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

Commenter Information:
Bruce Schneier

Bruce Schneier is an internationally renowned security technologist, called a “security guru” by *The Economist.* He is the author of 12 books -- including the *New York Times* best-seller *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* -- as well as hundreds of articles, essays, and academic papers. His influential newsletter “Crypto-Gram” and blog “Schneier on Security” are read by over 250,000 people. Schneier is a fellow at the Berkman Center for Internet and Society at Harvard Law School, a program fellow at the New America Foundation's Open Technology Institute, a board member of the Electronic Frontier Foundation, and an Advisory Board member of the Electronic Privacy Information Center. He is also the Chief Technology Officer of Resilient Systems, Inc.

Proposed Class 25: Software —Security Research

Statement Regarding Proposed Exemption

Important security research is being chilled by overly broad laws, among them the DMCA. The result is that we’re unwittingly relying on insecure systems, making us all less safe. I urge the Copyright Office to grant the exemptions being considered for security research on vehicles, medical devices, and other systems: Classes 22, 25, and 27.

This is important. Medical device makers, auto manufacturers, and others argue that broad prohibitions on research activities are justified because independent researchers have no business evaluating the security of their products. They say that security will, on balance, be reduced if independent experts are free to investigate vulnerabilities. This is categorically wrong. The argument has been widely debunked: security by obscurity does not work. In fact, obscurity leads to insecurity. When manufacturers are allowed to bar independent researchers from evaluating their products, they can get away with producing shoddy products. Again and again, we have seen manufacturers hide their insecure systems behind prohibitions designed to bar people from discovering exactly how insecure they really are.

Manufacturers also argue that independent research is harmful because researchers might disclose their findings irresponsibly, leading to exploitation by bad actors. Gagging researchers, though, results in even worse outcomes. When researchers are not free to disclose their findings, companies are free to ignore them. We know from experience that companies deny that researchers’ finding are real, avoid fixing bugs or improving security in a timely manner, and continue pretending that their insecure products are secure. As a result, end-users have no opportunity to protect themselves. If we expect the market to motivate manufacturers to design secure products, there

must be consumer-advocate testing and evaluation so that users can make intelligent buying decisions.

Responsible research often involves working with a vendor to ensure a bug is fixed before it is publicly disclosed, but sometimes full public disclosure is the best course. Disclosure is appropriate in cases where a vendor is likely to be hostile and refuse to fix the bug, or if the threat to the public is so great that people must be given the opportunity to protect themselves by avoiding the software in question. In some cases, approaching the vendor first could result in the vendor putting pressure on a researcher or their host institution or publisher to prevent the public from learning of the issue. We have learned from hard experience that requiring a specific time frame or format for disclosure only enables manufacturers to maintain the insecurity of their products for a longer time.

Manufacturers have pointed out that they sometimes work with select, authorized researchers from outside the company to audit their code for vulnerabilities. This kind of limited access is not sufficient to provide for secure systems. Researchers need independence to better evaluate the security of systems, and better put pressure on manufacturers to fix bugs. Letting manufacturers choose which security researchers they work with is yet another recipe for letting manufacturers hide insecurities in their products.

Finally, independent security research is important because that's how security improves. Prohibitions on security research harm security researchers and, by extension, harm all of us. We're all safer because independent researchers have found all sorts of vulnerabilities in all sorts of systems. It's impossible to design secure systems without understanding how to break insecure systems. I know of many security researchers who have refrained from conducting important security research because they fear the DMCA. I know of even more security research where the results are not being published because the researchers fear the DMCA. All future security research is harmed by this chilling effect. The security of our computers and networks is worse because of it.

The manufacturers' arguments are based on the myth that the bad guys are waiting for security researchers to publish vulnerabilities, and as soon as that happens they will pounce on them. The truth is that the bad guys conduct their own security research, and this rulemaking will have no effect one way or another on how much of that goes on. If the good guys are prohibited from conducting that same research, the bad guys win. The only ones who benefit from prohibiting researchers from exposing bad security are incompetent, deceptive, or just plain lazy manufacturers. On the other hand, we all benefit from exposing bad security: the products improve, our research improves, and security improves.