

Comments for Discussion 1201

Chris Heidelberger

Below are my responses to questions 1,2,18,19, and 20 posed in DOCID: fr24no99-23, "Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies" with regard specifically to the class of copyrighted works known as DVD (Digital Versatile Disk).

1) Digital encryption is the main form of copyright protection available and used in the technology field. The encryption can be as simple as three and five bit encryption to the much more secure and complicated 128 and 256 bit encryption. In some cases the simple encryption is all that is needed to keep the data secure. With more important data, however, where there is a large chance for a user or group to want to infringe on the copyright and where it is financially critical that the copyrighted information is kept secure; the stronger encryption is needed to a) prevent the decryption of the data, and b) make the time needed for decryption increase substantially such that it becomes infeasible (or close to impossible in the case of 256 bit encryption) to attempt the decryption. One example where it wasn't the type of encryption that failed but the application of the encryption that allowed for decryption of the data is in the case of the DVD consortium's CSS encryption. Their practice of giving "keys" to DVD manufacturers to put in the hardware to decode the file is what led to the decryption. This key is used in the hardware to be able to decode the file and is normally encrypted, too. One manufacturer forgot to encrypt the key and once it was found, the other keys could then be deciphered. In this case it wasn't the encryption method that was faulty, but the implementation of it. The DVD consortium's CSS encryption only prevented playing of the DVD and not the illegal copying of the DVD. Macrovision encoding is another way to prevent copyrighted material from being illegally used and copied. It encodes the video data such that when the data passes through a VCR, the data is degraded substantially. This allows normal playing of the video, but not copying by means of a VCR.

2) Digital encryption will allow one to keep data secure while still allowing the end-user to have easy access to the intended usage. In some cases, however, this is not true. Again, in the case of the DVD consortium, the implementation adversely affected the user's ability to make noninfringing use. The CSS encryption method inhibits the ability to play an encrypted DVD without the key given by the consortium. CSS in no way prevents the legal or illegal copying of the data. A user can copy the entire DVD and play it without any adverse effects (whether for backup purposes, which is legal, or for pirating purposes). CSS only says what can play a DVD, not who can copy or play it. Currently there are no players available for users of Linux based operating systems, so it was necessary for those users to decrypt CSS to be able to play DVDs that they owned. This directly affected the user's ability to make noninfringing use. Macrovision encoding shows the way copyright protection can work for both the user and the copyright owner. Any user can play the movie, but it is much more difficult to copy it. CSS makes it a trivial issue to copy the copyrighted movie, but makes it difficult to watch it. That is the key point when looking at copyright protection methods: the method of implementation is what makes the method useful or the infringement on the copyright legal.

18) Different protection methods can be circumvented in many ways. There is a saying that if humans can protect it, humans can break it. In some cases it is trivial to circumvent the protection. In the CSS case all it took was one manufacturer to make a mistake and forget to encrypt the key and the entire CSS encryption scheme was broken. With 128 bit encryption, it takes many years for 100,000 computers working together to break the encryption. Macrovision can be circumvented by means of a \$30 piece of hardware from an electronics store. The circumvention of the CSS is very limited. It is only done by people needing to play it on computers where players aren't available or where (for some reason) the raw data is wanted. Macrovision is circumvented much more often. It is more important for people performing illegal operations to copy material than to simply play it. It is also easier to bypass Macrovision.

19) The circumvention of CSS and Macrovision haven't obviously affected the price of the DVD media. There may be future effects, but since the inception of Macrovision a few years ago the price has remained steady, as has the price of DVD since the CSS encryption was broken. There doesn't seem to be any effects coming, though.

20) The circumvention of CSS and Macrovision haven't had any adverse effects on availability, either. If anything, it allows more users to play the DVDs meaning more people will buy DVDs. If more people are buying DVDs, then the availability should go up, as it becomes even more profitable to produce movies on DVD.