

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

Item 1. Commenter Information

*Dr. Ian Brown, Professor of Information Security and Privacy, University of Oxford, UK
Dr. Jon Crowcroft, Marconi Professor of Communications Systems, University of Cambridge, UK
Dr. Ross Anderson, Professor of Security Engineering, University of Cambridge, UK
Dr. George Danezis, Reader (Associate Professor) in Security and Privacy Engineering, University College London, UK*

Item 2. Proposed Class Addressed

Proposed Class 25: Software—Security Research

Item 3. Statement Regarding Proposed Exemption

As academics who specialize in the field of computer security, we urge the Copyright Office in the strongest possible terms to grant the exemption request of the Security Researchers under Proposed Class 25. The DMCA without this exemption both significantly damages international collaboration in computer security research and materially harms matters of national security in both the US and UK. Specifically, DMCA Section 1201 is actively research-hostile and destructive to security without the proposed exemption of the Security Researchers: it leaves us all more vulnerable to the criminality of both nation-state sponsored and independent malicious attackers.

The DMCA outlaws critical security research that is, by contrast, currently legal in the United Kingdom. To wit, the United Kingdom expressly rejected a Section 1201-like approach in our legislative process because of the material detrimental impact that such an approach would have had on computer security research. The Internet and, thus, harm caused by millions of defective, vulnerable connected devices have global reach. Ergo, the impact of security research is also global in its benefit. It is critically important for researchers in the U.S. to be able to legally find existing defects to protect all of us: criminals are surely already aware of these defects and exploiting them.

If the Copyright Office corrects the current research-hostile environment by granting the Security Researchers' exemption request, no negative repercussions will 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 – professionals who work in academic, government and corporate settings - will be better able to defend national and international security interests, critical infrastructure, and the economies of both the United States and its trusted allies.

With respect to the use of ISO 29147 and ISO 30111, the use of international standards referenced in the Security Researchers' proposed exemption is a logical choice that provides a floor of corporate conduct. These standards embody security practices already implemented by responsible corporate entities, and hinging an exemption on these standards creates a logical balance between information security and intellectual property protection in the private sector.