Reply to DMCA Comments

Ken Arromdee

March 29, 2000

I've read with interest the many other comments and would like to reply to some, as well as clarify some points that others have missed.

The DMCA and CSS

The first point is minor: many commentators have referred to the Motion Picture Association of America's (MPAA's) lawsuits and the use of the DMCA in the lawsuits obliquely, without explaining it. A short explanation follows:

Computers with DVD-ROM drives can play DVDs, including movie DVDs. However, playing DVDs is only possible with the appropriate software. This software exists for the Microsoft Windows operating system. However, in almost all cases, it does not exist for the Linux operating system, leaving Linux users unable to play DVDs.

The data on DVDs is encrypted with a system called CSS, so playing a DVD requires decrypting this data. CSS decryption is normally licensed by the MPAA through the DVD Copy Control Association (DVD-CCA), at a fee of thousands of dollars, which anyone wanting to create a player or playing software would have to pay.

Linux hobbyists worked on their own to reverse-engineer CSS; the first effort that succeeded was the one that resulted in the DeCSS program. DeCSS could be used as a part of Linux DVD-playing programs, and Linux users could now play DVDs under their operating system of choice.

In December 1999 the DVD-CCA sued distributors of DeCSS under California trade secrets law. In January 2000, the MPAA sued distributors of DeCSS in two cases, *MPAA v. Reimerdes, Corley and Kazan* in New York, and *MPAA v. Hughes* in Connecticut. These latter two cases were made under the DMCA, specifically clause (a)(2) which prohibits circumventing an access-control measure (CSS) to a work (DVDs).

The Open-Source Movement and CSS

A more important point is about open-source and the open-source movement; the impact of the DMCA on open-source is difficult to explain briefly.

The Linux operating system is what is known as "open-source software", which is software that can be freely copied and, because it has source code available, freely modified. There are still ways for companies to make money off of open-source software; some companies sell support, some sell their own distributions and count on the fact that many people prefer to buy a professionally packaged distribution with documentation (i.e. Red Hat); some sell hardware and make the software that controls it available as open-source, etc. But the business model is drastically different from that used for Microsoft Windows.[1]

There are many advantages to the consumer, whether he is a programmer or not, to open-source.

[1] I wrote this reply comment entirely on Linux, using only open-source software for text editing, text formatting, conversion to PDF format, and spell checking.

- *Open-source programs are available free of charge.* A consumer should not have to purchase a program that he could have obtained for free–if only the law allowed people to write a free program. The effect of the DMCA is as if automobiles came with their hoods welded shut and the law prevented "circumventing a hood access system".[2]Your neighbor could fix your car for free, but if he did so he would be committing a crime. Instead you were forced to pay a mechanic who has enough volume to afford a hood access license.

- *Open-source software is less likely to have bugs, and bugs that are found are rapidly fixed.* This is known in open-source circles as the "with enough eyeballs, all bugs are shallow" concept. Since anyone in the world can analyze a program that is open-source, there is a very good chance for bugs to be found and fixed, and once a fix is found, anyone can apply the fix immediately to the source code without waiting for the manufacturer to release a new version.

  A related fact is that open software cannot contain "backdoors", such as a hidden ability to transmit personal data without the user's permission.

- *Open-source software reduces dependency on the whims of manufacturers.* A manufacturer can stop supporting a product any time that it desires; many are the cases where a company stops producing a product and no longer releases updated drivers–meaning that the product may work poorly (if the consumer must use old drivers that contain bugs) or not at all (if the consumer wants to use the product on a new operating system for which drivers have not been made). With open-source, if a company abandons a product, anyone who can program can use the source code and continue supporting the product.

  (In the case of DVDs, some possible uncertainties include not only whether companies will update their drivers, but whether the MPAA will continue to allow CSS for computers at all.)

The Open-Source Movement, CSS, and the DMCA

CSS decryption, necessary for viewing DVDs, can be done either in hardware or in software. Some hardware decoder boards do CSS in hardware, and so software for them does not need to use CSS. Other hardware boards do MPEG-2 decoding in hardware, but not CSS, so software for them requires software CSS. Finally, a computer with a DVD drive but no hardware board at all can play DVDs by decoding everything, including CSS, in software; however, this process is slow and older computers might be too slow to do it.

The DMCA's impact on consumers is different depending on whether the CSS is done in hardware (some decoder boards) or in software (other decoder boards, or none at all).

First, what little software there is for Linux is limited to working with hardware CSS. Statements by Sigma Designs employees reveal that Sigma's current license does not permit writing Linux software for Sigma's Hollywood Plus board, because this board requires software CSS. The MPAA's reasoning seems to be that if software CSS is used, it is possible for computer hackers to obtain the decrypted data by hacking the operating system. Sigma will be allowed to support Linux on their newer Netstream board which uses hardware CSS.[3]

The problems for consumers are fewer if a decoder board does CSS in hardware, because the MPAA has less interest in restricting software when that is not where CSS decoding is done. However, no consumer should be required to purchase an unnecessary piece of hardware just because he is denied the fair use of his current hardware. Moreover, hardware decoder boards in general are becoming obsolete, and will probably be completely obsolete by 2003–only slower computers require them and computers are getting faster all the

[2]Of course, this all assumes that CSS is an access control system at all. The American Library Association and others have argued in comment 162 that many digital restrictions are use restrictions, and that these are different from access restrictions. This argument is compelling and, if accepted, would also apply to DVDs and CSS, making most of this reply irrelevant.

[3]It has sometimes been said that there is no DVD software at all for Linux. This isn't *quite* true, but it is very close. There is some upcoming software, but as of March 2000 what already exists are drivers for the DXR2 board and nothing else, certainly nothing else which needs software CSS decoding. The most common board appears to be the Hollywood Plus/DXR3, which is not supported now on Linux and for which Sigma refuses to work on future support.

time. By now, even an entry-level computer with a DVD-ROM drive does not need a hardware decoder board; in a few years, this entry-level computer will be (relatively speaking) an old, low-powered, computer.

Note that the effect on fair-use rights may be somewhat indirect; if it is illegal for a programmer to write software to do something, then all consumers are harmed, not because the DMCA prevents *them* from doing something, but prevents a (probably anonymous) programmer from writing software that allows them to do it. The distinction between 1201(a)(1) (making it illegal to circumvent an access-control system) and 1201(a)(2) (making it illegal to produce something that lets other people circumvent an access-control system) is very blurred for software because of this factor. If consumers were allowed to circumvent an access-control system for personal use but if distribution of software were prohibited, that would be functionally equivalent to not allowing the consumer to circumvent, as few consumers would or could write the software themselves.

The most direct harm to consumers, of course, is that most Linux users can't legally play DVDs on their operating system at all. And there are several points to consider in relation to open-source, which would be true whether there is any Linux DVD software or not:

- *Open-source programmers cannot afford licensed CSS.* Many open-source programmers are individuals writing software as a hobby. The fees to license CSS are thousands of dollars at a minimum and are scaled for corporations, not individuals; individuals have no practical alternative other than to circumvent CSS without licensing it, or to not write the software at all.

- *Software using licensed CSS cannot be open-source at all.* Because CSS is kept secret, the MPAA will never allow CSS to be used in open-source software whether the programmer can pay the fee or not. Since anyone can look at the source code of open-source software, that would reveal the secret. Furthermore, since anyone can distribute the software free of charge, the MPAA would be unable to obtain further licensing fees from additional copies of the software.

- *Licensed decoders, unlike open-source decoders, have a restricted set of features.* For instance, DVDs can contain advertisements that are difficult or impossible to skip. Some Disney DVDs require the consumer to press the chapter skip button ten times in the appropriate place to skip all the previews and advertisements (which cannot be fast-forwarded); if advertisements are placed in the section which is currently occupied by the FBI warning on most DVDs, they could be completely unskippable. The MPAA won't license a software driver that lets consumers skip "unskippable" advertisements, but open-source DVD-playing programs would allow this.

  A similar example is region coding. DVDs contain a region code which is checked by the player. A DVD from another country contains a different region code; the player checks the code and won't play the DVD if it is from the wrong country. Foreign DVDs cannot be played with any licensed software–the licensors don't like when people play DVDs from outside their region, since it's bad for their marketing strategy. But while viewing foreign DVDs is bad for the companies' marketing strategy, it is good for the consumer (enabling consumers to get material cheaper, get material earlier, get better versions, or sometimes get material which is otherwise not available at all). On drives which support it (which unfortunately is only older drives), software made using DeCSS would let people play such movies. [4]

  Other examples include pausing scenes which are not supposed to be pausable, defeating Macrovision[5], etc. Viewing a DVD without advertisements or viewing a legally purchased foreign DVD is certainly fair use, but no software which allows such uses will ever be licensed by the MPAA.

- *Users of less popular "alternative" operating systems may not benefit from licensed software.* Operating systems such as FreeBSD, OS/2, and BeOS are less popular than either Windows or Linux (even though the free BSDs probably have millions of users). There are no known plans for any commercial DVD software for them and open-source is their users' only realistic hope of having any DVD software.

[4] Interestingly, there are "cracks" for some Microsoft Windows DVD players and some standalone DVD players which bypass the region coding; if the courts rule that region coding is an access-control measure, these cracks would also be illegal under the DMCA–yet another way in which the DMCA makes fair use impossible.

[5] While Macrovision is promoted as a copy protection system, it has the side effect of making it impossible to play the DVD output through most VCRs–which is necessary if the user has an older TV set with only RF input.

- *Users of Linux on non-Intel-based PCs may not benefit from licensed software.* Manufacturers who release commercial software for "Linux" usually release it only for Intel-based PCs. It is unlikely that even if there is licensed software, it will run on a Macintosh running Linux, let alone a Dec Alpha or other less popular types of computers. Again, these users' only realistic hope is open-source.

Terminology: Class of Works

The original request for comments asks what classes of works should be exempted. I feel that this question is less useful than it might be unless "class of works" is defined in a very nonintuitive way. For instance, if an exemption were to be made to make it legal to play DVDs under Linux, the only straightforward "class of works" that is relevant is "all DVDs". One would have to consider "DVDs whose access control is circumvented for the purpose of..." as a separate class in order to define the class more narrowly, but it is not clear whether that is really a "class of works".

Sony's Remarks

An attorney for Sony Corporation sent in a comment which puts a very misleading spin on another important case where circumventing an access-control system is necessary for the consumer's fair-use rights.

The comment describes a "mod chip" as a device which enables pirates to play illegal copies of games. But what Sony fails to mention is that a "mod chip" also allows playing *legal* copies of *foreign* games. Playstation games are encoded so that Playstations from the USA, Japan, and Europe cannot play each other's games. This incompatibility was deliberately introduced by Sony.

The "mod chip" makes it possible for a person in the USA to play a game that comes from Japan. This is not insignificant, since games in Japan can be released a year or more before games in the USA, and many Japanese games are released in the USA only in modified versions or not at all. (For instance, the "story mode" in the game "Rival Schools" was removed from the US version of the game.) Without using a "mod chip", a person living in the USA and owning an American Playstation cannot play a foreign game.

Mod chips are even more necessary in Europe, because game companies have traditionally paid little attention to the European market, so European gamers are more heavily dependent on import games than American gamers. (I won't discuss this further, since the DMCA is an American law, not a European one.)

Sp contrary to Sony's claim that the access control does not restrict noninfringing uses, playing a Japanese game (which has legally been purchased through an importer) in the USA is clearly a noninfringing use which has been restricted by the access control on Sony Playstations. (Again, assuming for the sake of argument that this really is an access control.) Sony would have you believe that "mod chips" are only good for piracy, and this is an out-and-out falsehood.

I'm directly affected by this; I own a modified Playstation and no pirated games, but several imported games. I believe that this type of circumvention of access controls for interoperability should explicitly be permitted without qualification (the DMCA only has an explicit exemption for computer programs, and only when the computer program is independently written; it is not clear whether Playstation games are computer programs, and using a store-bought Playstation and store-bought import game does not involve independently writing anything). It should also be explicitly stated that the exception applies even if there are infringing uses in addition to the noninfringing uses.[6] (Something which the DMCA already says, but which is obviously not clear enough for Sony.)

[6] Again, the distinction between 1201(a)(1) and 1201(a)(2) is blurred. In order for a consumer to use his foreign disk on his American machine, he must purchase a mod chip made by someone else. No consumer has the facilities to reverse engineer a Playstation and design and manufacture chips on his own, so the only meaningful way to allow personal circumvention is to allow distribution.

Blocking Software

A completely different case has come up where the DMCA prohibits a fair-use activity that is vital to the consumer. Some libraries, workplaces, and schools use or intend to use software which keeps people from visiting certain locations (URLs) on the World Wide Web. The software is generally meant to keep people from accessing pornography or explicit materials, and often used to restrict the Web usage of teenagers. However, blocking software is notoriously inaccurate.

The relevance of the DMCA is that manufacturers of blocking software keep the list of blocked sites secret. It is protected by encryption, an access-control measure. Breaking the encryption to access the list of sites is likely a criminal activity under the DMCA.

But breaking the encryption was the only way to discover that, for example, the I-Gear program blocked sites at a 76% error rate. (See http://peacefire.org/censorware/I-Gear/igdecode/) It is absurd that three fourths of the blocked sites are blocked in error. But it is even more absurd that a student (or adult library patron) who attempts to decode the list of blocked sites to prove that the blocking software is inaccurate, could be sued by the manufacturers of the blocking program because the DMCA prohibits this activity.[7]

(In addition, the students who decrypted I-Gear's list of blocked web sites discovered that the program sends personal information to the manufacturer without the user's approval, contrary to the manufacturer's claims. Discovering this is also illegal under the DMCA. The DMCA contains an exception for security testing, but the exception is narrow; it doesn't apply when the security flaw was found as part of a general search for flaws of all types rather than a specific quest for security flaws. The exemption also considers whether the information was used only to help the owner of the computer and the "developer" of the computer; the people who discovered the security hole in I-Gear released this information to the general public, which would cause them to fail this test.)

If any activity is fair use, discovering the flaws in blocking software and discovering that a program sends personal data have *got* to be fair use. All works being reverse-engineered for (and all works whose access control is broken for) analyzing the flaws (in general) of a product should be exempt as permitted fair use.

[7] So far there has been no suit, but even the possibility of one, especially considering Mattel's similar lawsuit over Cyberpatrol, has caused great uncertainty.