"Authority of the copyright owner" in 1201(a), and First Sale

Robert S. Thau and Bryan Taylor

August 4, 2000

Contents

Acknowledgments

This paper is the result of discussions on the `dvd-discuss` mailing list, part of the Openlaw forum of the Berkman Center for Internet and Society at Harvard Law School, and has benefitted immensely from the insights of those on the list. All flaws are, of course, solely the fault of the authors.

1 Introduction

The Digital Millenium Copyright Act gave copyright holders remarkable new powers to regulate the distribution of their works, which have raised concerns that the traditional balance in the law — between the rights granted to copyright holders and the public interest — is being eroded. These concerns might be allayed somewhat if the copyright holders were carefully staying within the bounds and intent of the law. However, that seems not to be the case. In one of the first trials under the law, Universal et al. v. Corley (one of the so-called "DeCSS cases"), the copyright holders have adopted a sweeping view of their powers under the law; indeed, a view far more broad than anything envisioned by the members of Congress as described the intent of the law in their debates and reports.

Specifically, the movie studios' case in Universal et al. v. Corley relies on an interpetation of the Digital Millenium Copyright Act (DMCA), specifically 17 USC 1201(a) — a view already articulated by their attorney, Dean Marks, in hearings for the librarian of Congress — which we regard as fundamentally flawed. This section of the law provides protection for "access control mechanisms", which as we shall show, was clearly intended by Congress to mean mechanisms which perform some sort of affirmative check that a viewer is authorized to view a particular work. Several such systems have been deployed by the movie studios to protect their work, including one (codeveloped with Circuit City, and marketed to consumers under the name "Divx") which actually checked the authority of a particular viewer to view works distributed on DVD disk. However, the "Content Scrambling System" (supposedly "hacked" by the authors of the program at issue in this case) performs no such check; a CSS-enabled player will view *any* CSS formatted DVD without performing any check that the user is authorized to view it.

Further, the studios are claiming a right to impose arbitrary conditions on the implementation of the CSS technology, via the license terms which they seek to impose on player manufacturers. These terms already include the implementation of a "region coding" mechanism, which is intended to prevent disks sold in one region, designated by the movie studios, from being played in another — with an obvious impact on, among other things, the ability of a purchaser to resell a work, one of the cornerstones of first sale. And nothing in the studios' interpretation would keep them from imposing further conditions, which could very well have the effect of annihilating the first sale doctrine in practice.

The copyright office, in this round of requests for comments, asks how the implementation of the DMCA has affected the first sale doctrine. We will demonstrate in this paper that the effect is already substantial, and threaten to become worse. The copyright office also asks whether additional issues should be considered. We suggest the following:

- What is required for a technical measure to be an "access control mech-

anism", and how much control does the law grant copyright holders over those mechanisms?

- Are the movie studios using the DMCA to claim statutory protections for use of their works, and not just access? Are these claims consistent with the text of the law, and with Congressional intent in passing the law?

- Does the DMCA exceed the Constitutional bounds of Congress's power to grant intellectual property rights, by granting patent-like control over "access control" processes without any time limit?

- Is there an interpretation of the law which eliminates those Constitutional issues, and statutory protections for use controls, while still providing statutory protection for strong, effective technical mechanisms which allow copyright holders to protect their works?

This paper proposes such an interpretation of the law, demonstrates that it provides statutory protection for several strong, existing protection mechanisms (including one that applies to works distributed on DVD disk), and shows that it avoids severe problems with the interpretation advanced by the movie studios.

2 Technical facts of the case

The plaintiffs in this case are most of the major movie studios in this country. This case concerns movies which they publish on Digital Versatile Disc (DVD). The process of formatting these discs includes the application of the so-called Content Scrambling System (CSS), which transforms the files containing the video and audio comprising the movie into an obscured format. The details of this obscured format, and the process of converting it to industry-standard formats (e.g. MPEG) which may then, after many further conversions, be displayed to a human viewer are licensed by the plaintiffs, via their intermediary, the so-called DVD Copy Control Authority (DVD-CCA), to player manufacturers.

2.1 CSS, and restrictions on its use

Licensees are required to obey numerous conditions on their use of the CSS technology by the terms of the non-public license. These conditions are known to include implementation of a system called "region coding", which requires a player sold in America, for example, to refuse to play discs sold for use in Europe, or vice versa. (Among other measures, a player is required to keep a permanent record of the region it resides in, and to allow this record to be changed only a small, fixed number of times without being

reset at the factory). These requirements also currently include the implementation of certain copy-control technologies designed to inhibit transfer of movies onto VCR cassettes (the so-called "Macrovision" machinery). However, the studios and their agents have acknowledged that these mechanisms are technically distinct from CSS *per se*, and bound to it only legally by the requirements of their license. They have also included among these conditions such matters as region coding, which have nothing to do directly with either access control or copy control, which comprise between them the subject matter of the DMCA. As the plaintiffs' witness, Robert Schumann stated in his second declaration:

> 23. As I also stated in my recent deposition, CSS and the decryption of it via DeCSS has nothing to do with protecting so-called regional coding or any mechanism which prevents consumers from fast-forwarding through the initial audiovisual information contained on a DVD disc (which includes copyright infringement warnings. and the like).

(Schumann supplemental declaration, June 1, paragraph 23).

The defendants in this case are distributing an unlicensed implementation of the CSS technology, called "DeCSS", which, like the licensed implementations, can take the obscured video files stored on commercial DVDs and convert them to unobscured form. This is the first of several conversions required to make these files visible to a human viewer, and is a necessary step in viewing the content on a DVD (others being conversion from a highly compressed form called "MPEG" to uncompressed digital video, formatting that digital video so hardware display drivers can process it, and the conversion of the digital data to analog signals driving an actual display; the analog signals are generally processed further within a display, but those steps are of no concern to us).

As such, DeCSS performs a function which is absolutely necessary to viewing the content on legitimately purchased DVDs to which CSS obscuration has been applied — players which would clearly serve a legitimate function. In fact, as testimony at the trial has shown, DeCSS was originally written to serve as a component of such a player (Universal v. Corley, Johansen testimony, p. 619 of the trial transcript).

2.2 The "threat" of piracy

The movie studios have claimed, in submissions in Universal v. Corley and elsewhere, that CSS is part of a copy-control regime which is necessary to prevent "piracy" (that is, unauthorized coyping) of their works, justifying that claim in part by saying that digital technology allows the creation of limitless copies without generational loss.

This piracy could conceivably take one of two forms. One would be creation of unauthorized physical copies of DVD disks, by "bootleggers";

this is alleged to be common on the Pacific Rim. However, when pressed, representatives of the movie studios have been candid in admitting that the CSS technology does nothing at all to prevent such bootlegging. For instance, consider the following exchange, at a hearing held at Stanford University by the Copyright Office, Dean Marks, a lawyer representing the movie studios' trade organization, the Motion Picture Association of America (MPAA), stated flatly in colloquy with David Carson of the Copyright office:

```
21              MR. MARKS:  A duplicated DVD disk is
22  going to duplicate the CSS encryption.
23              MR. CARSON:  And can be played on any
24  legitimate player.
                                                    PAGE 247
 1              MR. MARKS:  And can be played on any
 2  legitimate player, legitimate licensed CSS player.
 3  And not be played on non-licensed players.
 4              MR. CARSON:  Okay.  So I don't see how
 5  you're stopping the -- I don't see how you're
 6  stopping the piracies of DVDs in that respect.
 7  Pirated DVDs can be sold on the open marketplace and
 8  played in any legitimate DVD player.
 9              MR. MARKS:  Without infringement
10  copyright?
11              MR. CARSON:  No, no, no.  Certainly not.
12  But we know pirated goods are on the market all the
13  time.
14              MR. MARKS:  Yes, they are.
```

(Transcript, LOC hearing on the DMCA, Stanford University, May 19, 2000, pp. 246-247).

We will be reviewing much more of this remarkable colloquy, and will in particular be returning to Mr. Marks' intriguing focus on control of DVD players, rather than control of works on DVD. But the important point here, for the moment, is that Mr. Marks freely admits that the CSS technology does nothing to prevent unauthorized copying of disks.

But, there is another form of illegitimate copying which the movie studios routinely invoke, namely copying of their works from person to person via the Internet — a threat supposedly enhanced by the possibility of making limitless copies of a digital work without generational loss over multiple generations of copies.

However, the trial has established that this is at best, a distant threat. The volume of information on a DVD — several gigabytes — is simply too vast to transmit over even a fast, local network, let alone the far slower, wide-area links which characterize the Internet as a whole. In order to argue that such transmission is even feasible, the movie studios have had to argue that the video data on the DVDs can be compressed far further. But,

that video data is already highly compressed; as testimony at the trial has demonstrated, performing this compression with any current compression technology necessarily involves throwing away some video data entirely, and substantially degrading the quality of the video in the process. Further, expert opinion in the field of compression is that breakthroughs which will allow drastically better high-quality compression of full-motion video (as opposed to special cases, like stills where 3-D geometric data is available) is unlikely, and further progress in the field will be incremental over the next few years. (Testimony of Peter Ramadge, Universal v. Corley transcript, pp. 884-932).

So, whatever digital copies can be made are in fact, significantly degraded from the originals, despite their digital nature. Furthermore, they are by nature missing any of the "extras" which the movie studios have included on many DVDs (alternate audio tracks, etc.), which are significant selling points for the DVD over alternatives such as VHS.

And yet unlike, say, compressed audio files, they are still too large to conveniently transmit over the Internet. The compression in Prof. Ramadge's examples was to make the files small enough to fit on a conventional Compact Disk (CD), about 650 megabytes. Extrapolating from experiments performed by Ole Craig, a witness for the defense, a file the size of a CD would take more than three hours to transmit over a dedicated T1 line, to another computer which was very close in internet topology. (Craig's experiment involved transferring a 1.5 gigabyte file, which took over seven hours; prorating to the smaller file at issue here is simple arithmetic). (Declaration of Olegario Craig, Universal v. Corley)

And this T1 line is many times faster than commonly available home internet access. The effective bandwidth available through even a fast home internet connection (e.g., DSL) is generally much less. The fastest home DSL connections from Bell Atlantic (now Verizon) are 0.64 million bits per second, compared to the 1.5 million bits per second available on a T1; prorating, we find nearly an eight hour download time for a CD's worth of data. And even DSL connections are still relatively rare. The movie studios note that higher bandwidth is available to researchers at some universities, but those are for supervised research and do not go, say, to the dorms. Very few people, no matter how ill their will, would have the patience to sit still for hours to receive a poor-quality copy of a movie over the Internet, when the price for renting the high-quality original, with all its extras, is nominal.

Lastly, it is worth noting that those who desire to obtain a digital copy of the video data on DVD, for whatever reason, have other tools available (e.g., "DOD speed ripper"). At trial, the MPAA's head of antipiracy efforts, Mikhail Reider, claimed, unconvincingly, not to remember hearing of those tools (Universal v. Corley transcript, Reider testimony, p. 680), but they were clearly available before DeCSS; at trial, one of the authors of DeCSS described how he examined such a tool in the course of his work. (Universal v. Corley transcript, Johansen testimony, p. 623). Yet, while the movie studios have filed not one, but three separate lawsuits seeking to enjoin distribution

of DeCSS, in three different states, they have not taken any legal action at all against distribution of these other tools, which facilitate "Internet piracy" in the exact same manner as DeCSS.

So, DeCSS rates three lawsuits, and "speed ripper" not even one. A reasonable person might conclude that DeCSS threatens the movie studios' interests in a way that these other tools do not — and in a way other than facilitating "Internet piracy", since they're all the same in that regard.

There is, however, a significant difference — "speed ripper" relies on the CSS descrambling performed by a commercial DVD player; it works by capturing that player's output in digital form. DeCSS implements CSS descrambling itself. As regards "Internet piracy" that's irrelevant — the same results are achievable either way.

However, DeCSS does allow you to do something which "speed ripper" does not — it allows you to build a player which will render works on DVD without going to the movie studios (or their agent, the so-called DVD Copy Control Authority) for a license. Indeed, as we have already noted, testimony at the trial has established that that is why it was written, and one of the authors has received a prestigious national prize for the work. (Universal v. Corley transcript, Johansen testimony, p. 627).

It is this sort of activity — making a legitimate DVD player, not "Internet piracy" —- which will be most directly affected by a finding in favor of the plaintiffs.

2.3 The prayer for relief

The plaintiffs are suing to enjoin further distribution of DeCSS, claiming that their licensed implementations of the CSS technology provide a form of access control which is being "circumvented", or more simply, bypassed, by the unlicensed DeCSS implementation.

What makes this a peculiar claim is that there is nothing about any implentation of the CSS technology, either licensed *or* unlicensed, which would ever, in the ordinary course of the operation of CSS, deny any viewer access to the contents of any CSS-formatted DVD. If an unlicensed CSS implementation would reduce the contents of a given disc to (more) readable MPEG video data, then *any* licensed implementation would do the exact same thing. There is never any case in which the two implementations do anything different. How, then, can the plaintiffs claim that one of these things is providing an access check which is bypassed by the other?

To answer that question, let us begin by examining the law, and how it may be applied to two access control mechanisms of a sort which it is unquestionably intended to cover. Having done so, we will return to CSS, and to the contorted interpretation of the law which leads the plaintiffs to claim that CSS is providing access control despite the fact that in the ordinary course of its operation, it can *never* deny access.

3 Access controls and the DMCA

3.1 The applicable statute

The Digital Millenium Copyright Act was enacted by Congress to protect certain forms of electronic defenses which copyright holders might adopt for their works, by adding a new chapter, 12, to Title 17 of the United States Code, which defines copyright law. Two distinct types of mechanisms are protected — access controls, in section 1201(a) of the law, and copy controls, in section 1201(b). The plaintiffs' case relies on construing CSS as an "effective access control", as defined in 1201(a). So let us examine how that term is defined. In section 1201(a)(3)(B) of the law, we find that, for purposes of section 1201:

> (B) a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

If that is the case, then section 1201(a)(2) provides that

> (2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that–
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
>
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

where "circumvention" is defined in 1201(a)(3)(A) as:

> (A) to 'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner

So, "effectively control access" is defined in terms of "gain access to the work" — which is not, itself, defined in the DMCA. Seeking definitions from common language, we find that any common dictionary (e.g., Merriam-Webster) defines three senses for the word "access": it can refer to a right, a means, or an act.

The most straightforward interpretation, in context, is that the technological measure must govern the *act* of access — that is, it must, "in the ordinary course of its operation", perform some explicit test that the user is authorized by the copyright owner to view a particular work, and allow the act of viewing the work only in case that he is, in fact, authorized.

But, there are other possible readings; let us consider them. Clearly, it makes no sense to adopt the sense of "access" in which to "gain access" is to be granted the legal right to view something. That would reduce the law to nonsense; it would speak of technical means which somehow require the application of a process to a copyrighted work in order to allow a viewer to form a contract.

This leaves the interpretation in which "access" is a means, and the technical measure checks whether the viewer is using authorized means of acccessing the work. However, the technical measure itself is necessarily part of the means of access, so at the very least this reading lends a strange circularity to 1201(a)(3)(B). But nevertheless, as we shall see, that is the plaintiffs' reading. (Strangely, they seem to think this control extends over only means which employ cryptography in some way, even though the definition of "effective access control" never mentions cryptography, encryption, or decryption; of that, more anon). We will also see that this is how CSS itself is designed to function — it does not and cannot check that the user has been authorized by the copyright owner to perform the act of access — and we shall show see that this interpretation is at variance with both expressed Congressional intent in passing the DMCA, and with basic Constitutional principles regarding intellectual property protection.

But before doing that, it may be worth showing that our alternative interpretation, that "effective access controls" are restricted to measures which govern *acts* of access, does provide copyright holders with an opportunity to provide meaningful protection for their work, and that we are not trying to read the statute into nonexistence or irrelevance. So, let us examine a few examples of effective access controls under this definition.

3.2 Examples

On our reading, then, an "effective access control" is one which performs an explicit test that the viewer is authorized, and circumvention consists of bypassing, or negating the effect of, such a test, in order to provide access to a work to a person who would have been denied access "in the ordinary course of [the access control's] operation".

This is a fairly broad definition, which provides statutory protection for numerous mechanisms which the plaintiffs can build to protect their works. We will consider three.

3.2.1 Pay-per-view cable

In pay-per-view (PPV) cable case, programs are distributed to everyone in a particular cable network, but in a scrambled form. If a viewer desires to view one of these programs, then they make arrangements, including payment, with their cable provider. The cable provider then downloads a "key" for that *particular* program into that *individual* viewer's set-top box. When the program is broadcast, the set-top box applies the key to the scrambled program, obtains the program in unscrambled form, and shows it to the customer. In this scenario:

- All cable customers have set-top box hardware, but only some are authorized to view a given program.
- In the ordinary course of the system's operation, there are PPV programs which a customer can view — but only those the customer has been specifically authorized to view (by arrangement with the cable company).
- In the ordinary course of the system's operation, there are PPV programs which a customer *cannot* view — namely, those which the customer hasn't paid for. The system is performing an explicit test as to what programs a user is authorized to view, and denying access if not.
- "Circumvention" on our present reading, would consist of measures which defeat the above check, by, for instance, fooling the cable company into downloading a key when the user hasn't paid for a program, or filching keys from another customer's set-top box.

3.2.2 Circuit City Divx

Of course, in the PPV cable case, the work being protected (the pay-per-view programming) is never fixed in tangible media. But that is not essential; it would be easy to design a scheme in which players for DVD-like discs would similarly require a key to be downloaded into them in order to play the contents of a particular disc.

This mechanism would preserve the essential properties of PPV authentication which we have already discussed:

- All customers have player hardware, but only some are authorized to view a given disc.
- In the ordinary course of the system's operation, there are discs which a customer can view — but only those the customer has been specifically authorized to view (by arrangement with the central office, mediated by the player).

- In the ordinary course of the system's operation, there are discs which a customer *cannot* view, those for which payment has not been arranged. The system is performing an explicit test as to what programs a user is authorized to view, and denying access if not.

- "Circumvention" on our present reading, would consist of measures which defeat the above check, by, for instance, fooling the player into playing a disc which had not been paid for, or billing the wrong account.

A scheme along these lines was actually marketed as "Divx" by Circuit City, in conjunction by the plaintiffs; the internal technical details of the scheme were different, but it looked the same to consumers in most respects, including most notably the requirement that the player be able to phone a central office (via an internal modem) to manage billing. (There is, of course, no connection between this scheme and a video compressor, also called "Divx", which has also been mentioned by the plaintiffs).

3.2.3 Certificates

We conclude with a less widely used, but still useful, example: certificates. MIT uses this mechanism to secure web access to student records. Briefly, a "certificate" is an electronic analog to a physical ID card with a watermark or raised seal — a datum which is difficult to produce by someone without particular authority, but which anyone may easily inspect to determine that it has been produced properly. These are used in electronic communication as follows: a "certification authority" issues certificates to individuals who wish to be identified. (MIT serves as its own certification authority) They can subsequently present these certificates, via their web browsers, to a web server, which verifies that they have a proper certificate (the analog to a physical ID card with the proper seal), and may read the certificate to verify the user's identify (as a guard might read the ID card). The web server can then use the "certified" identity to determine whether or not to server a particular web page to the viewer — in the MIT case, to assure that students view only their own records.

Note that while it is common practice to encrypt data protected by the certificate mechanism, simply to protect it from potential prying eyes as it traverses the network, that does not form part of the mechanism, and we would still have effective access control without it. This will become an important point later. To summarize again:

- All MIT students can get a certificate, but only some — in fact, only the student and administrators — can view any given student's records.

- In the ordinary course of the system's operation, there are records which a student can view — but only those the student has been specifically authorized to view (usually his own).

- In the ordinary course of the system's operation, there are records programs which a customer *cannot* view — in the MIT case, other students' records.

- "Circumvention" on our present reading, would consist of measures which defeat the above check, by, for instance, forging a certificate, or convincing the web server to serve a student's records in the absence of that student's certificate.

Many other access control mechanisms besides the ones we have discussed can be imagined, which all share those properties, but we need not go into all the possibilities here. The point is that the reading of the law which we have proposed allows the plaintiffs a variety of ways, some of which have already been deployed, to protect their content.

But, our reading does not provide protection under the law for a scheme like CSS, which, as we have seen, does not discriminate between movies that a user is authorized to view and those which they are not, and *always* grants access "in the ordinary course of its operation". To argue for protection for CSS under this law, then, the plaintiffs must adopt another reading. And they have.

4 CSS, DeCSS and plaintiffs' analysis

The plaintiffs believe this case is simple and straightforward. To quote one of their attorneys, Leon Gold, in pretrial hearings:

> Circumvent means to descramble, and that's what DeCSS does. A technological measure effectively controls the access here to do the protected work and CSS is such a measure and it's designed to control access to our copyrighted works. Because CSS is an encryption technology, you've got to have a software key to open it, so CSS qualifies as an access control measure. And all of the statutory requirements are met, and defendants are clearly violating them.

Note the peculiar statement that "Because CSS is an encryption technology, CSS qualifies as an access control measure". This already indicates that the plaintiffs have adopted a somewhat strained reading of the statute. The statutory definition of "effective access control" — that an effective access control measure is one that "requires the application of information, or a process or treatment, with authority of the copyright owner, to gain access to the work" — makes no specfic reference to encryption. Instead, as we shall discuss in detail, it requires that the technological measure so described have a particular *effect*. As we have already seen, it is perfectly possible to have an access control measure which does not encrypt the work it protects;

conversely, it is possible to employ encryption technology for purposes such as electronically signing documents, which have nothing to do with access control.

But rather than relying on Mr. Gold's perhaps hasty and off-the-cuff remarks, let's examine a more elaborate version of this argument, from the colloquy between David Carson and Dean Marks at the Stanford LOC hearing, concerning the notion of "authority" which is crucial to the statutory definition of "effective access control":

MR. CARSON: Are [DVD buyers] authorized to view [their DVD] on any machine they can find, that they can make to view it?
MR. MARKS: No, no. They're authorized to view it on a licensed device. If someone were to buy a VHS cassette, and they didn't have a VHS player, are they authorized to disassemble the videocassette, reproduce the film in there in 35-millimeter print and play it on their movie camera? I don't think so.

PAGE 249

MR. CARSON: Okay. But, first of all, there's no contractual privity between the purchaser of that DVD and Time Warner, I assume. There's no shrink-wrapped license. You know, you don't sign a license saying, "I agree only to play this on an authorized player," when you purchase the DVD.
MR. MARKS: That's correct. And neither is there a shrink-wrapped license when you buy a VHS cassette that's in NTSC format, and you only have a PAL player.

(Transcript of LOC hearing at Stanford, pp. 248-249).

So purchasers of a DVD are not entitled to view their DVD "on any machine they can ... make", but *only* on "a licensed device". But that is not due to any contractual obligation they personally have entered into, but due to the DMCA. However, once you have an authorized player, you are *guaranteed* to be able to play a given DVD; the player performs no authorization checks.

Note that the terms in which this is couched are rather different than in our analysis above — they speak, for instance, not of authorized *viewers*, who may or may not be authorized to view a particular movie, but rather of authorized *players*, which, if authorized, may play any DVD.

What makes such a player authorized is, in the plaintiffs' view, the CSS license. If removal of the CSS obscuration is done by a *licensed* player, then the player has the authority of the copyright owner, and is therefore authorized. However, if the *exact same process* is performed by a player

which was created by someone without a license, then it is unauthorized, and therefore circumvention, never mind that the two processes have the exact same effect.

Note also, that it is the manufacturer of the player who must be licensed in this view — CSS licenses are not required of individual viewers, nor even, in the usual case, available to them. This system is not about controlling the access of individuals to DVDs; it is rather used to control (via the CSS licensing requirement) who may create players for them.

This is how our reading of the statute differs from that of the plaintiffs. We read the "authority of the copyright owner" to be the authority of a given *user* to view a *particular work*. But in the case of CSS, the copyright owners are claiming the right to control how, or whether, a particular piece of *equipment* performs a particular *process*.

It should be noted that the plaintiffs go on to state that this control only applies to "access control processes", and they sometimes go on to state that CSS fits that description because it is "an encryption process". Of which, more anon.

5 Problems with plaintiffs' analysis

There are a number of problems with the plaintiffs' assertion of a right, stemming from 1201(a), to vet the application of certain processes to their content. The legislative record is clear that Congress did not mean to create such a right, on the part of the defendants, and indeed amended the bill to avoid such an interpretation. Also, there are some basic Constitutional problems with this new exclusive right to vet implementations of an access-control process, which simply do not arise if the statute is read, as it seems clear that Congress intended, simply to give copyright holders the right to control access (and sue only when access was or might be provided to an unauthorized viewer).

5.1 Conflicts with the First Sale doctrine

In the spirit of the LOC's request for comments, let us first consider how the plaintiffs' interpretation of the DMCA relates to the First Sale doctrine, codified at 17 USC 109. This section of the copyright laws governs what rights are transferred to the purchaser of a published work, in the absence of a contract with the copyright owner (which clearly does not exist in the case of DVDs). It states that when a copy of a published work is sold, the purchaser acquires all rights other than those listed in 17 USC 106 as exclusive rights of the copyright owner. In fact, 17 USC 109(c) specifically provides that the right to privately display the work is transferred.

In other words, the first sale doctrine states that when a published work is sold, the coypright owner voluntarily parts with the rights of control asso-

ciated with ownership of a copy, and the purchaser of the DVD acquires the right to display the work to an audience in the physical presence of the copy. Since display inherently requires the act of access if the work is scrambled, the right of access is part of the larger right to display — authority over which, once again, the copyright holder has voluntarily surrendered at the point of sale.

However, as we have seen, the movie studios claim that this rule no longer applies in the case of DVDs. They believe that they retain authority over how a work on DVD may be lawfully displayed, because that display is only lawful when it is performed, in Mr. Marks' words, on "a licensed device" — licensed by them, via their agents, the DVDCCA — despite the failure of the studios and their agents to ever announce this requirement to the DVD purchaser. And if all such devices implement some measure which restricts use of a work, such as region coding which prevents viewers from viewing a disk which they purchased in Europe, then the viewers have no lawful alternative way to access the content on the DVDs which they purchased. This obviously impacts the scope of possible resale, one of the rights traditionally acquired by the purchaser under the first sale doctrine. And the scope of further restrictions that might be imposed in the future is limited only by the studios' imaginations in drawing up their license.

In his colloquy with Mr. Carson of the LOC, Mr. Marks acknowledged that "the technological protection measure is not only dealing with access, but also with subsequent uses of the content" (transcript of the LOC hearing at Stanford, p. 261). (Representatives of libraries, universities and the public objected at those proceedings to the imposition of persistent use controls in the guise of 1201(a) access controls).

This analysis presumes that there is no contract which would alter the terms of sale of the published work, but in the case of DVDs, that is uncontested. See, for instance, Mr. Marks, representing the MPAA, once again in colloquy with Mr. Carson of the LOC:

```
1              MR. CARSON:  Okay.  But, first of all,
2  there's no contractual privity between the purchaser
3  of that DVD and Time Warner, I assume.  There's no
4  shrink-wrapped license.  You know, you don't sign a
5  license saying, "I agree only to play this on an
6  authorized player," when you purchase the DVD.
7              MR. MARKS:  That's correct.
```

(Stanford LOC hearing transcript, p. 249).

An alternative reading of the situtation, of course, would be that the first sale doctrine still applies, and that the movie studios have surrendered their right to control private viewing at the sale of a DVD. Note that if surrendering display rights as per first sale is not to the taste of certain copyright owners (including, evidently, the movie studios), the law does give them an option: they may license, rather than sell their works, as is commonly done with software, pursuant to an explicit license agreement which imposes whatever

additional restrictions are to their taste; contract law, then, rather than copyright law should apply. And such a model of sales would impose scant burden on the studios; following the practice of software shrink-wrap license agreements, they can simply notify the buyer of the contract in a prominent way, and allow the purchaser to return the work if they don't agree with the terms. In fact, there is precedent for exactly that arrangement with the "DivX" pay-per-view scheme for controlling DVDs, which did require the consumer to sign an explicit contract.

Incidentally, the prospect of communicating restrictions by license agreement could largely eliminate apparent conflict between 17 USC 109, the First Sale doctrine, and 17 USC 1201, the anticircumvention provisions of the DMCA. If a copyright owner wants to exercise their right to control access to a published work via technical measures, granted by 1201, all the First Sale doctrine requires is that they provide a license agreement in a manner which notifies the purchaser of the restrictions on what they have purchased, and allow for returning the product if they don't like the terms. That seems only fair.

But, on the studios' reading of the law, such a conflict clearly exists.

5.2 Encryption not required for access control; any process could be regulated

To summarize where we have arrived: the movie studios have adopted a reading of the law which allows them a patent-like control over processes which are required to gain access to their works — that is, once again, that the law is meant to give them control over not just the *act* of access, but the *means*. They are suing because DeCSS threatens to allow DVD purchasers to develop their own technologies and devices – competing DVD players – to access the works they have purchased.

When asserting this control, in court and elsewhere, the studios and their representatives are always careful to qualify it, by saying that this right to authorize means of access extends only to "access control processes", and not other kinds of processes. For instance, as we have seen, they have been careful to state in court that CSS is an access control process because it uses cryptography (a debatable position in and of itself, once the nature of that cryptography is analyzed, as we have seen).

However, no support for this assertion may be found in the statute. Neither the definition of access control nor that of circumvention in 1201(a) requires any particular structure of the access control mechanism, or the nature of the measures used to circumvent it. The definition of "effective access control" states simply that an effective access control must "require the application of information, or a process or a treatment, with the authority of the copyright ower, to gain access to the work"; there is no restriction on the technical means by which this requirement is met. And while the definition

of circumvention discusses descrambling and decryption, it also encompasses any other technique which allows a user to "avoid, bypass, remove, deactive, or impair a technological measure", again with no restriction to particular technical means.

Also, the studios use the terms "decrypt" and "descramble" interchangably, but standard rules of statutory construction tell us that different words apply to different things, and the range of technological measures which may be described as "scrambling" is so broad that it is no restriction in practice. For instance, we have already mentioned the MPEG compression process which is used on DVD video even without CSS. This process is intended solely to compress the data, with no pretense of access control. Yet, the compression process involves throwing away some of the data and thoroughly scrambling the rest, and intensive computation is required to "descramble" it back to ordinary digital video.

Lastly, let us note that there are real, deployed examples of access control (certificates, as discussed earlier) where the use of encryption, if any, is wholly incidental, and not a part at all of the access control provided. You *can* have access control without encryption — and the movie studios' reading would have the bizarre effect of denying such systems protection under the law.

In short, the notion that the law is restricted to processes which are somehow cryptographic is fallacious. If the law actually grants the movie studios the authority they claim, then they could exercise that authority over *any* process which is necessary to gain access to one of their works, such as, for instance, a video compression algorithm. Thus, they would secure the benefits of a patent on that process without meeting any of the requirements (originality, protection for a limited time), a point to which we shall return.

5.3 Access controlled is access to a market, not access to a work

Another problem with the studios' analysis is that, contrary to the letter of the statute, they are not using CSS to control access to works. As we have noted already many times, any DVD will play in any DVD player. What they are using it for is to impose conditions on the manufacture of players — some of which have to do with the goals of the DMCA (e.g., imposition of Macrovision copy control), and some of which simply do not (e.g., region control).

In other words, the studios are asserting that the DMCA gives them the right to control access into the market for DVD players, by requiring anyone who builds a player to enter into a license agreement, to which they can attach arbitrary terms.

Again, it is interesting to observe the colloquy of Mr. Carson of the LOC, and Mr. Marks, representing the MPAA, on this point. Mr. Carson began by noting that CSS, as described by Mr. Marks, had nothing to do with

access control as he (correctly) understood it:

> It strikes me that what we are describing is perhaps a copying control device in access control clothing. In other words, you've got a device that controls access to a work, but not in the way that, certainly before this rulemaking began, I thought we were talking about. We were talking about access control devices.
>
> In other words, I assumed -- naively, perhaps -- that a technological measure that controls access to a work, the purpose of that is to make sure that authorized users and only authorized users are getting access to the works. So if I paid the price to the copyright owner otherwise be able to use that work, then I'm entitled to use it.
>
> And if he somehow gets access to it by circumventing encryption or passwords, or whatever, then she's in trouble because she's not an authorized user. I'm not in trouble because I am. That's got nothing to do, as far as I can tell, with what you're talking about.

(LOC hearing transcript, p. 245)

Here is what Mr. Marks had to say in response:

> MR. MARKS: I think it's partially a fair description. I think it is also used -- the fact that the work is encrypted is used to try and guarantee that the user has legitimately -- has legitimate access to the work as well. I mean, I don't think it's completely devoid, the CSS system, of trying to ensure that those people that -- for example, would just simply duplicate the DVD disks -- you know, pirates who would duplicate the DVD disks.
>
> And if there were pirate players that were unlicensed, they wouldn't be able to play those disks because they were encrypted with CSS. That serves an access control function as well.

(LOC hearing transcript, p. 246)

So, Mr. Marks suggests two "access control" functions for CSS. One of these functions is, in fact, copy control, not access control; the other has to do with "pirate" players. Furthermore, Mr. Marks immediately admitted that CSS does not, in fact, have anything to do with copy protection, per se, returning once again to players:

> MR. CARSON: But a duplicated --

MR. MARKS: A duplicated DVD disk is going to duplicate the CSS encryption.
MR. CARSON: And can be played on any legitimate player.

PAGE 247

MR. MARKS: And can be played on any legitimate player, legitimate licensed CSS player. And not be played on non-licensed players.

(LOC hearing transcript, pp. 246-247)

So, the only "access control" function served by CSS is, by Mr. Marks own testimony, regulation of the player market — specifically, restricting it to "licensed players". Where a licensed player, of course, is one whose manufacturer agreed to the full terms of the CSS license agreement — terms which, like region controls, may have absolutely nothing to do with the purposes of the DMCA. And later, when Mr. Carson asked what defined an "authorized user", in the view of Time Warner, Mr. Marks replied that that was *anyone* who had legal possession of a DVD and a licensed player (the only legal kind of player, in the MPAA's view):

[MR. CARSON:] In other words, there's no reason to believe as a general proposition that someone who has a commercially manufactured and marketed DVD, manufactured by Sony, perhaps, or any of the major studios -- Time Warner, whatever -- is not an authorized user.

PAGE 248

If someone has that DVD which is manufactured by Time Warner, you're going to presume they're an authorized user, aren't you?
MR. MARKS: Yes. Although you'd have to sort of define what you mean by authorized user. If someone has purchased a DVD from Time Warner, they're authorized to play it on a licensed DVD player. They can play it as many times as they want, there's no restriction on saying it's a one-time play, it's a two-time play.

(LOC transcript, pp. 247-248)

So, again, Mr. Marks makes plain that CSS has nothing with do with seeing whether a given *user* gets to see a movie — if they have the disk, CSS will allow any licensed player to play it for them. The sole "access control" function of CSS, on Mr. Marks' own explicit testimony, is to restrict DVD playback to "licensed" players — i.e., those whose manufacturers have agreed to abide by the movie studios' restrictions, whatever they may be.

Before the passage of the DMCA, this would have been somewhat questionable; indeed, it has at least the appearance of an illegal tying arrange-

ment. But that is not what we wish to investigate here — we simply wish to know if this is the sort of arrangement that Congress meant to protect when they passed this law. So, let us see.

5.4 Inconsistent with Congressional intent

The legislative history, unsurprisingly, does have something to say about how Congress envisioned the relationship between the copyright holders and makers of players for their works. Both houses of Congress wanted to maintain the rule established in the Betamax case, that any device with a legitimate purpose was legal, and that the copyright holders not be able to decide among themselves what constituted a legitimate purpose. Sen. Ashcroft, in the Senate:

> In discussing the anti-circumvention portion of the legislation, I think it is worth emphasizing that I could agree to support the bill's approach of outlawing certain devices because I was repeatedly assured that the device prohibitions in 1201(a)(2) and 1201(b) are aimed at so- called "black boxes" and not at legitimate consumer electronics and computer products that have substantial non-infringing uses. I specifically worked for and achieved changes to the bill to make sure that no court would misinterpret this bill as outlawing legitimate consumer electronics devices or computer hardware. As a result, neither section 1201(a)(2) nor section 1201(b) should be read as outlawing any device with substantial non-infringing uses, as per the tests provided in those sections.
>
> If history is a guide, however, someone may yet try to use this bill as a basis for initiating litigation to stop legitimate new products from coming to market. By proposing the addition of section 1201(d)(2) and (3), I have sought to make clear that any such effort to use the courts to block the introduction of new technology should be bound to fail.
>
> As my colleagues may recall, this wouldn't be the first time someone has tried to stop the advance of new technology. In the mid 1970s, for example, a lawsuit was filed in an effort to block the introduction of the Betamax video recorder. I think it useful to recall what the Supreme Court had to say in ruling for consumers and against two movie studies in that case:
>
> > One may search the Copyright Act in vain for any sign that the elected representatives of the millions of people who watch television every day have made it unlawful to copy a program for later viewing at home, or have enacted a flat prohibition against the sale of machines that make such copying possible.

> As Missouri's Attorney General, I had the privilege to file a brief in the Supreme Court in support of the right of consumers to buy that first generation of VCRs. I want to make it clear that I did not come to Washington to vote for a bill that could be used to ban the next generation of recording equipment. I want to reassure consumers that nothing in the bill should be read to make it unlawful to produce and use the next generation of computers or VCRs or whatever future device will render one or the other of these familiar devices obsolete.

(Congressional record, 14 May 1998, p. S4890).

Which was echoed on the other side of the aisle; here are remarks from Rep. Klug, in the final debate on the Conference Committee bill:

> Both of these changes share one other important characteristic. Given the language contained in the Judiciary Committee's original bill, specifically sections 1201(a)(1), (a)(2), and (b)(1), there was great reason to believe that one of the fundamental laws of copyright was about to be overruled. That law, known as Sony Corporation of America v. Universal Studios, 464 U.S. 417 (198), reinforced the centuries-old concept of fair use. It also validated the legitimacy of products if capable of substantial non-infringing uses. The original version of the legislation threatened this standard, imposing liability on device manufacturers if the product is of limited commercial value.
>
> Now, I'm not a lawyer, but it seems irrational to me to change the standard without at least some modest showing that such a change is necessary. And, changing the standard, in a very real sense, threatens the very innovation and ingenuity that have been the hallmark of American products, both hardware and content-related. I'm very pleased that the conferees have meaningfully clarified that the Sony decision remains valid law. They have also successfully limited the interpretation of Sections 1201(a)(2) and (b)(1), the "device" provisions, to outlaw only those products having no legitimate purpose. As the conference report makes clear, these two sections now must be read to support, not stifle, staple articles of commerce, such as consumer electronics, telecommunications, and computer products used by businesses and consumers everyday, for perfectly legitimate purposes.

(Congressional Record, 12 Oct. 1998, p. H10621)

But, might it change things if a player manufactured without the cooperation of the copyright holders exposed their works to the possibility of unauthorized duplication? The answer, as clearly envisioned by Congress, is no; they even amended the law to try to preclude such an interpretation.

Sen. Ashcroft, again, in the immediate continuation of the speech quoted above:

> Another important amendment was added that makes clear that this law does not mandate any particular selection of components for the design of any technology. I was concerned that this legislation could be interpreted as a mandate on product manufacturers to design products so as to respond affirmatively to effective technical protection measures available in the marketplace. In response to this concern I was pleased to offer an amendment, with the support of both the Chairman and the Ranking Member of the Committee, to avoid the unintended effect of having design requirements imposed on product and component manufacturers, which would have a dampening effect on innovation, and on the research and development of new products. Accordingly, my amendment clarified that product designers need not design consumer electronics, telecommunications, or computing products, nor design and select parts or components for such products, in order to respond to particular technological protection measures.
>
> This amendment reflects my belief that product manufacturers should remain free to design and produce consumer electronics, telecommunications and computing products without the threat of incurring liability for their design decisions under this legislation. Nothing could cause greater disaster and a swifter downfall of our vibrant technology sector than to have the federal government dictating the design of computer chips or mother boards. By way of example, during the course of our deliberations, we were made aware of certain video boards used in personal computers in order to allow consumers to receive television signals on their computer monitors which, in order to transform the television signal from a TV signal to one capable of display on a computer monitor, remove attributes of the original signal that may be associated with certain copy control technologies. I am acutely aware of this particular example because I have one of these video boards on my own computer back in my office. It is quite useful as it allows me to monitor the Senate floor, and occasionally ESPN on those rare occasions when the Senate is not in session. My amendment makes it clear that this legislation does not require that such transformations, which are part of the normal conversion process rather than affirmative attempts to remove or circumvent copy control technologies, fall within the proscriptions of chapter 12 of the copyright law as added by this bill.

(Congressional record, 14 May 1998, pp. S4890-S4891).

In this example, Sen. Ashcroft cites a device which actually bypasses a technical protection measure as *not* actionable circumvention under the law, because the end effect is not to provide a work to an unauthorized person. (The amendment to which Ashcroft refers was codified as 1201(c)(3)).

In these quotes and others, Congress was expressing a clear intent that the DMCA *not* be used as a club for copyright owners to dictate how products like computers, programs, and DVD players could be designed — an intent that was echoed in the House debate (by Klug and others), and carries straight through to the Conference Committee report:

> Persons may also choose to implement a technological measure without vetting it through an inter-industry consultative process, or without regard to the input of affected parties.

(Congressional Record (House), 8 Oct. 1998, p. H10065)

Note here that copyright owners are specifically denied the right to vet and approve implementations of their access control measures. In fact, they go on to stress that such reimplementations are allowed to suppress incidental effects, if that's needed for usability:

> Under such circumstances, such a technological measure may materially degrade or otherwise cause recurring appreciable adverse effects on the authorized performance or display of works. Steps taken by the makers or servicers of consumer electronics, telecommunications or computing products used for such authorized performances or displays solely to mitigate these adverse effects on product performance (whether or not taken in combination with other lawful product modifications) shall not be deemed a violation of sections 1201(a) or (b).

(Congressional Record (House), 8 Oct. 1998, p. H10065)

This makes plain that the *only* protection afforded under 1201 is against products which perform circumvention per se — for 1201(a), that would be actually allowing unauthorized access — and not for whatever incidental effects an access control mechanism might have or perform. Other Congressmen made similar remarks, and some were even more emphatic than the ones I've quoted so far. Here's Sen. Kohl, speaking before the floor vote on the Conference Committee's final bill:

> [1201(c)(3)] reflected my belief that product manufacturers should remain free to design and produce the best, most advanced consumer electronics, telecommunications, and computing products without the threat of incurring liability for their design decisions. Creative engineers–not risk-averse lawyers–should be principally responsible for product design.

(Congressional Record (Senate), 8 Oct. 1998, p. S11888)

5.5 Inconsistent with other provisions of the DMCA

We might also note that the injunction sought by the plaintiffs in Universal et al. v. Corley would harm some fields of activity specifically protected by the DMCA.

Cryptographic research, for example, is the study of security systems and their failures; to the extent that CSS qualifies as an access control mechanism, or security system, at all, it is clearly a fit subject for such research. And it is a field of endeavor granted specific protections in the DMCA, as 1201(g). However, that research can only proceed if the researchers are allowed to communicate precise descriptions of the system, its components, and its operation — and it is exactly that communication, in the form of computer source code, which the plaintiffs are seeking to enjoin.

The movie studios' interpretation is also somewhat difficult to reconcile with the provisions for reverse engineering in the Act. The whole point of reverse engineering, as it is ordinarily practiced, is to allow an engineer to discover features of a system or product which its manufacturer has chosen not to disclose, in order that the engineer can design a device with similar functions without having to license the relevant details from the manufacturer. But if a license is required for the engineer's product to be legal anyway, why protect the process of reverse engineering?

5.6 Inconsistent with Constitutional principles

Finally, the movie studios' claimed rights of access control break the constitutional balance between the copyright holder's limited monopoly and public access to information. What they are claiming, once again, is a patent-like power to regulate the manufacture of players which perform their "access control" process, allowing them to retain control over the use of content they are ostensibly publishing. Constitutional enabling language for both patents and copyrights (in Article I, Sec. 8) grants Congress the power ...

> To promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their respective writings and discoveries.

This has traditionally been interpreted as restricting the power of Congress to create exclusive rights for authors and inventors in several ways:

- The protection granted must extend "for a limited time".
- The form of protection must be appropriate — authors are granted protections for expressive content of their works, but not functional elements, and inventors protection for functional elements of their inventions, but not expressive content.

- The form of protection granted must in some way promote "the progress of science and the useful arts". Traditionally, authors and inventors have received exclusive rights in exchange for public disclosure, through fair use rights in copyrighted works or the enabling disclosure of a patent application

The access-control right fails the first two of these tests flat — there is no time limit; more strangely, in this case, we have authors (copyright holders) claiming an exclusive and perpetual right to the functional elements of a "process or treatment" which is applied to their work — clearly an invention.

5.7 Abuse of paracopyright

Lastly, even if we accept that studios have been granted a patent-like right to control the implementation and use of CSS, in perpetuity, the courts have long held that there are limits to the scope of such grants, based on a long history of jurisprudence which states that in order to fulfill its Constitutional purpose, the monopoly grant provided by laws is limited tightly to the actual intellectual property.

The basis of this jurisprudence is not the antitrust laws, but the Constitution itself. Indeed, as the Supreme Court ruled in Morton Salt (quoted below) the question of antitrust violation *per se* is irrelevant; what matters is the public purpose underlying the intellectual property grant. Morton Salt stated this rule for patents; several circuits have extended the principle to copyrights; it is clear that similar limits should apply to whatever new "paracopyright" rights were granted by the DMCA. And in already tying CSS to mechanisms like region coding — a mechanism whose explicit, designed purpose is restraint of trade between the regions — the studios are clearly exceeding the bounds.

The studios' representatives admit and relish the tying between movies and players, as the numerous quotes about "authorized" and "licensed" players clearly show; the whole purpose of the CSS licensing regime is to impose restrictions on the players. As Mr. Marks testified at the LOC hearing:

```
 6              Those devices, whether they be players
 7  or personal computers or the Sony PlayStation who
 8  would like to have their devices be able to display
 9  and play back those DVD disks need to get a license
10  to be able to decrypt the CSS encryption system.
11  They do that by going to the DVD-CCA and applying
12  for a CSS license.
13              That CSS license gives them the keys and
14  tools to be able to decrypt the disks.  It also
15  imposes certain conditions on what the device can do
16  with the content once it is decrypted.  One of those
```

```
17  obligations, for example, is that the content is not
18  allowed to flow out in the clear on a digital
19  output.
```

(LOC hearing transcript, p. 242). The collective market power of the movie studios in the DVD market is obvious and undisputed. Through contractual arrangement with the DVD-CCA, the studios have formed a trust which seeks to force an unwanted licence on all prospective members of the DVD player market. This is as obvious a case of tying as one can imagine. The collective force of the trust of all movie studios has subordinated an entirely new technology market under the guise of access authorization.

"First, as to antitrust liability, case law supports the proposition that a holder of a patent or copyright violates the antitrust laws by 'concerted and contractual behavior that threatens competition.' " Image Technical Services Inc v. Eastman Kodak Co, No. 96-15293, (9th Cir. 8/26/97).

The problem becomes clear when we read the statute's requirement for the authorization of "the" copyright owner. Setting aside the "which came first, the access or the device" question, if each studio were to market its access authority independently, no trust would exist and there would not be a problem. However, through collusion the Copyright Act is subverted. The MPAA authorization model provides authority not from the copyright holder of the individual movie, but rather from a single entity which speaks for the entire trust of all movie studios. Copyright holders not acting as part of a trust might disagree on whether and end user could create unencrypted copies for certain purposes. If the MPAA model does not create a trust, how can can authorization be coherently defined when different copyright holders make different determinations on authorization in a common protection scheme.

The industries' desire for standardization cannot serve as the escape hatch here. The true intent of the DMCA was to allow First Sale to be taken for the keys to encrypted works. These keys could easily be placed in a variety of standardized players without the need for a trust that would drive restrictive conditions and expensive prices to all would be player developers.

It is commonplace for encryption algorithms to be openly distribution and yet the keys they use to remain proprietary. In fact, this is the prefered model for the field, because it is widely acknowledged that trying to keep the alogorithm secret is doomed to failure. So-called "security through obscurity" is a "beginners mistake", in the words of the expert witnesses for the defense.

While a violation of antitrust laws is sufficient, it is not strictly necessary for a defense to an intellectual property violation, as argued persuasively in Lasercomb v. Reynolds:

> A patent or copyright is often regarded as a limited monopoly – an exception to the general public policy against restraints of trade. Since antitrust law is the statutory embodiment of that public policy, there is an understandable association of antitrust law with the misuse defense. Certainly, an entity which uses

> its patent as the means of violating antitrust law is subject to a misuse of patent defense. However, Morton Salt held that it is not necessary to prove an antitrust violation in order to successfully assert patent misuse:
>
> "It is unnecessary to decide whether respondent has violated the Clayton Act, for we conclude that in any event the maintenance of the present suit to restrain petitioner's manufacture or sale of the alleged infringing machines is contrary to public policy and that the district court rightly dismissed the complaint for want of equity." 314 U.S. at 494. See also Hensley Equip. Co. v. Esco Corp., 383 F.2d 252, 261 & n. 19, amended on reh'g, 386 F.2d 442 (5th Cir. 1967); 8 Walker on Patents, at 28:33.
>
> So while it is true that the attempted use of a copyright to violate antitrust law probably would give rise to a misuse of copyright defense, the converse is not necessarily true – a misuse need not be a violation of antitrust law in order to comprise an equitable defense to an infringement action. The question is not whether the copyright is being used in a manner violative of antitrust law (such as whether the licensing agreement is "reasonable"), but whether the copyright is being used in a manner violative of the public policy embodied in the grant of a copyright.

Morton Salt expressed the Supreme Court's view on misuse of patents, which Lasercomb translated into copyrights. It is only since the rise of copyrighted computer programs that misuse of copyright has gotten attention. Still, Lasercomb's perspective has subsequently been endorsed by the 5th Cirtuit as well, eg Alcatel USA v. DGI Technologies, No. 97-11339, (5th Cir. 1999). When the Lasercomb standard is take together with that of Morton Salt, a comprehensive statement covering intellectual property can be formed:

The grant to the creator of the special privilege of a intellectual property grant carries out a public policy adopted by the Constitution and laws of the United States, "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors ... the exclusive Right ..." to their original works and novel inventions (United States Constitution, Art. I, section 8, cl. 8). But the public policy which includes original works and inventions within the granted monopoly excludes from it all that is not embraced in the original expression or novel invention. It equally forbids the use of the intellectual property grant to secure an exclusive right or limited monopoly not granted by the Copyright or Patent Office and which it is contrary to public policy to grant.

Interestingly enough, the judicial origin of intellectual property misuse is traced by James A.D. White in his article "Misuse or Fair Use: That is the Software Copyright Question" (Berkeley Technology Law Journal 12-2, Fall 1997) to a Supreme Court case strikingly similar to the one at hand.

> The doctrine of intellectual property misuse first arose in the early 1900s in conjunction with the use of patents. In the 1917 case of Motion Picture Patents v. Universal Film Mfg. Co. [243 U.S. 502 (1917)], the patentee licensed its patented movie projector on the condition that the film used in the machine must be purchased from the patentee (a type of tying arrangement). The Court found that:
>
> > [S]uch a restriction is invalid because such a film is obviously not any part of the invention of the patent in suit; because it is an attempt, without statutory warrant, to continue the patent monopoly in this particular character of film after it has expired, and because to enforce it would be to create a monopoly in the manufacture and use of moving picture films, wholly outside of the patent in suit and of the patent law as we have interpreted it.
>
> In short, the Court denied relief to the patentee because the licensing restrictions attempted to extend the scope of the film projector patent into the unpatented area of film.

The same logic applies to the studios' use of CSS on movies. Were it confined to assuring that the consumer purchased the descrambling key before viewing the work, there might not be a problem. However, just as in Motion Picture Patents, the intellectual property rights to the work are tied not just to the key, but to full blown players which implement additional technology that is not part of the monopoly grant. Further this technology can only be obtained, according to the MPAA, subject to the DVD-CCA licence which contains anticompetitive terms that attempt to restrict end-users from reverse engineering it and prevent public disclosure of the ideas it contains. Both restrictions violate 17 USC 102(b) which forbids copyright protection to "ideas" or "methods of operation".

The reasoning from 1917 is timeless. These restrictions are invalid because a player is obviously not any part of the creation of the intellectual property in suit; because it is an attempt, without statutory warrant, to extend the intellectual property monopoly in this instance movies on DVD, beyond the scope and duration statutorily protected, and because to enforce it would be to create a trust in the licencing and use of DVD players, wholly outside of the intellectual property in suit, and hence beyond the reach of intellectual property laws as the Supreme Court has interpreted them.

5.8 These problems inhere only to the studios' reading

It is noteworthy that the problems discussed above largely go away when the statute is read, as seems clear it was intended, to protect only measures

which test whether a user is authorized to view a particular work, and only to the effect that copyright holders can sue if such a test is subverted, not if it is performed correctly by a device which they have not licensed. In this reading, the law becomes reflective of the expressed Congressional intent, not completely at variance with it. And the law is no longer seen as granting exclusive rights over any process to copyright holders. No such grant is necessary to protect legitimate access control; Congress can ban circumvention tools without granting exclusive rights to manufacturers of access controls just as they can ban burglary tools without granting a new form of intellectual property right to locksmiths.

6 Consequences of adopting plaintiffs' reading

We have argued so far that the studios' reading of the DMCA is at odds with the text of the statute itself, with legislative intent, and with the Constitution. However, if they were to prevail in their lawsuit, it would establish a precedent which would, in the long run, be enormously harmful to the public interest. To see this, let us examine what rights the studios are claiming in this case, and consider what similar claims they might make in the future.

6.1 Imposition of arbitrary use controls on work, via license restrictions

To begin with, the movie studios are claiming a monopoly right to vet and approve implementations of the CSS process, a process which is necessary to render the video from any DVD (deriving this supposed right from the notion that CSS is an "access control" process, even though it does no more to check that the viewer of a given disk is in any sense authorized than do any of the other, numerous processes such as MPEG decompresssion which are necessary to achieve the same end). To put the matter simply, it is not possible to build a useful DVD player — one which will render the movies on any of the DVD disks commonly sold in stores — which does not perform the CSS process. (One could build a DVD player which did not do CSS, but it would not render the vast majority of current DVD titles, and would be very little use in the usual role of such a player in home entertainment). So, if the studios succeed in their case, it will not be possible to build a useful DVD player without a license.

And, while the fee for these licenses is (so far!) nominal, and they have been given out (so far!) to anyone who was willing to agree to the terms of the license, there is a catch — namely, the terms of the license, which already impose conditions which many might find obnoxious.

One such condition, for instance, is the implementation of the "region

coding" mechanism, by means of which the studios mark certain disks as intended for particular markets, so that a DVD sold in the United States, for instance, is not supposed to be playable in Brazil. Many people (not excepting Americans, who are not supposed to be able to view disks sold in Europe!) might find this to be an obnoxious restriction. Indeed, in Europe, there is already a substantial market for DVD players without region control, and for kits to disable the region control mechanism in DVD players. This region coding mechanism has nothing to do with either access control or copy control, the two nominal rights provided by copyright holders under the DMCA. Yet, the studios are using their supposed right to license the CSS mechanism as a club to force player manufacturers to adopt it.

And there is nothing in the studios' reading of the law to prevent them from imposing even more restrictions on CSS licensees in the future, which, if translated into mechanisms such as region coding, would be translated directly into controls of the use of their works by the consumer. In effect, the studios would have bootstrapped the access control power, which they were given by Congress into a power to control the *use* of their works, which they were denied. And they would have reestablished the end-to-end control of the chain through which their works are distributed which they lost decades ago in U.S. v. Paramount — they would not directly control the players in peoples' homes, but they would have so much control over what those players were allowed to do that the effect on the public interest would be as severe as if they did.

6.2 Economic control of the player market

Likewise, while the studios are not charging excessive fees or discriminating against potential licensees now, there is nothing in their reading of the law to prevent them from doing so in the future, thereby allowing them to pick and choose among potential licensees. They would have bootstrapped the "access control" power into power to control the design of products which play their works — another power which Congress specifically denied them.

In short, if the movie studios are allowed to impose arbitrary terms in the CSS license, and to require such a license as a condition of legal manufacture of players for their work, they would have acquired a power of enormous scope, of immense value to them, but hugely inimical to the public interest.

7 Conclusion

The law regarding intellectual property protection in the United States has always stressed a balance of interests, between, in particular, copyright holders and the general public. This theme of balance was kept carefully in mind by Congress as they deliberated over and enacted the DMCA — in particular, it is a theme of the Congressional debates, repeated over and over, that the

ban on "circumvention" devices would be narrow, would cover only devices specifically designed to grant unauthorized access, and would not cover any device with a legitimate purpose.

The interpretation of the law adopted by the MPAA stands this balance on its head. The movie studios are asserting an absolute right to control the manufacture of *any* machinery which is capable of viewing their CSS-protected works, specifically including the LiViD project, whose sole purpose is in fact producing a player functionally equivalent to those already commercially available for Windows and Macintosh computer systems. And they are already using this power to restrict the options available to the general public (by making players artificially unable to view films from outside "region 1", the U.S. and Canada), and so to artificially restrain trade. This is not about piracy, it is about control. It should not, and cannot stand.