



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

Item 1. Commenter Information

The Internet Association <http://internetassociation.org/our-members/>

Item 2. Proposed Class Addressed

Proposed Class 25: Software—Security Research

Item 3. Statement Regarding Proposed Exemption

The corporate members of the Internet Association support the proposal of Professors Bellovin, Blaze, Felten, Halderman, and Heninger (the “Security Researchers”) to establish a security research exemption to Section 1201 of the Digital Millennium Copyright Act.

All computer code that is embedded in devices and components is likely to suffer from malfunctions, security flaws or vulnerabilities. While companies strive to write error-free code, code is written by humans, and all humans make errors. However, as responsible corporate citizens, we seek to constantly improve the quality of our code and the information security of our services and products. Our internal corporate security teams regularly engage in security testing not only of our own code, but also the code embedded in the products of other companies with which our products must sometimes interoperate.

The DMCA currently suffers from ambiguities regarding the legality of this type of necessary and every-day security testing performed by or at the request of responsible companies such as ours. Our business planning is meaningfully damaged by legal ambiguities such as those in the DMCA. The DMCA exposes us and our employees to additional legal risk as we strive to protect our customers’ safety and our own intellectual property assets and goodwill.

We have a legitimate and essential business need for defending our corporate assets and our customers’ data through security testing. This interest should be protected by the Copyright Office. We would expect no negative repercussions to arise with respect to the safety or security of software from granting this exemption. Indeed, to the contrary, if the exemption is granted, security researchers inside companies will be better able to defend corporate intellectual property assets, as well as the data of the consumers who trust us with their information. Similarly, external security researchers would more readily report any malfunctions, flaws or vulnerabilities to us in order to assist us in improving our offerings – a practice we support and financially reward through bug bounty programs. In brief, granting this exemption would be a significant step toward improving information security in the economy.

ISO 29147 and ISO 30111, the standards referenced in the proposed exemption, provide a floor of corporate conduct that embodies security practices already implemented at responsible corporate entities. Hinging an exemption on these standards assists in creating a logical balance between information security and intellectual property protection for responsible corporate entities such as ours.