Before the

U.S. COPYRIGHT OFFICE

LIBRARY OF CONGRESS

In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

Docket No. RM 2011-7

Submitted by:
Daniel Onley
MA Candidate
Department of Political Science
University of Oklahoma
Building 4, Room 205
555 E. Constitution Ave
Norman, Oklahoma 73019
(405) 306-1517
Daniel.Onley@ou.edu

Pursuant to the Notice of Inquiry of Emption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, this comment is submitted in support of the Software Freedom Law Center's comment requesting that the Librarian of Congress exempt from 17 U.S.C. § 1201(a)(1)'s prohibition on the circumvention of access control technologies, for the period 2012-2015, computer programs that enable the installation and execution of lawfully obtained software on a personal computing device, where circumvention is performed by or at the request of the device's owner.

The so-called "jailbreaking" exemption is an important part of both consumer freedom and a necessity of academic life. Without drawing this letter out needlessly, I shall state upfront that I fully support the ability for a consumer to use a device however they see fit upon purchasing it – the consumer has paid for the hardware and owns it outright. The "jailbreaking" procedure allows the consumer to bypass highly restrictive operating system software that greatly curtails the ability to use the device however the consumer sees fit, which is a right someone should have after they have paid for the hardware. This, however, is not the critical issue that I am writing this letter for – that is reserved for the necessities of academic confidentiality and privacy of research subjects.

Within my academic work I am necessarily engaged in projects that involve human subjects revealing private information that I am entrusted with. This private information is necessarily used in the creation of academic research, but is confined by the consent of the human subjects. The Belmont Report[1] requires that I, as the person who obtains

[1] http://ohsr.od.nih.gov/guidelines/belmont.html

informed consent from the human subjects as well as obtaining the private information, am able to ensure the information is used only in the method described in the consent process and for absolutely nothing else – and most assuredly that the private information will never be publicly disclosed without additional consent. To this end I come back to the subject of “jailbreaking.”

Much computing hardware today, especially in the form of smartphones and tablets, comes to the consumer configured with an operating system and an array of consumer software. In addition to this, the hardware can also come pre-configured with non-consumer software designed to improve consumer experiences in using the hardware by relaying information back to manufacturers or cellular service providers – most notable among such software is the recent press surrounding the software known as “CarrierIQ.” This presents an academic researcher such as myself with a significant problem – I must know what this software is doing with the information I put into the personal computing device.

Without the ability to “jailbreak” pre-configured hardware I am, essentially, unable to use the device within the expectations of privacy set forth by the Department of Health and Human Services via the National Institutes of Health’s Office of Human Subjects Research. I must be sure that any electronic device I use to input information cannot use the information in any way, whatsoever, that goes beyond the confines of the permission I have been granted from both my Institutional Review Board, and more importantly than that, the personal trust placed in me by human subjects with regard to their personal privacy.

To put this into more plain English terms I shall speak more directly. My research involves public policy revolving around illicit drugs and their use. Inherent to such research, when engaging with human subjects, I am asking them to speak of illegal activities that would put them in legal jeopardy if the information were revealed. To this end I am expected to afford the highest caliber of protection of this information I can bring to muster, which means not just password protection and encryption of data files, but assuring that the device itself cannot be hijacked to record keystrokes or any other information that might violate the right to privacy of my human research subjects or breach the confidentiality of the research itself. To this end, the software known as CarrierIQ that records such information brings me much concern, and the ability to stop the software from running on my personal computing devices is critical to using them in my research.

The only way I can ensure both privacy and confidentiality, while still using my electronic devices, is to have the ability to” jailbreak” them. Without this ability I am, essentially, unable to use the devices in my research. In this era it is wholly unreasonable to expect me to forgo using a personal computing device simply to maintain a nuance of copyright law where, in fact, I am not engaging in piracy or any other similar affairs. I am simply required to ensure that the software has no ability to violate the privacy and confidentiality of my research, which means I must have the ability to “jailbreak.”

To this end I implore you to accept the Software Freedom Law Center's exemption request for the ability to "jailbreak" personal computing devices. The need to be able to "jailbreak" in pursuing my research is critical. I can only begin to imagine the sheer quantity of research that would also have to forgo personal computing devices if they cannot be able to assure the privacy and confidentiality inherent to their research. This is, simply put, a much needed exemption in copyright law.

Thank you for taking my comment into consideration,

Daniel Onley
MA Candidate
Department of Political Science
University of Oklahoma