This is a comment on the class of works proposed by Edward W. Felten and Deirdre K. Mulligan to be exempt from the prohibition on circumvention of DRM under the DMCA.

Our comment is that the Felten-Mulligan class is drawn too narrowly. We present an amended definition of the Felten-Mulligan class of works, with brief arguments.

0. The class of works which should be exempt from the Anti-Circumvention Clauses of the DMCA consists of all malicious software, including viruses, worms, spywares, trojan horses, remote controllers, rootkits, and more. The phrase "malicious software" designates programs which cause harms to a computer and/or its owner, and which are placed on the computer against the owner's wishes and without the owner's express consent. Malicious software might be delivered with a computer or be installed later. Some malicious software may be contained in, or make use of, components installed as hardware.

1. Harms from not granting the exemption: Millions of home and business computer owners have had to remove malicious software from their computers. Many computer owners have had credit card numbers and bank passwords appropriated and compromised. If the circumvention of Technological Protective Measures preventing malicious software from being detected, analyzed, or removed, were illegal, then the DMCA would be used as a shield against computer owners' rights to maintain control over their computers.

The numbers here are easy to estimate as being in the billions of dollars per year losses caused by malicious software, and the number of people adversely affected by malicious software as being in the millions.

2. Harms from granting the exemption: Some malicious software works are under copyright. The malicious software author would lose an apparent right of concealment, and thus, often, the practical ability to commit a crime, or crimes, against the intended victim or victims. In some cases the author, or other rightsholder, might be unable to make a living by making and distributing malicious software, or software which is in part malicious.

The numbers here are harder to estimate, since we know of no successful suit by a malicious software rightsholder against a person who has discovered the malicious software and removed it, on the basis of copyright infringement, or DMCA violation. Perhaps a thousand, or perhaps ten thousand, malicious software authors/rightsholders might lose their chance to sue their victims under the DMCA Anti-Circumvention Clauses.

3. General argument for exemption: Decrypting lists of blocked sites in filtering software presently enjoys an exemption to the anti-circumvention provisions of the DMCA. Computer owners throughout the world are today at great risk of infestation by malicious software. If an exemption were not available for circumvention of malicious software, the scale of harm that would ensue would be far greater than for filtering software. Fewer computer owners are at risk of missing/seeing some sites due to false positives and false negatives on blocked sites lists. The danger from malicious software is in most cases much higher.

The harms our exemption would defend against are not hypothetical: Recently many computers have been infested by the Sony BMG rootkit, and the rootkit has been used by other distributors of malicious software to compromise home and business computers. The Sony BMG rootkit attempts to conceal itself, is under copyright (though it likely also infringes others' copyrights) and is itself malicious software, in that it is installed without consent and damages the computer. Our exemption would prevent Sony BMG from successfully

claiming that the computer owner who gains access to the rootkit has violated the Anti-Circumvention Clauses of the DMCA.

For information on the Sony BMG rootkit see:

http://www.eff.org/IP/DRM/Sony-BMG

The Sony BMG rootkit is an example of a kind of DRM which Microsoft, in cooperation with Intel, IBM, and various computer vendors, intend to place in many home computers in the next few years. The Sony BMG rootkit is weak in practice, in that an expert in Microsoft OSes, if hired to find, analyze, and craft defenses against it, would almost surely succeed pretty quickly. The system of DRM once called by Microsoft "Palladium", and today called by Microsoft "NGSCB", would offer to licensees of Microsoft the same cloaking capabilities as the Sony BMG rootkit does today. But Palladium is much harder to crack open and remove than the Sony BMG rootkit. And Palladium offers other services to authors of malicious software beyond what the Sony BMG rootkit has made available.

Here is a quote which shortly conveys part of the threat Palladium poses to owners of home computers:

> From
> http://zgp.org/linux-elitists/20031211171507.GK3918@cannabis.html#20031211164911.V52507@shaitan.lightconsulting.com
>
> Re: [linux-elitists] Monday 15 Dec: first all-Open Source System-on-Chip
> Jason Spence <jspence@lightconsulting.com>
> Thu, 11 Dec 2003 16:49:11 -0800 rfc822
> mailmethis
> On Thu, Dec 11, 2003 at 01:23:33PM -0600, D. Joe Anderson wrote:
> >
> > w00t! Here's a good start to the the back-up plan if
> > TCPA/Longhorn/Palladium/"Fritz-chips"* get out of hand.
>
> You know, the black hat community is drooling over the possibility of a secure execution environment that would allow applications to run in a secure area which cannot be attached to via debuggers and such.
>
> --
> - Jason Last known location: 2.5 miles northwest of MOUNTAIN VIEW, CA
>
> Under a government which imprisons any unjustly, the true place for a just man is also a prison.
> -- Henry David Thoreau

End quote.

Our exemption would, in part, lift the burden of legal risk a computer owner would face in the attempt to remove malicious software that lies behind the cloak of Palladium.

For information about Palladium see

http://en.wikipedia.org/wiki/Trusted_computing
http://en.wikipedia.org/wiki/Talk:Next-Generation_Secure_Computing_Base

4. Our proposed exemption differs from some proposed exemptions in that our exemption is not aimed at preserving decades old textbook examples of fair use rights, such as the right to quote a work in argument, the right of parody, etc.. Rather, our exemption, if granted, would defend important personal property, that is, the home computer. The exemption would also defend privacy and free speech rights, because of the use of home computers to communicate using the world's Net. The dangers our exemption defends against cannot

be classed as picayune inconveniences nor as negligible impairments of rights. Our exemption would help defend fundamental human rights.

New Yorkers for Fair Use
http://www.nyfairuse.org

Jay Sulzberger
jays@panix.com

US Mail Address:
New Yorkers for Fair Use
622A President Street
Brooklyn, NY 11215