Name:

Todd Colvin

Particular class of works proposed for exemption:

All classes of copyrighted works should be exempted under certain conditions.

Brief summary:

The DMCA does not take into account the need for legitimate, non-copyright holders to circumvent "a technological measure that effectively controls access to a work protected under this title" by stating that "[t]he trafficking in, inter alia, any device or service that allowed others to circumvent such a technological protection measure may, however, be actionable under section 1201(b)." The problem is: 1) Criminals are implementing copyrighted technology that controls access to works which may be considered protected under the DMCA (i.e., the tool used is copyrighted and the work protected is copyrighted), 2) Government agencies often lack the ability to create tools capable of circumventing copyrighted works protected by copyrighted technological measures; therefore relying on the private sector to make tools available. The DMCA does not make exceptions when 1) the copyrighted tool used to protect access was used for criminal activity, 2) the protected work involves criminal activity, or 3) the trafficking of circumventing tools when designed for use in situations where there are exemptions such as the need to access protected works in the course of an investigation.

Facts and evidence:

As an instructor of high-tech crime investigations for Federal, State, and local law enforcement agencies throughout the United States, I am seeing more and more incidents reported of people using access control technology to protect incriminating information. In particular, there is a growing use of encryption and steganography tools of which many are considered copyrighted tools. The DMCA is not clear whether it is acceptable to circumvent the protection on these tools in order to determine how they are protecting works which may or may not also be protected under the DMCA. The DMCA is also not clear as to when it is accepted to circumvent the protection technology when the protected work is material to the investigation. If no exceptions are specified for lawful investigations, criminals will learn of this and exploit it to their advantage. For example, a popular hacker magazine called 2600 published an article this year explaining how steganography can be used to hide information in privileged documents (e.g., communications between a lawyer and the suspect) that law enforcement will not have access to thereby providing total protection of the incriminating information from any search warrant. Without the ability to circumvent any protections placed on the copyrighted tools that make this process possible, criminals will have a full-proof method of protecting information.

Even if an exception is made for investigative purposes, it will not do any good if there are no tools available to law enforcement for this. Currently, the DMCA prevents "[t]he trafficking in, inter alia, any device or service that allowed others to circumvent such a technological protection measure." Since law enforcement is often dependent on the expertise of people and companies in the private sector, such as Guidance Software (www.encase.com) and Access Data (www.accessdata.com), with no exception for circumventing tools for use in investigations any law enforcement exception described above will be useless. For example, a company called WetStone (www.wetstonetech.com) has a tool for detecting information hidden with steganography tools, however, they will not make another product of theirs available to law enforcement which can extract the hidden information because the methods incorporated may violate the DMCA (this information supplied to me by one of their sales representatives).

Because of these problems, there needs to be exceptions in the DMCA which allow the circumvention of any work protected under the DMCA (i.e., the protecting tool and the work being protected) and the "trafficking" of any tool that makes this possible for the purpose of lawful investigations.