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

Item 1.Commenter Information: Catherine R. Gellis, on behalf of herself and the Digital Age Defense project, a project focused on governmental efforts to control the use and development of technology. (See http://digitalagedefense.org for contact information.)

Item 2. Proposed Class Addressed:

Proposed Class 11: Unlocking – wireless telephone handsets

Item 3.Statement Regarding Proposed Exemption

Exemptions for all proposed classes, including this one, should be liberally granted for many reasons but particularly in light of the relationship Chapter 12 of Title 17 has with the Computer Fraud and Abuse Act of 1986 ("CFAA"). *See* 18 U.S.C. § 1030.

It is a close relationship. For instance, the built-in exemptions from Chapter 12 for encryption and security research reference it directly. *See* § 1201(g)(2)(D) and § 1201(j). These exemptions remove this research from Chapter 12's general prohibition against circumvention of technical measures, provided that the research does not violate the CFAA. But this statutory language is circular: research is acceptable under Chapter 12 so long as it does not violate the CFAA, but without being authorized pursuant to Chapter 12, the research may be construed as the kind of access of a computer the CFAA is often presently interpreted to bar.

There have been numerous legal actions, including criminal prosecutions, targeting people's interactions with computers, even ones they were generally entitled to interact with, because it was interpreted that this interaction was either without authorization or in excess of what was authorized. *See* 18 U.S.C. § 1030(a)(2)(C). Notable examples from the past three years include the prosecutions of Andrew Auernheimer, who had accessed material publicly (albeit unintentionally) available on a web site (which consequently led to the site owner being alerted to the security defect), and Aaron Swartz, who was prosecuted for accessing academic content he was entitled to access on a computer network was entitled to access as well.[1]

However one feels about these or other CFAA defendants, the prosecutions reveal a truth the Copyright Office cannot ignore: the CFAA has been a powerful weapon against people who have used computing devices in ways that some have thought they shouldn't, regardless of whether those uses were consistent with promoting the progress of the arts and sciences, or even whether the people targeted otherwise had the right to use the computing device as they chose. While assessing the correctness of these CFAA interpretations is beyond the remit of this Office, the Office works in a universe where the threat to punish the use of computing technology not explicitly permitted is a very real one, and one that stands to chill the sorts of activities the Office is charged with protecting under § 1201(a)(1)(C)(iii). Without these exemptions there is significant legal uncertainty for people who want to research, or even just modify in the course of ordinary use, the types of computing devices described in proposed classes 11-27, if the ways they seek to interact with these devices are ways the technical measures built into them do not allow. If this Office is to protect these activities it must therefore issue the petitioned-for exemptions in order to remove the uncertainty that these activities will be sanctioned.

---

[1] Auernheimer's conviction was ultimately set aside for reasons not directly related to the CFAA itself. *See*, e.g., 748 F.3d 525, 532-535 (2014). For Swartz the specter of felony conviction and imprisonment zealous federal prosecutors threatened him with drove him to take his own life. *See*, *e.g.*, http://unhandled.com/2013/01/12/the-truth-about-aaron-swartzs-crime/