Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies: Comment

Dr. Kevin B. Theobald
Research Associate
University of Delaware

February 17, 2000

The recent boom in the computer industry would not have happened without the use of open, published standards. The Internet was made possible through common protocols such as TCP/IP, and grew to become a household word thanks to common formats such as HTML. The use of open standards is a boon to consumers, who value the ability to interact with other consumers, and to new businesses, who can find a ready market for their products if they conform to the standard. This leads to vigorous competition in the marketplace.

On the other hand, when competitors in a field don't agree upon or abide by a common standard, the tendency is for one or a small number of standards to win ultimately, with other competing standards eliminated. Once this occurs, new companies have no choice but to support the dominant standards. This is straightforward when standards are published. However, when formats are kept secret, competitors must resort to reverse-engineering the formats in order to design compatible products. The alternative is to allow a single company to control the market through control of the standard.

Yet the Digital Millennium Copying Act (DMCA) is being used in a legal battle to suppress the right to reverse-engineer a standard to achieve interoperability. Section 1201(f) of the DMCA specifically allows such reverse-engineering, and Congressional discussion[1] supports the use of reverse-engineering for interoperability. However, recent court rulings have interpreted it too narrowly. It is essential to the vitality of the computer industry that Congress clarify and uphold the right to reverse-engineer standards. Otherwise, the protection of proprietary formats will become a legal weapon used by the dominant players in a given field to stifle competition.

The specific case addressed in this comment is the use of the DMCA to support legal prosecution and intimidation of the designers and distributors of DeCSS.

Movies stored on Digital Video Discs (DVDs) are encoded using a weak key-based encryption system called CSS. DVD owners must use a means to decrypt the stream from the DVD in order to watch the movie. This requires either a special-purpose DVD player (designed

[1] S. Rep. No. 105-190 (1998)

only for reading DVD movies), or a computer with a DVD reader and appropriate software to decrypt the contents of the DVD. Currently, the DVD Copy Control Association (DVDCCA) licenses software for use under variants of the Microsoft Windows operating system, yet does not license equivalent software for use under other operating systems for Intel-compatible computers, such as Linux and FreeBSD.[2] Thus, an owner of an Intel-compatible personal computer with DVD reader, who has legally purchased DVDs, is unable to make fair use of copyrighted material legally acquired, unless he or she incurs the additional expense of a license for Windows or a special-purpose DVD player. Alternative forms of access are less acceptable; VHS tapes degrade and are subject to numerous failure modes, while Laserdiscs are a dying standard and unlikely to be supported in the future.

DeCSS is a program for decrypting CSS-encoded DVDs. It was designed by reverse-engineering the CSS format and its keys. An important by-product of DeCSS is a program called css-auth, which allows owners of DVD readers to play their DVDs under the Linux operating system. Yet the DVDCCA and representatives of the movie industry have aggressively pursued the designers and distributors of DeCSS in the courts, alleging the threat of piracy.

In a recent New York court case,[3] a temporary injunction was granted against distributors of DeCSS. An argument by the defendants that they were exempted by the reverse-engineering section 1201(f) was rejected by Judge Kaplan. His ruling said, in part:

> [...] Section 1201(f) permits reverse engineering of copyrighted computer programs only and does not authorize circumvention of technological systems that control access to other copyrighted works [...]

Unfortunately, by restricting the protection of Section 1201(f) to computer programs only, Judge Kaplan effectively disallows the decoding of file formats, which is essential for achieving interoperability. (An example of a file format is the PDF format, which is the format of this document.) If his interpretation prevails, a dominant company wishing to preserve its monopoly over a particular file format could implement a trivial encryption method, such as inverting the data bits, and then claim that since some copyrighted material is stored in these formats, any competitor's product which can read these formats is a method for circumventing access control, and is hence illegal under the DMCA.

The fundamental flaw in DMCA is that it makes the mere use or distribution of a circumvention device illegal, *regardless* of whether the circumvention is actually used to violate a copyright or is only used to make a fair use of copyrighted material. The implicit assumption that any "unauthorized" circumvention is *a priori* for nefarious purposes places reverse engineering on shaky legal ground, in spite of the weak attempt to protect it through Section 1201(f). Congress *must* repair this flaw and vigorously uphold the right of reverse engineering, or risk causing irreparable harm to many companies in the computer business by giving the designers of dominant file formats a legal weapon to protect themselves from competition.

[2] Current estimates of the number of users of Linux range from 7 million to 10 million.

[3] http://www.nysd.uscourts.gov/courtweb/pdf/00-01149.PDF