that could potentially be mined by these channels could be used for ill will."[3] The Medical Device Innovation, Safety and Security Consortium asks whether "all 'researchers' [will] have the necessary domain expertise to responsibly and safely hack a patient's device and associated data."[4]

But opposition commenters fail to recognize that to the extent there are existing vulnerabilities in software that expose personal information, malicious attackers may already be exploiting those vulnerabilities to gain access to the information, and may continue to do so as long as such vulnerabilities go undiscovered and unaddressed by those with the power to issue patches. Indeed, at a time when every month seems to surface another high-profile data breach, it is clear that those who would misuse personal information can and will find vulnerabilities to exploit. It is in the best interest of the public to dismantle roadblocks, including the § 1201 prohibition on circumvention, that chill important

---

2015/comments032715/class%2025/AdvaMed_Class25_1201_2014.pdf; *see* Class 27 Comments of Advanced Medical Technology Association and Medical Imaging and Technology Alliance at 7, *available at* http://copyright.gov/1201/2015/comments-032715/class%2027/AdvaMed_Class27_1201_2014.pdf ("In certain instances, networked devices could be used to access information which third parties should not be able to access and/or monitor.").

[3] Class 25 Comments of LifeScience Alley at 4, *available at* http://copyright.gov/1201/2015/comments-032715/class%2025/LifeScience_Alley_Class25_1201_2014.pdf; Class 27 Comments of LifeScience Alley at 4, *available at* http://copyright.gov/1201/2015/comments-032715/class%2027/LifeScience_Alley_Class27_1201_2014.pdf.

[4] Class 25 Comments of Medical Device Innovation, Safety and Security Consortium at 1, *available at* http://copyright.gov/1201/2015/comments-032715/class%2025/Medical_Device_Innovation_Safety_and_Security_Consortium_Class25_1201_2014.pdf.

security research to discover vulnerabilities that expose consumers' personal information to unauthorized access.

I. Vulnerabilities that Threaten Consumer Privacy Are Plentiful, and Malicious Attackers Will Exploit Them

Vulnerabilities that leave consumers' personal information exposed are plentiful. As commenter Mark Stanislav of Rapid7 explains,

> Many of the technologies that consumers buy have no real assurances that they adequately protect our privacy as the device's box may claim. . . . . In my own research with . . . web cameras and Internet-connected children's toys—I have seen real horrifying examples of a gratuitous lack of security.[5]

When it comes to medical devices, Suzanne Schwartz, director of emergency preparedness/operations and medical countermeasures at the FDA's Center for Devices and Radiological Health, says, "there is no such thing as a threat-proof medical device."[6]

Moreover, malicious attackers are clearly motivated to access personal information without authorization. As broader sets of personal information are stored by more parties for ever-expanding purposes, breaches of that information are on a clear upward trend. Each year sees more reported data breaches than the last.[7]

---

[5] Class 25 Comments of Mark Stanislav at 1, *available at* http://copyright.gov/1201/2015/comments-020615/InitialComments_ShortForm_Stanislav_Class25.pdf.
[6] U.S. Food & Drug Admin., *FDA News Release: The FDA Takes Steps to Strengthen Cybersecurity of Medical Devices* (Oct. 1, 2014), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm416809.htm
[7] Identity Theft Resource Center, *ITRC Breach Statistics 2005–2014* (2015), http://www.idtheftcenter.org/images/breach/MultiYearStatistics.pdf.

This is particularly the case with respect to medical information. From 2009 to 2014, the number of reported breaches in the health/medical industry sector nearly quintupled.[8] For the past three years, that sector has experienced more data breaches than any other sector.[9] Daniel Nutkis, the chief executive of the Health Information Trust Alliance, told the *New York Times* in February that "the industry has become, over the last three years, a much bigger target."[10]

Health sector software is thus at high risk for breaches. As explained last October in *Fortune*, "With the increasing digitization of health information (in the form of electronic health records) and the formation of health exchanges (due to the Affordable Care Act), the trend in medical identity theft is unlikely to abate any time soon."[11]

Attackers also target medical devices to gain access to the rich stores of health information that devices hold. The *Wall Street Journal* reported last year, "Health-care organizations increasingly are having trouble protecting data because medical equipment, such as dialysis and imaging machines, can be serviced through the Internet. That often is so the machines' software can be administered or updated remotely."[12] According to that article, the SANS Institute, a cybersecurity research and educational organization, "found evidence of hacked dialysis and MRI machines and compromised personal health information." Well-

---

[8] There were 70 reported breaches in the health/medical sector in 2009 and 333 in 2014, a ratio of 1:4.8. *Id.*

[9] *See id.*

[10] Reed Abelson & Julie Creswell, *Data Breach at Anthem May Forecast a Trend*, N.Y. Times (Feb. 6, 2015), http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html.

[11] Laura Shin, *What's Behind the Dramatic Rise in Medical Identity Theft?*, Fortune (Oct. 19, 2014), https://fortune.com/2014/10/19/medical-identity-theft/; *accord* Abelson & Creswell, *supra* note 10 ("Moving medical records from paper to electronic form . . . has also made patient records susceptible to breaches, whether unintentionally or through a criminal attack.").

[12] Rachael King, *Nursing Homes Exposed To Attacks By Hackers*, Wall St. J. (Feb. 18, 2014), B1.

known medical device security expert Kevin Fu explained in 2009 that an independently built medical device programmer that exploits security vulnerabilities in passersby's personal medical devices "could be easily miniaturized to the size of an iPhone and carried through a crowded mall or subway."[13]

Vulnerabilities in software and medical devices that expose consumers' personal information are real, unavoidable, and are being exploited today.

II. These Vulnerabilities Must Be Detected As Soon As Possible

It is critically important to identify and address vulnerabilities as soon as possible—ideally before breaches even take place—not only so that consumers' personal information is less likely to be compromised, but also because breaches are notoriously difficult to detect after the fact. Neal O'Farrell, the founder of security firm Privide, notes that even relatively sophisticated large firms are often unaware they have suffered a breach until they begin to see compromised data appear on the black market.[14] According to O'Farrell, unless companies identify threats in the first instance, it is very difficult to find out about them because "hackers don't leave traces."[15] Isolated breaches of individual records, such as breaches of individual medical devices, could be particularly difficult to detect.

Security researchers can help ensure that vulnerabilities are identified in a timely manner. Research that reveals vulnerabilities before personal information is breached would inform both companies interested in taking steps to remedy vulnerabilities, and regulators tasked with enforcing data security standards.

---

[13] Charles Graeber, *Profile of Kevin Fu, 33, TR35 2009 Innovator*, Tech. Rev., http://www.technologyreview.com/TR35/Profile.aspx?trid=760 (last visited May 1, 2015).
[14] Megon Leonhardt, *Cybersecurity Breaches Not Rare, Just Undetected*, WealthManagement.com (Sept. 11, 2014), http://wealthmanagement.com/technology/cybersecurity-breaches-not-rare-just-undetected.
[15] *Id.*

III. It Is Not the Role of the Digital Millennium Copyright Act nor the Copyright Office To Protect Against Malicious Attackers

Recognizing that the threat of data breach is prominent and real, the DMCA was not intended to address issues of consumer privacy and data security. There are other laws and offices of government much better suited to that purpose, and the fact that this proceeding has veered into such areas that Congress never intended is as good a proof as any that the DCMA's anti-circumvention provisions are having a worrisomely overbroad impact far beyond the scope of copyright law. This office can and should help address that overbreadth through the approval of sensible exemptions such as those being sought for software and medical device security research.

Respectfully submitted,

/s/

Laura Moy
New America's Open Technology Institute
1899 L St, NW Suite 400
Washington, DC 20036
(202) 596-3346

Filed: May 1, 2015