1. What technological measures that effectively control access to copyrighted works exist today?

To my knowledge, only two categories of effective access controls exist today:

1. Non-electronic copyrighted works, such as printed books, are difficult to copy because they are not in a format easily handled by a machine. This does not mean that copying them is impossible; but it is usually more tedious, difficult and time-consuming to copy a printed book than to buy a copy from the publisher.

   This argument does not hold true for works which are no longer published. Out-of-print books cannot easily be purchased; in such cases, it may be more expedient to find an illegal copy of the work than to purchase a copy from the publisher. Hence, the non-electronic format is only an effective means of copyright protection for so long as the work remains widely available through normal distribution channels.

2. Certain copyrighted works (such as computer software) require a decryption key or "code word" before they can be used. In these cases, a different key is usually issued to each user (customer). It would be a trivial matter for one customer to copy the copyrighted (encrypted) work, and to give a copy of the work and a copy of the decryption key to another customer; but presumably the copyright holder knows which key was issued to each customer, and could therefore hold the first customer (to which the key was issued) responsible if the key is found in someone else's possession.

13. What impact has the use of technological measures that effectively control access to copyrighted works had on the ability of interested persons to engage in noninfringing uses of such works, including fair use and activities permitted by exemptions prescribed by law?

Computer software which uses a decryption key (or "code word") to enable it places several burdens on the user:

- The decryption key is usually printed on a piece of paper which is shipped with the media containing the software, not on the media themselves. Thus, it is easy to separate the decryption key from the copyrighted work it unlocks, and misplace it. The administration of these decryption keys requires additional overhead for the user.

- Because the decryption key is often printed on paper, instead of in an electronic format, it is sometimes difficult to read it (especially when reinstalling the software after a few years, at which point the paper and/or ink may have deteriorated).

- Often the decryption key is useful only for one particular computer (it may interact with a unique serial number of the computer's CPU, or ethernet card, etc.). Reinstalling the software on a second computer after removing it from the first computer (after a hardware upgrade, or hardware replacement in the event of failure) requires the acquisition of a new decryption key. This is often time-consuming, and prevents the noninfringing use of the work during the time when the new key is being acquired.

I also wish to mention some technology from the past:

- In the past, it was common for computer software distributed on floppy diskettes to be "copy-protected". This usually meant that the format of the data on the diskette was nonstandard in some way; the number of data tracks may have been larger than normal, or the number of sectors within each track may have been non-uniform, etc.

  This practice was abandoned in part because of the burden it placed on noninfringing use of the software. Legal users were unable to make archival copies of the works. And since the work had to be accessed by using the original floppy diskette, this also meant that the software could not be copied to the user's hard drive for faster start-up. Complaints about this burden led to the demise of this technological measure of access control.

- It was also common for some copyrighted computer software to ask the user for a random piece of information from a printed manual. (For example, while playing an game, it was common for the game to stop at some critical moment and ask the user for the seventh word of the second paragraph of page 57 of the manual.) It was also common for the manuals to be printed with colored ink, in combinations which made photocopying the manual difficult or impossible given the state of xerographic technology at the time.

  This technological means of access control was also discontinued due to the burden it imposes on noninfringing use. Users often misplaced the manuals, leading to an inability to access the protected work. The colored inks used to prevent photocopying the manual also prevented users from making (useful) archival copies of the manuals.

18. In what ways can technological measures that effectively control access to copyrighted works be circumvented? How widespread is such circumvention?

Any copyrighted work in an electronic format can be copied easily. It is *not possible* to create *any* technological measure that effectively controls access to it.

As I mentioned in response to question 1, the only effective measures in use today are ones which rely at least in part on non-technological means. As I mentioned in response to question 13, the technological measures that controlled access to copyrighted computer software in the past have been abandoned.

The fundamental nature of electronic formats is to make automatic duplication easy. This is because the electronic format must be converted by a machine into a human-readable format if the work is to be of any use to humans. The end result of this conversion process will *always* be something which can be copied; and depending on the nature of the medium, it may be possible to copy the information which constitutes the protected work at some earlier point in the conversion process.

Since the DVD is such a controversial technology today, I will use it as an example. The DVD is an optical medium which contains data that can be read by a computer. This data is encrypted, and must be decrypted using a key known only to the DVD player. Once the decryption has occurred, the data (a movie, song, etc.) can be read and converted into a video stream, an audio stream, and so on.

There are at least three ways to "circumvent" this "protection" (I use the terms loosely because I do not truly believe that there is any effective protection involved here, and thus there is no true "circumvention" required to make a copy).

- An exact copy of the encrypted DVD can be made easily. There is no protection of the encrypted data; a user can simply read the encrypted data from one DVD and write it onto another. The copy is exactly the same as the original, as far as any DVD player knows; a DVD player that will play the original will play the copy.

- One or more of the encryption keys known only to the DVD player can be learned, and used to decypt the data on the DVD. Once one of these encryption keys is known, any DVD encrypted with that key may be decrypted, nullifying the "protection" of the content.

  In fact, due to the weakness of the encryption algorithms which were used in DVD technology, many of these keys are already known to the public. These keys are readily available on the Internet for anyone who knows how to find them. The software known as DeCSS (decrypt content scrambling system) will decrypt a DVD and requires no knowledge of cryptography to use.

- Finally, the content itself can be copied during playback. In order to watch a motion picture on a DVD, the data must be decrypted, and then the video stream must be sent to a television or other machine which converts the video stream into light which our eyes can perceive. The video stream may be copied while it is being sent to the television; or the light which the television emits can be copied.

  A similar argument holds for audio streams, or any other type of information which can be encoded electronically. So long as the information must be presented in human-readable form, it can be copied while it is in that form.

I have no knowledge of how widely such "circumvention" is used. But given the sheer *ease* with which any of these steps can be performed by an average person, I think would be foolish to assume that such "circumvention" is *not* widespread.

When "copy-protected" diskettes were still in use, circumvention was also common. Software which could read the non-standard diskette formats was available and was widely used. For diskettes that were particularly hard to copy, more sophisticated users used hardware or software that could copy the memory of the computer that was running the protected work; thus, after loading and starting the protected software, a "memory snapshot" would be taken, and copied to produce a new piece of software. When this new software was loaded, it would have an effect identical to the copyrighted work at the time the "snapshot" was made.

20. Has such circumvention (or the likelihood of circumvention) had any impact on the availability of copyrighted works? In particular formats or in all formats? Please explain.

There is a widespread rumor that George Lucas is refusing to release *Star Wars: The*

Phantom Menace on DVD because of DeCSS. But only Mr. Lucas can confirm or deny this rumor with any authority.

- -
Greg Wooledge
661 Lakeside Avenue
Lorain, OH 44052-2037
USA
(440) 288-8135
wooledge@kellnet.com
http://www.kellnet.com/wooledge/