

June 29, 2015

Jacqueline Charlesworth
General Counsel and
Associate Register of Copyrights
United States Copyright Office
Library of Congress
101 Independence Ave. SE
Washington, DC 20559-6000

Re: Docket No. 2014-7
Exemptions to Prohibition Against Circumvention of Technological Measures
Protecting Copyrighted Works

Dear Ms. Charlesworth:

The following represents my and Public Knowledge's response to your post-hearing questions in Proposed Class 27: Software—networked medical devices.

1. Disclosure to manufacturers

Disclosure to manufacturers should not be a requirement for a research exemption, much less an exemption for personal access to data.

The proposed exemption includes circumvention for both research and improvement of medical devices; the research component encompasses not only security research but also research into the ordinary reliability, safety, and operation of the devices. The circumstances surrounding different avenues of research, and the different possible results in each case, as well as the different reactions of the involved parties militate against a bright-line rule preventing such research absent a future duty to disclose. Furthermore, preventing researchers from disclosing their results before notifying a manufacturer can delay the sharing of vitally important information (in the case of product failures or security vulnerabilities), or encourage manufacturers to discourage further work, in the case of patient-directed modifications.

The record on what security risks could result from the proposed exemption is already sparse, and what is there corroborates Proponents' request for a broad exemption with minimal conditions. The record on the consequences of failing to disclose to a manufacturer is even sparser. Disclosure conditions were neither discussed by exemption opponents in their comments, nor at the hearing. As such, there is no evidence on the record that a disclosure requirement would prevent copyright infringement, promote security research, or increase patient or consumer safety.

This is not to say that disclosure is not often the responsible course of action for researchers; merely that there is insufficient information for the Office to determine the circumstances of when such disclosure would and would not be appropriate.

For instance, Petitioners noted that many flaws in medical devices are product failures, as opposed to security vulnerabilities that require active threats to be exploited. Such ordinary product failures would not be more likely to occur if the researchers published immediately. If researchers determine that a large number of devices will suffer failure under ordinary use conditions, they have a responsibility to share that information as widely as possible so that patients and their caregivers can take appropriate action, without building in a delay time for manufacturers to separately assess the problem.

Even in the case of security vulnerabilities, the threat can be immediate enough that public disclosure is warranted without delay. This is particularly true if it seems likely that the vulnerability is known to potential bad actors, but not to patients, healthcare providers, or others. In such a case, again, rapid disclosure could easily be warranted.

It should not be a surprise that manufacturers have a clear incentive not to advertise flaws in their products. A manufacturer taking a more Pollyannaish view of the likelihood of its products' failure may, upon receiving disclosure, attempt to downplay its severity. Manufacturers may also attempt to threaten action under not only the DMCA, but also other causes of action, such as defamation or other sector-specific laws, in attempts to chill or silence criticism. Other researchers simply attempting to modify their own device's outputs to gain better access to their own data might also be discouraged from doing so by manufacturers who wished to sell upgraded models, or who simply wished to demonstrate out of an excess of litigation caution that they did not explicitly endorse such modifications. These considerations will apply to varying extents in different situations; it would be difficult for any policymaker, let alone one not specialized in security issues, to create an exemption that can successfully thread the needle between promoting responsible disclosure (the definitions and benefits of which are not fully developed in the record here) and preventing or chilling legitimate research.

An additional question arises regarding how a disclosure requirement could be applied to an exemption: would a requirement to disclose to a manufacturer prevent the circumvention itself, or merely subsequent publication of the results? If the former, the condition can even more readily chill research, stopping it before it even starts, if the manufacturer exerts pressure (through legal action or refusing device access) against the researcher. Often, too, a researcher might not be able to recognize until a project has begun that circumvention might be necessary; requiring researchers to stop midstream and wait for approval would have a clear deleterious effect on research. Nor would it do to have researchers be left in a cloud of uncertainty if they are allowed to circumvent, but are required to disclose within a timeframe potentially divorced from the progress of their research.

If a disclosure requirement were tied instead to disclosure before publication of results, additional problems arise. First, researchers who circumvent, but do not end up creating publishable results, should not be penalized for their investigation. But more

crucially, publication should not be delayed if immediate disclosure would benefit the public—a determination that must be made on a case-by-case basis.

In addition, as noted at the hearing and in the questions, conditions placed upon publication face First Amendment concerns. Penalizing publication would be a prior restraint on speech, presumptively disfavored under the First Amendment.¹ The record thus far has not made an adequate showing of a sufficient government interest that would be promoted by preventing security research (or its publication) prior to manufacturer disclosure.²

The prior restraint problem would be exacerbated should there be a time limit built in to the disclosure requirement; delaying news of product flaws or security vulnerabilities can be as significant, or more so, to delaying the reporting of news by the press.³

The First Amendment considerations remain relevant even where, as here, they are not an affirmative prohibition, but a condition upon the grant of a government benefit. The doctrine of unconstitutional conditions prevents restraints upon speech as conditions of grants of benefits such as the exemptions requested here. For instance, while the government is not required to renew the contract of a state junior college professor, conditioning such renewal upon his exercise of his First Amendment rights was.⁴ In order for the government to impose a condition that impinges free speech, it must show a compelling government interest.⁵ That compelling interest has not been demonstrated here, nor can the Office likely narrowly tailor such a condition to address the as-yet unspecified interest to fit the Congressional intent behind section 1201.⁶ As noted above, and by Petitioners and many commenters, such disclosures are unlikely to resolve the problems, if any, caused by lack of advance manufacturer knowledge of product flaws, and may simultaneously prevent or chill desirable speech and research. This is particularly problematic if the disclosure is mandated at the initiation of research, or if there is a time limit required between notice and publication.

2. Relationship to Other Laws and Regulations

¹ See, e.g., *Bantam Books Inc. v. Sullivan*, 372 U.S. 58, 70 (1963); *Carroll v. President Com'rs of Princess Anne County*, 393 U.S. 175, 181 (1968); *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 558 (1976); *New York Times Co. v. United States*, 403 U.S. 713, 714 (1971); *R.A.V. v. City of St. Paul*, 505 U.S. 337, 430 (1992); *CBS v. Davis*, 510 U.S. 1315, 1317 (1994).

² See, e.g., *Religious Technology Center v. Lerma*, 897 F. Supp. 260 (E.D. Va. 1995) (“If a threat to national security was insufficient to warrant a prior restraint...then the threat to plaintiff’s copyrights and trade secrets is woefully inadequate”) (citing *N.Y. Times Co. v. United States*, 403 U.S. 713.).

³ See, e.g., *Nebraska Press Ass'n v. Stuart*, 427 U.S. at 560 (As a practical matter, moreover, the element of time is not unimportant if press coverage is to fulfill its traditional function of bringing news to the public promptly.”)

⁴ *Perry v. Sindermann*, 408 U.S. 593, 597 (1972). See also *Speiser v. Randall*, 357 U.S. 513, 526 (1958); *US Agency for Intn'l Dev. v. Alliance for Open Soc'y Intn'l, Inc.*, 133 S.Ct. 2321, 186 L.Ed. 2d 398 (2013).

⁵ *Speiser*, 357 U.S. at 529.

⁶ *Alliance for Open Soc'y v. USAID*, 430 F. Supp. 2d 222 (S.D.N.Y. 2006) *aff'd*, 651 F.3d 218 (2d Cir. 2011) *aff'd sub nom. Agency for Int'l Dev. v. Alliance for Open Soc'y Intn'l, Inc.*, 133 S.Ct 2321.

The exemption should be granted without reference to other laws and regulations. The grant of the exemption does not affect the force or applicability of FDA regulations. To the extent that it may intersect with the Computer Fraud and Abuse Act, granting the exemption without reference to the CFAA would allow for legitimate uses, while still permitting nefarious circumvention to be prohibited under CFAA.

Conditioning an exemption upon meeting the standards of other laws can lead to unnecessary complications in researchers assessing potential liability for their research. The various uncertainties already can pose certain problems for many of them; creating complex interactions between disparate areas of potential liability will not improve security can will curb many good faith researchers from proceeding.

For the foregoing reasons, Public Knowledge believes that the Class 27 exemptions should be granted without conditions upon manufacturer disclosure and without conditions based upon other areas of law that may affect device research.

Sincerely,

/s/

Sherwin Siy

Vice President of Legal Affairs

Public Knowledge