In the matter of **Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies**, Docket No. RM 2011-07, I, Robert J. Stratton III, hereby submit my comments in response to the Notice of Inquiry issued in the aforementioned proceeding in accordance with the Digital Millennium Copyright Act ("DMCA").

In summary, I respectfully request that the Copyright Office approve exemptions for Proposed Classes 1 and 2 in the Electronic Frontier Foundation's filing, and the Proposed Class in the filing by the Software Freedom Law Center, with a particular focus on the statutory factor of Section 1201(a)(1)(C) relating to impacts on criticism, comment, news reporting, scholarship or research, with information security research being of particular consequence.

For the better part of a career spanning more than 25 years, I have been working to protect people from security threats and vulnerabilities within the Internet and other critical infrastructures. I established the security organization at UUNET, one of the earliest Internet backbone providers, have co-founded or joined three security startup companies providing new technologies to protect computer and Internet users, have evaluated information security technologies for investment by In-Q-Tel on behalf of the U.S. Intelligence Community, and have managed a laboratory for U.S. Government-sponsored research at Symantec, one of the world's largest security software companies.

Unfortunately, even as the U.S. Government works to support many efforts to better understand and mitigate the growing set of security vulnerabilities we experience as a nation, it also occasionally functions at cross purposes to those goals. The Office is aware that the DMCA's prohibition on circumvention of certain technologies has had the unintended consequence of creating disincentives (perceived or otherwise) to legitimate computer security research.

I respectfully submit that most (if not all) users of modern information technologies expect that the term "interoperability" necessarily implies safe or secure interoperability. Were that not the case, it is unlikely that any would find enhanced interoperability to be a particularly desirable outcome. As a result, any exemptions for software development for improved interoperability would support efforts by information security researchers to better secure these devices upon which a large portion of our nation's population depend. While these measures may not mitigate the sum total of the risk perceived by legitimate researchers, they are a step in the right direction to secure our infrastructure.

I regularly review submissions for an international series of security conferences and correspond with information security researchers worldwide. Based on my observations some interpretations of the DMCA have generated a "chilling effect" on certain security research, and at times this has driven sorely needed research offshore. "Computer security" is no longer simply the domain of desktop personal computers. Every smartphone, electronic tablet, and embedded system (such as in automobiles) is based on modern microprocessor technology, and shares design, code, hardware features and vulnerabilities with the traditional personal computer.

The reality of these industries is that the original vendors do not always identify critical security vulnerabilities before products are released into the market. This problem exists in every non-PC platform just as it does in the case of traditional desktop computers. The existence proof of this is the reality that "unofficial" software and hardware tools for compromising access controls on electronic tablets, video game consoles, and smartphones almost always take advantage of exactly the same pre-existing software flaws that would be exploited by a malefactor to install malicious software on these devices. While vendors usually take care to find security bugs before release, the reality is that perfect security has been unattainable to date.

Unfortunately, there is an exacerbating factor that increases the risk to users of these non-PC products over that of their desktop analogues. It is the fact that the useful life of devices like smartphones is dramatically shorter than that of desktop computers be it through customer preference or technical realities.

As a result the development and release lifecycles of these devices are far shorter and more rapid than in the computer industry. The amount of time spent on ensuring software quality is commensurately reduced, and the number of flawed products potentially exposing their users to security threats is far greater. Additionally, the likelihood of continuing "patches" for older devices becomes increasingly remote with the release of every new device within a given technology family.

In one study of Android device software updates released between mid-2010 through October 2011[1], the following became apparent:

- 7 of the 17 Android phones never ran a current version of the operating system ("OS")
- 12 of 18 only ran a current version of the OS for a matter of weeks or less
- 10 of 18 were at least two major versions behind, well within their two-year contract period
- 11 of 18 stopped receiving support updates less than a year after release
- 13 of 18 stopped receiving any support updates while the carriers were still selling the device, or very shortly thereafter
- 15 of 18 phones couldn't run the Gingerbread release, which shipped in December of 2010, as late as October 2011

By now, even laypersons realize that software updates fix security problems, and that the unavailability of such updates increases the risk of compromise to a device. It is critical to note that virtually every vendor maintains programs for reporting of security vulnerabilities by people not employed by the vendor. Some vendors offer "bounties," while others credit the researchers who report these flaws when the vendors' software updates are released.

---

[1] Android Orphans, Visualizing a Sad History of Support, M. Degusta, at http://theunderstatement.com/post/11982112928/android-orphans-visualizing-a-sad-history-of-support

The point is that even product vendors who otherwise avail themselves of recourse under the DMCA find benefit every day from independent researchers who write software to run on these devices, often in a manner not contemplated by the original vendor.

Telecommunications is a "critical infrastructure", be it embodied in smartphones, tablets, or video game consoles (which are increasingly supplanting broadcast television for consumption of televised content).

There is a robust "ecosystem" of security researchers and auditors who are continually writing software to test, assess, and mitigate security vulnerabilities on commercially available products. In order to protect this critical infrastructure, there is a necessity for security researchers to attempt circumvention of all manner of product security controls and to write software to test both flaws and mitigation techniques. Several Departments of the U.S. Government have gone on record to inform the public that adversaries (often well-funded) are doing these things on a daily basis, in order to develop methods to exploit vulnerabilities so as to propagate malicious software ("malware").

Whether the goal is to deny service to authorized users, surreptitiously intercept communications, illegally re-sell copyrighted multimedia content, or commit fraud and identity theft, the first step is often to break the security of a consumer's device. In order to protect the public, the security research community needs to be able to find and fix these problems before a less-desirable actor does. In order to do that, they must have the legal ability to install software on any manner of device currently in the market.