Note: Please submit a separate comment for each proposed class.

This is a Word document that allows users to type into the spaces below. The comment should be no more than 25 pages in length (which may be single-spaced but should be in at least 12-point type), not including any documentary evidence attached to the comment. The italicized instructions on this template may be deleted.

Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201

[ ] Check here if multimedia evidence is being provided in connection with this comment

Please note that such evidence must be separately submitted on a disc or flash drive. See the Notice of Proposed Rulemaking for detailed instructions.

Item 1. Commenter Information

Identify the commenting party and, if desired, provide a means for others to contact the commenter or an authorized representative of the commenter by email and/or telephone. (Please keep in mind that any private, confidential, or personally identifiable information in this document will be accessible to the public.)

LifeScience Alley is the largest trade organization of its kind based in Minnesota, representing the medical device, biotechnology, pharmaceutical, digital health and diagnostic industries. LifeScience Alley is a global leader in enabling life science business success with a 30-year track record of delivering results-oriented outcomes. We are committed to leading the conversation in improving our community's operating environment and supporting advancement in research and healthcare innovation. By influencing proactive policy change, leading solutions-based initiatives, delivering vital information and intelligence, and uniting members with critical resources, LifeScience Alley works to ensure that collectively we remain the world's strongest life science community. The Association's membership and supporting community extends throughout the world, employing more than 300,000 Minnesotans and many more globally. Founded in 1984, LifeScience Alley has played a leadership role in growing Minnesota's Medical Alley for 30 years.

Shaye Mandle, CEO & President
LifeScience Alley
1550 Utica Ave South, Suite 725
St. Louis Park, MN 55416
smandle@lifesciencealley.org
www.lifesciencealley.org

Item 2. Proposed Class Addressed

Identify the proposed exemption that your comment addresses by the number and name of the class set forth in the Notice of Proposed Rulemaking (e.g., "Proposed Class 7: Audiovisual works – derivative uses – noncommercial remix videos").

These comments concern Proposed Class 25: Software—Security Research

Item 3. Overview

Provide a brief summary of the circumvention activity sought to be exempted or opposed and why.

For the reasons stated below, we respectfully request that the Copyright Office oppose the inclusion of medical devices in an exemption under Proposed Class 25.

I. The Food and Drug Administration (FDA) is the correct administrative body to monitor medical devices

a. Implantable medical devices are highly regulated by the FDA

The FDA has been responsible for regulating medical devices since 1976. Medical devices go through years of scrutiny by the FDA before approval.[1] The FDA monitors reports of adverse events and other problems with medical devices and alerts health professionals and the public when needed to ensure proper use of devices and the health and safety of patients.[2] This level of scrutiny includes every aspect of the device, including any software package embedded in the device.

The FDA has recently published draft guidance on the Management of Cybersecurity in Medical Devices. [3] The guidance has been developed to assist the industry by identifying issues related to cybersecurity that manufacturers should consider in the design and development of their medical devices. [4] The FDA recognizes that medical device security is a shared responsibility between stakeholders, including health care facilities, patients, providers, and manufacturers of medical devices. The first recommendation in this document is to limit access to the devices to trusted users only by limiting access to devices through the authentication of users. Additionally, the guidance has a list of recommendations for detection, response, and recovery in the detection of a cybersecurity event.

This FDA recommendation is in direct opposition to the proposal before the Copyright Office. Allowing unauthorized users to have access to networked medical devices goes against guidance set forth by the agency responsible for their regulation.

Additionally, any changes, however insignificant, made to a post market approved device must go through additional screening by the FDA. This includes any changes to software, which if this proposal were to pass could lead to changes in operation and effectiveness of the device. In addition, this could affect labeling, warranty, directions, etc. Any changes to a medical device, however insignificant, must go through the agency's scrutiny.

---

[1] http://www.fda.gov/MedicalDevices/
[2] Medical Device Safety: http://www.fda.gov/MedicalDevices/Safety/default.htm
[3] Content of Premarket Submissions for Management of Cybersecurity in Medical Devices. http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf
[4] Id.

Currently, the Department of Homeland Security is investigating two dozen cases of suspected cybersecurity breaches involving medical devices.[5] The agency's ICS-CERT or Industrial Control Systems Cyber Emergency Response Team has purview over this inquiry. This is being done in concert with the FDA. The objective of this inquiry is to "catalyze collaboration among all stakeholders within the healthcare and public health community in order to address current cybersecurity gaps and challenges."[6]

Additionally, the Energy and Commerce Committee Subcommittee on Oversight and Investigations is holding a series of hearings on cybersecurity and the broader implications for businesses and consumers. [7] This inquiry is in direct response to that committee's 21st Century Cures initiative which is looking to overhaul the drug and device approval apparatus to better align with fast moving health research and innovation.[8]

Lastly, the University of Minnesota's Technological Leadership Institute in partnership with the National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) are currently conducting a use-case on Securing Networked Medical Devices.[9] This project is being conducted in collaboration with many of our member companies. NIST & NCCoE are helping to develop industry guidelines for medical device security. This use-case will be presented in coordination with its formal release by NIST/NCCoE for public comment.

Since the FDA is the federal agency charged with the safety, efficacy, and security of medical devices, they are the logical government agency to have purview over medical device safety, efficacy, and security. The FDA is already involved in many projects with other federal agencies to address concerns of potential cyber vulnerabilities in medical devices. There are already avenues of collaborations for other agencies and academic institutions to have access to networked medical devices and their operating systems and communication hardware for study. Additionally, the FDA routinely monitors the efficacy of medical devices in premarket and post market studies. Allowing the "fixing" of medical devices would circumvent this process.

The Copyright office is not the forum in which to address these possible issues. We respectfully request that the Copyright Office oppose the creation of an exemption for Proposed Class 25 and defer to the FDA for the framework to further research on the safety, efficacy, and security of medical devices.

II. Unauthorized Circumvention Activity for Security Research should not be permitted for any medical device

[5] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01
[6] Collaborative Approaches for Medical Device and Healthcare Cybersecurity (Oct., 2014) http://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM419427.pdf
[7] House Energy & Commerce Committee http://energycommerce.house.gov/press-release/committee-kicked-thoughtful-review-cybersecurity
[8] House Energy & Commerce; 21st Century Cures Mission Statement: http://energycommerce.house.gov/cures
[9] University of MN Technological Leadership Institute: http://tli.umn.edu/index.php?id=1057

The current request is broadly written, capturing medical devices in this call to identify, disclose, and fix malfunctions along with other technologies such as cars, electronics, etc.

Medical devices are highly regulated technologies that go through many years of design, research, development, and clinical trials under the purview of the Federal Drug Administration (FDA). Any circumvention activities would be outside of the manufacturer's design, potentially voiding any warranty associated with the device. Additionally, this type of circumvention could expose the manufacturer to unforeseeable liability. This type of unauthorized activity may significantly change the device's operation, resulting in injury or death.

a. Risk to Patient Safety

Medical devices include but are not limited to: pacemakers, implantable defibrillators, insulin pumps, glucose monitors, neurostimulators, deep brain stimulators, ambulatory monitoring, etc. These are highly complicated and technical implants that are necessary and critical to the lives of these patients. Anyone having access to reprogram these implantable devices could compromise the health of these patients.

In addition, if this type of unauthorized activity 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.

Exposing these patients to possible vulnerabilities in their devices will inevitably lead to patient death. Devices are used for the clinical care of patients and any unauthorized circumvention activity would lead to unnecessary risks and a breach in patient safety and privacy. Any compromise of the proper operation of the software on a medical device could easily lead to patient death.

b. Battery Life Affected

Attempts to access this data will drain the finite battery charge of an implantable medical device. The research and development that has gone into the development of these devices is extensive, down to the expected battery life. If these programmers are allowed to mine data over and over again, thereby draining the battery life, more frequent surgical replacements will be necessary to service the devices. This will add to the cost of healthcare, with no apparent positive value to the healthcare system nor to the patient that has to undergo unnecessary surgery to replace the battery.

c. Warranties Null and Void

If these proposed changes pass, programmers will be allowed to “fix” these medical devices, which would nullify the current warranties. Warranties on devices are tied to the lifetime of the device. This type of undetectable activity is currently not sanctioned, unless a research institution formally asks to collaborate with the manufacturer. Allowing this type of circumvention will create a loss of warranty exposure and may result in an increase in the cost of the device.

Item 4. Technological Protection Measure(s) and Method(s) of Circumvention

Describe the TPM(s) that control access to the work and the relevant method(s) of circumvention. The description should provide sufficient information to allow the Office to understand the nature of the relevant technologies, as well as how they are disabled or bypassed.

a. Definition of a Medical Device

A medical device is "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory which is:

- recognized in the official National Formulary, or the United States Pharmacopoeia, or any supplement to them,
- intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
- intended to affect the structure or any function of the body of man or other animals, and which does not achieve any of its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of any of its primary intended purposes."[10]

b. Trade Secrets

The source codes used in current medical devices are considered trade secrets. The current recommendation would remove restrictions on that source code. If this information is published this could lead to products being replicated in other markets that have lax regulatory bodies. Software and data streams are passed in formats that are secret and known only to the manufacturer. Allowing for trade secrets to flow uncontrolled would severely devalue the innovation in these devices.

c. Doctor-Patient Relationship; Access to Data

The doctor-patient relationship is evolving as technology and innovation evolves. The doctor is responsible for prescribing the medical device to individuals and monitoring and maximizing its effectiveness. There are a small number of direct to consumer devices (e.g., insulin pumps). The doctor is an essential participant in the interpretation of the information produced by the medical device. Currently, a patient has access to

[10] Definition of a Medical Device in statute, FDA: http://www.fda.gov/aboutfda/transparency/basics/ucm211822.htm

their data through their physician. Allowing this exemption will directly interfere with the doctor-patient relationship – in effect inducing patients to make decisions without the support of their doctor.

d. Patient Potentially Unaware of the Data Mining

The way the exemption is currently written is so broad that patients may not even be consulted when data is being mined from their device. The exemption states that the circumvention could be done 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." That secondary clause should be very concerning to patient advocates seeking access to their personal data. This could create another unforeseeable layer of risk for the patients, those conducting research, and the manufacturers of medical devices.

Item 5. Asserted Noninfringing Use(s)

Explain the asserted noninfringing use(s) of copyrighted works said to be facilitated by the proposed exemption, including all legal (statutory or doctrinal) bases for the claim that the uses are or are likely noninfringing. Commenters should provide an evidentiary basis to support their contentions, including discussion or refutation of specific examples of such uses and, if available, documentary and/or separately submitted multimedia evidence.

As noted above in section I. a. (University of MN Project), there are already other avenues in which an institution/entity can do research in this area of networked medical devices. Formal relationships between the manufacturer and research institution currently exist. All major companies in the medical device community are participating with the guidance of the FDA to do research in this area.

Item 6. Asserted Adverse Effects

Explain whether the inability to circumvent the TPM(s) at issue has or is likely to have adverse effects on the asserted noninfringing use(s), including any relevant legal (statutory or doctrinal) considerations. Commenters should also address any potential alternatives that permit the asserted noninfringing use(s) without the need for circumvention. Commenters should provide an evidentiary basis to support their contentions, including discussion or refutation of specific examples of such uses and, if available, documentary and/or separately submitted multimedia evidence.

Item 7. Statutory Factors

Evaluate the proposed exemption in light of each of the statutory factors set forth in 17 U.S.C. 1201(a)(1)(C):

(i) the availability for use of copyrighted works;

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) any other factor that may be appropriate for the Librarian to consider in evaluating the proposed exemption.

Item 8. Documentary Evidence

Commenters are encouraged to submit documentary evidence to support their arguments or illustrate pertinent points concerning the proposed exemption. Any such documentary evidence should be attached to the comment and uploaded through the Office's website (though it does not count toward the 25-page limit).