Proposed Exemptions from Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works

by Darrin Cardani
President, Buena Software, Inc.

I am president and owner of Buena Software, Inc., a software company that sells video and image processing software and services. I am also a musician. Thus, I hold several different types of copyrights on several different things, ranging from musical compositions to computer applications. Because of this I have a need to both protect my intellectual property as well as a need to create products that allow users to make the most of the intellectual property they have purchased, licensed, or own. Below is my proposal of a class of works which should be exempt from the prohibitions on circumvention of technological measures that control access to copyrighted works as laid out in the Digital Millennium Copyright Act.

Class of Work for Proposed Exemption

I believe that the anti-circumvention clauses in the DMCA need to be amended to exempt tools which circumvent access protections to devices, applications, and media created at a later time. To be more clear, any tool which already exists, and happens to be able to circumvent the access protection on a newly created device, application, or medium, should be exempt.

Summary

Many companies are using encoding schemes rather than strong encryption to minimally protect their works from being accessed. Further, many of them are using old, well established encoding techniques which can be decoded by existing software or hardware tools. It is unfair to potentially penalize companies that have existing products which happen to be able to circumvent the extremely weak access protection on newer works. Further, if not exempt, this could become an anticompetitive tactic to threaten products that currently serve existing markets.

Facts

I would like to detail a few examples based on both a case that is currently being prosecuted, as well as on my own experiences.

Over the past year, the case of Adobe vs. ElcomSoft has been widely publicized. While the outcome of the case is still pending at the time of this writing, it provides a good example of the class of tools to which I’m referring. In the interest of disclosure, I should point out that I do have a business relationship with Adobe. They sell some of my company’s products in their web store, and I work directly with them in the development of some of our products. And with all due respect to both Adobe and ElcomSoft, my comments should not be construed as implying that I feel the outcome of their case should go one way or the other. I am merely using their case to illustrate the particular class of tools I feel should qualify for an exemption.

As I understand it, Adobe has sued ElcomSoft under the DMCA for writing a computer application which circumvents the access protection on their electronic book software, thus allowing a user to access the text of the book without paying license fees to Adobe or the book publisher. The application ElcomSoft created was written after Adobe released their eBook software. However, for the sake of illustrating my point, let’s assume that they produced the product before Adobe announced their eBook software, and that ElcomSoft had no idea that Adobe was going to be releasing such a product.

The access protection that Adobe employed in their eBook software was a simple, and extremely well-known encoding scheme named “ROT 13”. It takes the usual method of encoding text as numbers, but adds 13 to the values for the letters A-M and subtracts 13 from the values for the letters N-Z. As such, it is not really encryption, just a different encoding. Many other possible encodings are currently in use, too, such as EBCDIC, UTF-8, Unicode, and many more.

I mentioned that the ROT 13 encoding scheme was very well known. How well known is it? A search on a popular Internet search engine turns up over 65,000 pages describing the format. Several of the pages have a text field where you can enter text encoded in ROT 13 and get back readable text and vice-versa. (See <http://the-stable.lancs.ac.uk/~esarie/bibble/rot13.htm> for one example.) It appears that those pages are capable of circumventing the access controls Adobe used in its eBook software.

It is inconceivable that someone who wrote an application which decodes ROT 13 several years ago, could face prosecution for having written that application simply because another company made a poor choice for their access control years later. In the case of ElcomSoft, they didn't write their application before Adobe released theirs, but if they had, they should be exempt from prosecution. Otherwise, no company could write any software without fear of being sued under this clause. Further, companies could write software which uses encoding schemes that their competitor's currently shipping applications decode, simply for the purpose of threatening them with legal action.

This may sound like a rather absurd scenario. After all, how often does a company use an existing, easy to circumvent form of access control? I've personally come across several tools which circumvent other tools' access controls accidentally. For example, I first started doing video editing about 10 years ago when I bought a computer with a video capture card. It allowed me to take video from an analog video camera or VCR and store it digitally in my computer, where I could edit out mistakes, add effects and transitions, and other interesting things. One evening I was testing out some video editing software I was writing, and I needed some video footage to test with. I simply turned on my VCR and connected it to the computer. I started changing channels looking for something interesting to capture for my test, when I came across a cable channel that I wasn't paying for. I was surprised to see that my computer was displaying the channel just fine. I hooked the VCR back up to the TV to check if the channel was still scrambled, and it was. It turns out that on older analog cable systems, one method of limiting access to premium channels ("scrambling" them) is to make the video signal just slightly out of the required specifications. Cable boxes have the hardware to correct the signal, but it will cause most VCRs and TVs to either not display it, or to display it in its "scrambled" format if they don't have a cable box connected, thus denying access to the nonpaying viewer. But some equipment, like the video capture card I was using, will actually correct a bad signal before displaying it, too. The card was not designed to steal cable. It just happened to be able to do so.

Clearly companies are using well known techniques as access control every day. This puts designers of new products in the impossible position of having to assure that their products, which may do something unrelated, don't accidentally infringe on someone else's poorly conceived access control scheme at a later time. My company has already canceled 1 product for fear of running afoul of the anti-circumvention clauses in the DMCA. Our product would have allowed the user to capture and playback a stream of video and/or audio data that they watched on the Internet. It's intent was not to allow the user to make illegal copies of music or movies. It was simply to allow future access to something you couldn't view live, as a VCR does with television programs. And while it didn't have any code in it which allowed trading of saved video or audio data, that would have been possible with the tools available in every currently shipping operating system used on home or business computers. It's probably a good thing that I did cancel the product, because other companies that make similar products have been threatened with such legal action. (See <http://www.macintouch.com/audiostreaming.html> for some examples.) In other words, they wrote tools to record data, but it also happened to get around the access controls built into the file formats or transmission formats which other companies came up with, and they have now been threatened with legal action.

Conclusion

As a copyright holder, myself, I am painfully aware of the need to protect intellectual property. I personally spend time writing both access control and copy protection code for our products. Nevertheless, it would be unjust not to exempt tools which are created first, and later become capable of circumventing someone else's poorly thought out access control scheme.