Response to U.S. Copyright Office Post-Hearing Questions

Submitted by
Martine Courant Rife, JD, PhD
Writing in Digital Environments Research Center Affiliate Researcher, Michigan State University
Professor, Lansing Community College
7805 N. Gregory Rd.
Fowlerville, Michigan 48836
h517/2230168::c517/2940895::w517/4839906
martinerife@gmail.com
July 10, 2009

U.S. Copyright Office Question: "Please explain whether the legal consequences of using capture software differ from the legal consequences of using a digital video camera (with particular reference to 17 U.S.C. § 1201)."

Legislative Intent and the CSS Dilemma

In order to properly answer this question, we should revisit the original legislative intent of the DMCA. Section 1201 clearly divides two types of circumventing behavior, circumvention for purposes of gaining unauthorized access, and circumvention for purposes of unauthorized copying (i.e. fair use):

> Section 1201 divides technological measures into two categories: measures that prevent unauthorized access to a copyrighted work and measures that prevent unauthorized copying of a copyrighted work. Making or selling devices or services that are used to circumvent either category of technological measure is prohibited in certain circumstances, described below. **As to the act of circumvention in itself, the provision prohibits circumventing the first category of technological measures, but not the second.**
>
> This distinction was employed to assure that the public will have the continued ability to make fair use of copyrighted works. Since copying of a work may be a fair use under appropriate circumstances, **section 1201 does not prohibit the act of circumventing a technological measure that prevents copying.** By contrast, since the fair use doctrine is not a defense to the act of gaining unauthorized access to a work, the act of circumventing a technological measure in order to gain access is prohibited. [emphasis added] (U.S. Copyright Office, 1998, pp.3-4)

All of the users testifying in favor of an exemption at both the general-use (combined with documentary filmmakers) panel hearing and the educational-use (DVD-related) panel hearing were asking for permission to circumvent in order to copy, not to gain access. All of the users already had legal access to the materials they wished to copy. All wanted to copy within fair use.

Section 1201 was written such that it does not prohibit the act of circumventing in order to make a copy. The Copyright Office should take this opportunity to clarify this issue which continues to problematize, even haunt any determination on exemptions especially in light of technological developments that make the methods by which one records audio-visual materials "inside" the computer invisible to all but the software developer. The Copyright Office should use this year's hearings as an opportunity to seek more information on how and why the content industry can explicitly and implicitly assert that anti-access technology and anti-copying technology are one and the same thing, if they are in fact so. The content industry opposes an exemption for the class of works consisting of CSS encrypted DVDs. It is apparent that the content producing industry believes circumventing CSS in order to obtain a copy of audio-visual materials is a violation of 1201. Logically, this must be because CSS protects both access and copying. CSS allegedly serves as both an anti-copying mechanism and an anti-access mechanism.

Yet, the correct interpretation and implementation of 1201 would negate the need for an exemption for any user who has legal access, because under a correct reading of the statute as evidenced by the legislative intent, circumventing in order to make a copy is not a violation of the statute: "section 1201 does not prohibit the act of circumventing a technological measure that prevents copying" (U.S. Copyright Office, 1998).

The Copyright Office and the community participating in the hearings would be well served by revisiting the original intent of 1201, including the broad definition of "copying" as understood at the DMCA's enactment. According to the U.S. Copyright Office Summary (1998): " 'Copying' is used in this context as a short-hand for the exercise of any of the exclusive rights of an author under section 106 of the Copyright Act. Consequently, a technological measure that prevents unauthorized distribution or public performance of a work would fall in this second category" (footnote 2, p.4).

Technological measures that prevent copying, including distribution, and technological measures that prevent access, were clearly two distinct categories as anticipated by the

legislation, and copying was defined broadly. Circumventing for purposes of copying, including circumventing for purposes of unauthorized distribution (such as distribution of remix videos on YouTube) is not prohibited under 1201. The only type of circumvention that is prohibited is that intended to gain unauthorized *access*, and as was clear during the 2009 hearing testimony, users asking for an exemption already had *legal access* – what they wanted to do was *make copies* of bits and pieces under fair use.

Further evidence of the importance of revisiting the clear separation of technological measures that prevent copying versus technological measures that prevent access, is illuminated in the 2006 Recommendations of the Register of Copyrights:

> The prohibition in § 1201(b) extends only to devices that circumvent copy control measures. The decision not to prohibit the conduct of circumventing copy controls was made, in part, because it would penalize some noninfringing conduct such as fair use.
>
> In the House of Representatives, the DMCA was sequentially referred to the Committee on Commerce after it was reported out of the Judiciary Committee. The Commerce Committee was concerned that section 1201, in its original form, might undermine Congress's commitment to fair use. While acknowledging that the growth and development of the Internet has had a significant positive impact on the access of students, researchers, consumers, and the public at large to information and that a "plethora of information, most of it embodied in materials subject to copyright protection, is available to individuals, often for free, that just a few years ago could have been located and acquired only through the expenditure of considerable time, resources, and money, the Committee was concerned that "marketplace realities may someday dictate a different outcome, resulting in less access, rather than more, to copyrighted materials that are important to education, scholarship, and other socially vital endeavors. Possible measures that might lead to such an outcome included the elimination of print or other hard-copy versions, permanent encryption of all electronic copies and adoption of business models that restrict distribution and availability of works. The Committee concluded that "[i]n this scenario, it could be appropriate to modify the flat prohibition against the circumvention of effective technological measures that control access to copyrighted materials, in order to ensure that access for lawful purposes is not unjustifiably diminished." (pp. 6-7)

The future imagined by the Committee is upon us: elimination of print or other hard-copy versions, i.e., the elimination of VHS and analog, copy-able audio-visual materials; permanent encryption of all electronic copies, i.e., the merging of "anti-access" and "anti-copy" technological measures; and adoption of business models that restrict distribution and

availability of works, i.e., pay per use, video-on-demand, and other distribution control models. These practices proliferate and are now dominant. It is unclear where “anti-access” measures stop and “anti-copy” measures begin, thus dashing the intent of the carefully crafted language in 1201(a) and 1201(b). The way that 1201(a)(1)(A) is now interpreted by the U.S. Copyright Office, it should read: “No person shall circumvent a technological measure that effectively controls access **and/or copying of/**to a work protected . . .” But that was not the intent of this statute, as evidenced in the congressional record and in documents produced by the Copyright Office.

According to an intriguing study of the 2000 and 2003 DMCA Exemption Hearings (Herman & Gandy, 2006), “the fourth most common claim by [exemption] proponents was that the ban on circumventing access controls was effectively becoming a ban on circumventing use controls” (p. 159). In her 2000 Recommendation, the Register of Copyrights called attention to the problem raised by exemption proponents due to the merging of copy controls and access controls:

> In this view, the merger of access and use controls would effectively bootstrap the legal prohibition against circumvention of access controls to include copy controls and thereby prevents a user from making otherwise noninfringing uses of lawfully acquired copies, such as excerpting parts of the material on a DVD for a film class, which might be a fair use.
>
> While this is a significant concern, there are a number of considerations to be balanced. From the comments and testimony presented, it is clear that, at present, most works available in DVD format are also available in analog format (VHS tape) as well. . .
>
> If in a subsequent rulemaking proceeding one could show that a particular “copy” or “use” control could not in fact be circumvented on a legitimately acquired copy without also circumventing the access measure, one might meet the required burden on this issue. (p. 64568)

Times have changed in the nine years since this original recommendation. It is common knowledge, and the 2009 hearing testimony clearly showed that VHS is completely obsolete. The only digital copies of audio visual material available now are those encrypted with anti-copying technologies such as CSS. During my educational-use panel testimony I showed a

student-created work, a montage challenging stereotypes of African Americans as portrayed in popular movies. I testified that the student had legally obtained the DVDs of each movie used in the montage. But for circumventing the CSS on the DVD-housed movies, this student would not have been able to complete the montage. There were many other examples in the 2009 testimony, for example witness Roger Skalbeck stated:

> For educators who want to use short clips from audiovisual works, if one cannot circumvent CSS, one is left with the options of foregoing use of the clips in the classroom, or creating poor replicas of the higher quality originals from their inferior versions of the films, if available. The CSS makes the contents of the DVD inaccessible to all users, including those who would use a small portion for educational purposes. Without the ability to circumvent CSS in these circumstances, the small portion of the work needed requires a time-consuming set-up that actually works against the purpose of enhancing the student's education experience. (May 6, 2009 Transcript, p. 0155)

The time is now ripe for the Copyright Office to examine and untangle the dilemma caused by the merging of copy and access controls in the form of CSS since DVDs encrypted with CSS are the only practical form of audio-visual media commonly available for educational use. In transcripts from the 2006 hearings, the Register pondered these issues:

> I'm trying to get a handle on the issue of access control. Somehow I think I've lost it. In this instance, you actually do have access to the work . . . But when you're decrypting, aren't you focusing on the copy control, rather than the access control? . . . You really do have 24 access to the content on the DVD. I mean, you have an authorized copy, you have a compliant player, and therefore, you do have access to "the work." So, I'm still struggling a little bit with regard to the issue of this being an access control problem. Yes. (Register Peters, DMCA Hearing Transcripts, April 3, 2006, pp.95-98)

Yet in the 2006 Recommendation no resolution to this crucial issue was forthcoming.

Understandably, the Copyright Office would be assisted with guidance from Congress on this issue. Admittedly: "The merger of technological measures that protect access and copying does not appear to have been anticipated by Congress" (Recommendation, 2000, p. 64568). While the Register has requested in her previous Recommendation clarification from Congress "since the implementation of merged technological measures arguably would undermine Congress's decision to offer separate treatment for access controls and use controls in section

1201" (Recommendation, 2000, p. 64568), that clarification has not been forthcoming (to the best of my information and belief). However, in the meantime, Congress clearly delegated a form of quasi-legislative power to the U.S. Copyright Office by way of these exemption hearings to occur every three years. The power here is obviously limited in that whatever recommendations the Register makes will be limited in time – for three years only. In the absence of clarification from Congress which was requested almost a decade ago, clearly *Congress is insisting that the proper venue for dealing with technological developments and user needs as they bump up against 1201 is these rulemaking hearings.* Exemption proponents have nowhere else to turn but these hearings. I therefore respectfully request that the U.S. Copyright Office "spend more time exploring the possibilities of the rulemaking" (Herman & Gandy, 2006, p. 189) and work towards a recommendation that clarifies the serious problem that has occurred due to the content industry's merger of anti-copy and anti-access controls.

Almost a decade ago, the Register correctly predicted that "the issue of merged access and use measures may become a significant problem" (2000, p. 64568). Ample evidence was provided in the 2009 hearings that CSS-protected DVDs cannot be accessed for purposes of copying bits and pieces for fair use without circumvention, and such CSS-protected DVDs are the only accessible medium by which one can create remixed audio-visual works for purposes of criticism, news reporting, comment, and so on.

In 2009, it appears that the U.S. Copyright Office assumes that anti-access controls and anti-copy controls are one and the same thing. Clarification on this issue and a bold statement on its position would be very helpful to all concerned. However, what evidence has been received from the content industry that actually shows, empirically, that access control and copy control are totally merged? Due to the crucial nature of this issue, since circumventing to copy is not a violation of 1201, it would benefit all parties if the Copyright Office would request evidence from the content industry that CSS is not primarily a technological measure intended to prevent

copying rather than access. Revisiting the 2000 post-hearing comment submitted by EFF's Robin D. Gross is very illuminating:

> . . . DVDs using CSS do not protect against unauthorized access to a work. Pirated DVDs have no trouble playing in DVD-CCA's license players. Rather, the system's design and ultimate objective is to prevent unauthorized copying – by requiring consumer to use devices which obey design restrictions that prevent such copyright. (quoted in Herman & Oscar, 2006, p. 159; See also Gross, 2000)

Since the content industry takes the position that anti-access technology is one and the same as anti-copy technology (CSS for example), it seems that important, reasonable questions are questions which have not been posed by the Copyright Office. Such questions would ask the content industry to explain how anti-access technology works, how anti-copying technology works, and why these two "anti" technologies have been collapsed into one technology, thus preventing users from making legal copies under fair use.

The "Anti" Measures

Rather than placing the burden of these proceeding determinations on software companies to defend their screen capturing technologies against possible charges of violating 1201 (even though they were not asking for nor defending against an exemption to 1201; they were not parties on the relevant panels), the burden in these proceedings should be placed squarely on the shoulders of the industry directly benefitting from 1201. The content industry should explain and justify why they have decided to make the two "anti" measures one and why it is not, if it is not, in the decade following the enactment of the DMCA and in light of the speed at which technology develops, why it is not possible to separate out the anti-access technology from the anti-copying technology. What possible reason could there be for disallowing users to make short-duration copies of audio-visual materials once they have legal access other than to use "technical and legal strategies to 'circumvent Congress'" (Gross, 2000)?

I understand that the Register's position is that "the burden is on the proponent of the exemption to make the case for exempting any particular class of works from the operation of

section 1201(a)(1)" (Recommendation, 2000, p. 64558). However, the burden or elements needed for an appropriate exemption as outlined in the 2006 Recommendation have certainly been met by the educational community (e.g., not "mere inconvenience," no alternative formats, will be a fair use). Placing the burden on proponents of the exemption does not mean the opposers of the exemption, the content industry, should go scot free. The content industry needs to show some evidence other than just their words, that CSS, for example, is not primarily an anti-copying technology – that there is some true and valid reason for merging anti-copying and anti-access measures, that such tactics are not used simply to undermine Congressional intent and disavow fair use. During the 2009 hearings (witness) Mr. Attaway seemed to focus on the anti-copying features of CSS and the ability of CSS to protect the integrity of content (harkening to a kind of "moral rights" protection) rather than CSS's ability to prevent unauthorized access.

> Jonathan Band pointed out in his testimony that the circumvention utility for CSS, which protects DVDs from copying, is readily available; that, we all understand that. Nonetheless, CSS has been an extremely effective protection measure, because it's inconvenient, and the copies it produces are not always of optimum quality . . . it's what makes CSS effective and useful in protecting the integrity of our copyrighted movies. (May 6 Transcript, 2009, p. 0204)

If CSS is in fact primarily an anti-copying technological measure, then circumventing it for purposes of making copies is not a violation of 1201 and no exemption is needed.

When pressed on the issue, (witness) Mr. Metalitz stated that CSS is both an anti-copy and an anti-access measure, but offered no technical illustration or empirical evidence:

> I think all the examples that were given do involve the making of copies. But it -- it's also clear that -- and I think it's been well-established in this proceeding and in the courts that CSS is also an access control. It may have copy control features as well, but is an access control. (May 7, 2009 Transcript, p. 0144)

I disagree that it has been "well established" that CSS is both an access control and a copy control, simultaneously. To the contrary, in *Universal City Studios v. Corley* (2001), Judge

Newman reminded us of the unresolved controversy around the functioning of CSS as a copy *and* access control:

> An item of some controversy, both in this litigation and elsewhere, is the extent to which CSS-encrypted DVDs can be copied even without DeCSS. The record leaves largely unclear how CSS protects against the copying of a DVD, as contrasted with the playing of a DVD on an unlicensed player. The Defendants' experts insisted that there is nothing about the way CSS operates that prevents the copying of a DVD . . . (Testimony of Professor Edward Felten) (CSS "could [not] have prevented the encrypted content from being copied to somewhere else") . . . Some of the Plaintiffs' experts countered simply that "copying to a hard drive is something that compliant DVD players are not allowed to do," without explaining why . . .
>
> However, none of this detracts from these undisputed findings: some feature of either CSS itself, or another (unidentified) safeguard implemented by DVD manufacturers pursuant to their obligations under the CSS licensing scheme, makes it difficult to copy a CSS-encrypted DVD to a hard drive and then compress that DVD to the point where transmission over the Internet is practical . . . Conversely, a DVD movie file without CSS encryption is easily copied, manipulated, and transferred . . . In other words, it might very well be that copying is not blocked by CSS itself, but by some other protection implemented by the DVD player manufacturers. Nonetheless, in decrypting CSS, the DeCSS program (perhaps incidentally) sidesteps whatever it is that blocks copying of the files. (footnote 5, p. 438)

This controversy remains unresolved and yet its resolution appears to be *crucial* to these hearings.

Certainly, considering its technological-savvyness, the content industry should be able to create a technology that limits access to those who have legally obtained certain media, and subsequently allows them to make short-duration copies, take bits and pieces of that media, once they have legal access. The answer to these questions focused on the content industry and the dilemma created by collapsing anti-access technology and anti-copying technology, if in fact those two technologies are working within a single mechanism, would help inform the Copyright Office about the content industry's motivations for the development of a single "anti" mechanism (if this really is a single mechanism) that has crushed the ability of law abiding citizens to make copies of limited portions of audio-visual materials within legal fair use.

“Circumvention”?

In addition to revisiting the legislative intent of the statute, it is also important to revisit the clear language of the statute in the context of the question above referenced, as posed by the Copyright Office. The content industry ineffectively asserts that using a digital video camera to record the screen is somehow not illegal “circumventing.”[1] Surely, recording the screen using a digital video camera is circumventing the CSS or the anti-copying protections of DVD material. According to 1201(a)(3)(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. [emphasis added]

Further, 1201(b)(2)(A) states:

> To “circumvent protection afforded by a technological measure” means **avoiding, bypassing**, removing, deactivating, or otherwise **impairing** a technological measure. [emphasis added]

When considering levels of importance of terms within this statute, it is noteworthy that only the first definition contains references to descrambling or decryption but both definitions stress the importance of disallowing broader types of circumvention. Recording the screen using a digital video camera is certainly a “bypass,” an “avoidance,” or an “impairment” of a “technological measure” and so is thus a “circumvention of a technological measure” under 1201. There is some case law that supports this. In the recent case of *I.M.S. Inquiry Management Systems, v. Berkshire Information Systems* (2004), Judge Buchwald considered as a matter of “first impression” whether inducing a third party to provide his/her password in order to enter a password protected website was a “circumvention” of an anti-access technology under the DMCA. In this case, two competing information companies became involved in litigation when one company was able to examine the online databases of the other company by inducing a third party to share his/her password in order that the competitor’s website could be entered,

examined, and information gathered. To answer the question about whether using a password in this context was a violation of the DMCA because it was a circumvention of the anti-access technology, the Judge posed two questions:

1. Was an effective technological measure in place?
2. Was the technological measure circumvented?

As to the first question, Judge Buchwald said that password protection is a technological measure intended to prevent access as defined under the DMCA. As to the second question, Judge Buchwald stated:

> It is of course the case, as defendant propounds, that the DMCA addresses activity such as decryption, descrambling, deactivation and impairment, and that these are all forms of circumvention under the subsection commonly involving technologically-sophisticated maneuvers. One might associate these activities with the breaking and entering (or hack-ing) into computer systems.
>
> **On the other hand, other actions proscribed by the DMCA, connote broader application of the anti-circumvention prohibition, such as the terms "avoid" and "bypass". These actions are far more open-ended and mundane, and do not necessarily involve some kind of tech-based execution.** [p. 532, emphasis added]

Because the defendant in the *I.M.S.* case had obtained (but not stolen) someone else's password and used that to enter the website just as the person who owned the password would have, the court decided that this was not "circumvention" under the statute. "More precisely and accurately, what defendant avoided and bypassed was permission to engage and move through the technological measure from the measure's author . . . the DMCA 'targets the circumvention of digital walls guarding copyrighted material'" (p. 532). This case differs from the present case of camcording the computer screen, because camcording is not the normal method by which a user accesses DVD material. Camcording the computer screen is an abnormal behavior that is purposely and intentionally completed in order to bypass and avoid the anti-copying features of CSS. Further, if an individual wishes to make copies of items on their computer, the normal method (for which the computer is designed) is to make a screen capture or print a PDF, not snap pictures or take videos of their computer screen. Clearly, neither the technologies of the

computer nor the camcorder were designed with the strange uses in mind that are suggested by the content industry.

Another case suggests that user intent is relevant when deciding whether or not circumvention occurred. In the 2007 case of *Healthcare Advocates v. Harding*, a dispute arose because in the course of legal investigation from a previous trademark case, the defendant-law firm's employees had obtained archived screenshots from a public website (the Wayback Machine) and used those screenshots as evidence. Although the plaintiff argued that the defendant had intentionally and purposely tampered with technological measures (e.g., a robots.txt file) protecting the images taken, the court found that a server malfunction had made the images available to the investigators. The court found that in this context a robots.txt file was a technological measure preventing access as defined by the DMCA. Expert witnesses in the case, Felton and Lenkey, defined circumvention to including "hacking," "malicious intent," and "activity that is devious and out of the ordinary" (p. 644). Because the defendants did not intentionally avoid the technological measures, the court found there to be no circumvention as defined by the DMCA. The opinion states:

> Healthcare Advocates' argument focuses on the terms "avoid" and "bypass" presumably because the other terms do not encompass what occurred in this situation. "Avoid" is defined as "to keep away from; keep clear of; shun; or to make void." The Random House College Dictionary, 84 (1973). "Bypass" is defined as "to avoid" . . . These words, as well as the remainder of the words describing circumvent, imply that a person circumvents a technological measure only when he **affirmatively** performs an action that disables or voids the measure that was installed to prevent them from accessing the copyrighted material. [emphasis added, p. 644]

Because the defendant was able to access the materials due to a technological malfunction rather than because he affirmatively and purposely attempted to circumvent the robts.txt file, the court found that the defendants' accessing and printing of screenshots did not constitute a circumvention of a technological measure under the DMCA.

> When the Harding firm accessed Internet Archive's database on July 9, 2003, and July 14, 2003, it was as though the protective measure [**47] was not

> present. Charles Riddle and Kimber Titus simply made requests through the Wayback Machine that were filled. They received the images they requested only because the servers processing the requests disregarded the robots.txt file present on Healthcare Advocates' website. As far as the Harding firm knew, no protective measures were in place in regard to the archived screenshots they were able to view. They could not avoid or bypass any protective measure, because nothing stood in the way of them viewing these screenshots. Healthcare Advocates has not presented any evidence to show that the Harding firm did anything to avoid or bypass the robots.txt file [*645] in place on its website. The facts presented show that the Harding firm benefitted from a malfunction in Internet Archive's servers. Plaintiff has not shown that Defendants circumvented the robots.txt file. (pp. 644-645)

In the context of the Copyright Office's question regarding differences in legal consequences for using screen capturing software versus digitally camcording the computer screen, clearly when camcording there is great intentionality to avoid or bypass the CSS that prevents copying. It is devious, out of the ordinary, and abnormal behavior. On the other hand, most users are not going to know that they could potentially be doing something illegal by using legally produced and openly marketed screen capturing software, software used in educational institutions across the U.S., because whatever that software does to copy is invisible to the naked eye. Therefore, if taking into consideration the matter of intentionality and motivation, camcording a computer screen would more likely be a circumvention under the DMCA than would using screen capturing software. Camcording would eliminate the chance of making an argument under 1203(c)(5)-innocent violations. With screen capturing, an unsuspecting user could still leverage that section of the statute as a defense or mitigating factor.

Beside the clear language of the statute, we might also be informed by the *Oxford English Dictionary*'s definition of "circumvent": 1) "To surround or encompass by hostile stratagem, esp. so as to cut off or capture"; 2) "To get the better of by craft or fraud; to overreach, outwit, cheat, 'get round', 'take in'. Also, to evade or find a way around (a difficulty, obstacle, etc.)". The word "circumvent" implies an intentionality that just was not present among hearing witnesses requesting an exemption for working with DVDs. Witnesses who admitted circumventing CSS did so with *no intention* of gaining unauthorized access. All such witnesses

had the sole intention of circumventing copying measures in order to copy. It appeared during the hearings the only kind of circumvention understood by the content industry is “descrambling” and “decryption” “inside” the computer, and that user intention is irrelevant. As I have illustrated, these issues are much more complicated than presented at the 2009 hearings.

Using a digital video camera is a method to outwit, to evade the CSS encryption on DVDs. Yet the content industry offers this up as an unseemly solution to the problem posed. But if the anti-copying technology of the DVD, the CSS, is one and the same as the anti-access technology as asserted by the content industry, then using a digital video recorder to circumvent the anti-copying technology is also using a digital video recorder to circumvent the anti-access technology. This is the only logical outcome.

It does not make sense that the content industry can argue on one hand that because the anti-copying technology and the anti-circumvention technology are one and the same, to circumvent “inside” the computer in order to make a copy is a violation of 1201, but on the other hand argue that somehow the anti-copying technology is separate when one is outside the computer and thus it is legal to record the screen. Recording the screen externally is still circumvention. The content industry should not be able to have it both ways – to argue simultaneously that the anti-copying technology and the anti-access technology are one and the same when one is “inside” the computer, and that they are not one and the same when one is “outside” the computer. Either they are or they are not.

Either a user has lawful access to the work or she does not, whether recording the screen from “inside” the computer or from “outside” the computer. The end result of the content industry’s position is completely illogical and ultimately erases any possibility of users making any types of fair uses of audio-visual materials despite the industry’s claims to the contrary. No one is realistically going to camcord the screen of their computer. The content industry failed to offer any empirical evidence that users actually use this phantom method in order to copy audio-visual materials. A single demonstration tape is insufficient to show this is actually an alternative

used by real people. As I have illustrated, the legality of camcording the computer screen is sketchy at best. What this means is that there is no fair use available for CSS encrypted DVDs. The harm to users, particularly those in education when you consider the crucial social value of the work they do, is great as the 2009 hearing testimony illustrated witness after witness.

As to the remaining questions posed by the Copyright Office regarding how screen capturing software works, my experience is with TechSmith's Camtasia which I have used for over three years for purposes of preparing teaching materials for my online (distance education) and face-to-face courses. I have never successfully captured copyright-protected DVDs by screen capturing, regardless of the settings used. Therefore I am unable to use material on DVDs for educational, teaching purposes. Obviously this creates an empty space in my curriculum.

With respect to the Copyright Office's other questions, the only source that could actually answer the questions about how individual software works to record the screen (if it is even possible to do this) would be individual software developers. Otherwise, the answer to these questions might involve revealing trade secrets, patented software methods, and conducting reverse engineering beyond the scope of any existing exemption to 1201.[2]

The questions posed by the Copyright Office regarding whether DVDs can be decrypted in part (rather than in entirety), to the best of my understanding, can only be answered by research that would create behavior violating 1201. Since I am not a researcher examining security flaws, or a researcher falling under any other of the existing exemptions for 1201, I am unable to legally complete this research. The fact that I cannot legally complete the research should inform the Copyright Office as to variable 1201(a)(1)(C)(iii): "the impact that the prohibition on the circumvention of technological measures applied to copyright works has on . . . research." There is no exemption that allows me to research how different DVD ripping software functions and which software would be least intrusive into the encryption technologies developed by content producers.[3] Regarding the question on whether or not output from screen

captured files are encrypted, those concerns should be addressed by section 1202 of the statute.

Additionally, the question on whether or not DVD ripping software is able to rip portions of audio-visual materials rather than entire works seems off point in light of the fact that the content industry has suggested camcording computer or TV screens is an acceptable means to avoid 1201 liability, yet certainly one can camcord entire works.

What I have ultimately tried to show in my response thus far is the absolute legal uncertainty present here no matter what method is used for copying CSS encrypted DVDs. Because of this legal uncertainty and possible legal liability, users are adversely affected as demonstrated again and again and again during the hearings. The only way to address this problem is by issuing exemptions.

In my Request to Testify I have supported the EFF class:

> Audiovisual works released on DVD, where circumvention is undertaken solely for the purpose of extracting clips for inclusion in noncommercial videos that do not infringe copyright.

In the alternative, as a further limit, I propose this class be exempted as previously stated in my educational-use panel testimony:

> Motion picture and audiovisual works released on DVD, housed in a US library collection where the student attends or where the teacher is employed, or legally obtained and owned by the teacher/student, where circumvention is undertaken solely for the purpose of extracting clips for inclusion in videos or multimedia texts that do not infringe copyright and that are composed either as part of student coursework or as part of course curriculum. This exemption shall apply even for works that are gifted from students/teachers to community groups/non-profits as part of service learning or community outreach.

As an additional alternative, I urge the Copyright Office to consider clarifying whether 1201 retains the punch of *any of its original legislative intent* that clearly avoided making circumvention for copying illegal. The most correct and just outcome in these hearings would be for the Copyright Office to remember these hearings are the only remedy for many participants,

and to forthrightly draw on its quasi-legislative powers as delegated by Congress, and craft a clear and bold statement in the form of a rule that an exemption is unnecessary for any use where the user has legal access but intends only to make a copy because such circumvention is not prohibited by 1201 to begin with. Such a rule might look like this:

> While it is the Register's view that an exemption for purposes of circumventing CSS protected DVDs that a user has legal access to solely for the intentions and purposes of making fair use copies of limited portions of those DVDs is not needed because such circumvention for copying is not prohibited by 1201(a)(1)(A), to the extent that such an exemption is deemed necessary by users, it is hereby granted.

Answering the Question

To answer the question, "Please explain whether the legal consequences of using capture software differ from the legal consequences of using a digital video camera (with particular reference to 17 U.S.C. § 1201)," as outlined above, the correct possible answers to this question are, assuming we are a) referring to CSS encrypted DVDs; b) CSS is the technology being circumvented; c) and in all cases the purpose of the circumvention is to make a copy within fair use and not to wholesale pirate:

1. If 1201 is now interpreted by the U.S. Copyright Office as prohibiting circumvention for copying, then both using capture software and digital video camera recording are arguably illegal acts of "circumvention" (because both methods allow the user to copy something that has been protected from being copied regardless if that copying is completed by "decrypting" CSS or bypassing/avoiding it);
2. If 1201 prohibits circumvention of technologies that simultaneously are anti-copying and anti-access technologies and CSS is in fact such a technology, then both screen capturing and camcording the screen of a media device are arguably illegal under 1201;

3. If CSS is primarily[4] an anti-copying technology, although it may contain anti-access features, and 1201 is interpreted as not prohibiting circumvention for purposes of copying but only circumvention for purposes of access, then neither using capture software nor a digital video camera, nor any other circumvention tool or method is a violation of the statute.

Thank you for your time in reviewing this response.

References

April 3, 2006 DMCA Hearing Transcript. Retrieved on July 8, 2009 from http://www.copyright.gov/1201/2006/hearings/index.html.

Gross, R.D. (2000). EFF post-hearing comments requesting exemption of DVDs from § 1201(a). Retrieved on July 8, 2009 from http://www.copyright.gov/1201/post-hearing/gross.pdf

Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey. (2007). 497 F. Supp. 2d 627; 2007 U.S. Dist. LEXIS 52544.

Herman, B.D. & Gandy, O.H. Jr. (2006). Catch 1201: A legislative history and content analysis of the DMCA exemption proceedings. *Cardozo Arts & Entertainment, 24,* 121-190.

I.M.S. Inquiry Management Systems, Ltd. V. Berkshire Information Systems, Inc. (2004). 307 F. Supp. 2d 521; 2004 U.S. Dist. LEXIS 2673; 70 U.S.P.Q.2D (BNA) 1105.

May 6, 2009 DMCA Hearing Transcript. Retrieved on July 7, 2009 from http://www.copyright.gov/1201/hearings/2009/transcripts/

May 7, 2009 DMCA Hearing Transcript. Retrieved on July 9, 2009 from http://www.copyright.gov/1201/hearings/2009/transcripts/

Oxford English Dictionary Online. 2009.

Recommendation of the Register of Copyrights and Determination of the Librarian of Congress. (2000). 65 FR 64555.

Recommendation of the Register of Copyrights in RM 2005-11;Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies. (2006). Retrieved on July 9, 2009 from http://www.copyright.gov/1201/docs/1201_recommendation.pdf.

Universal City Studios, Inc. et al. v Eric Corley and 2600. (2001). 273 F.3d 429; 2001 U.S. App. LEXIS 25330.

U.S. Copyright Office Summary. The Digital Millennium Copyright Act of 1998. Retrieved June 6, 2006, from http://www.copyright.gov/legislation/dmca.pdf.

[1] To the best of my knowledge, this idea was first suggested 8 years ago in the *Universal v. Corley* (2001) decision. In that opinion Judge Newman (incorrectly) wrote: "The DMCA does not impose even an arguable limitation on the opportunity . . . [to record] portions of the video images and sound on film or tape by pointing a camera, a camcorder . . . at a monitor as it displays in DVD movie" (p. 77). This quote evidences a misunderstanding of the DMCA as it is being interpreted by courts most recently. However, this case was primarily a first amendment case and a case dealing with the anti-trafficking provisions of the DMCA. It was not a fair use case nor was it a case focusing on circumvention.

[2] After posting the Copyright Office's questions on my blog, I did receive an unsolicited comment from the CEO of one of the software companies listed as exemplary in the Copyright Office's questions. Via email, I confirmed this CEO's identity and also asked permission to include his comments wherein he answered the questions. Those comments can be viewed here: http://martinecourantrife.blogspot.com/2009/06/us-copyright-office-submits-questions.html.

I also corresponded with a software developer and expert in these areas, and his opinion was that screen capturing software does not decrypt CSS because it works after decryption occurs.

Here is what he said (I'm keeping his identity anonymous for now due to the short notice I had with which to prepare these answers. However, he is definitely an expert software developer working in the business for many, many years. In the event the Copyright Office wants more information from him I could ask him if he is available. He is traveling now and only has sporadic availability to the internet.):

[Begin expert's quote]
I can't speak to legal consequences, but there are some technical differences which Congress or the courts might take into account. The main technical difference is that with capture software there's no "analog step".

With filming the screen, digital content from the DVD is rendered on the computer screen; so far that's all digital and exactly reproducible (though the image may differ from one computer to the next, due to differences in hardware and software). But then the camera films the screen image as a whole; that's an analog step. Like an audio recording of a live event, it isn't an exact reproduction of the original content. (In theory, you could build a camera with the resolution to precisely film every pixel, then use software to reconstruct the images frame-by-frame and come up with something close to the original content, but that's not a plausible scenario.)

Screen-capture software, on the other hand, can in principle capture all the images sent to the computer screen in exact digital form. That's still not precisely the same as the original content on the DVD, because it's been decoded and rendered, and different hardware will render the images somewhat differently; also, capture software usually doesn't try to capture in full resolution, because that would take a lot of resources (possibly more than the computer has available).

So, for example, if you had two people with identical equipment trying both of these methods, they should get bit-for-bit identical copies with capture software, but their video-camera copies wouldn't be identical. Some people might consider that grounds for different treatment under the law.

> Is there particular capture software that decrypts the Content
> Scrambling System on DVDs?

I don't think any *legal* capture software itself decrypts CSS.

Usually it doesn't have to; capture happens after the content has already been decrypted. That's a function of playback software. Capture software is usually separate from playback software.

My understanding is that it's illegal for software to decrypt CSS unless the publisher of the software holds a license for the CSS technology, which includes restrictions on how it's used.

There are software programs which can decrypt CSS even though the publishers don't have a CSS license, because CSS was cracked (because it was a lousy design and a worse implementation). Some of those might combine playback and capture functions. Usually those programs just create a copy of the source material with the CSS encryption removed, though.

> Is there particular capture software that does not decrypt the Content
> Scrambling System on DVDs?

I believe this is usually, or always, the case. Decrypting CSS isn't a job for capture software as such.

> To the best of your ability, please explain how screen capture
> software operates, e.g., does reproduction take place after the work
> is lawfully decrypted?

Typically (always?) yes. Capture itself would always be taking place after decryption; whether that decryption is "lawful" is another question, but I doubt mass-market capture software would touch decryption at all.

> Does the capture software reproduce the
> digital output from the computer, or does the capture software
> reproduce the analog output from the computer?

Digital. This is actually getting into a rather complex area, as the "digital"/"analog" dichotomy is not really so well-defined. With many computer devices these days you have a mix of digital and analog signaling, or digital signals over an analog carrier, or some other combination.

The digital/analog distinction was always something of a convenient fiction. It was shorthand for saying "is there an obvious loss of quality in the copy?". If someone pirated a DVD by making a digital copy of it, the copy was indistinguishable from the original. But when someone copies a DVD by playing it and filming their TV screen, the copy is usually noticeably inferior to the original.

With today's equipment, the distinction is getting smaller. CRT screens are analog, but LCD screens are digital. As I noted above, in theory you could record an LCD screen at such high resolution that you'd record each pixel - and then you have a digital recording, even if there's an air gap between the screen and the camera.

> Does this
> analog/digital distinction matter for determining whether a violation
> of § 1201(a)(1) is taking place?

Good question.

> Is the output encrypted at the time of capture by the software or is
> the output decrypted at the time of capture?

Decrypted.

There's some potential for confusion here, because with modern equipment there can be multiple stages of encryption.

DVDs (with commercial content) are typically encrypted with CSS. That usually gets decrypted by the playback hardware or software – the standalone DVD player, or the DVD player software on the computer. (Sometimes it's built into the DVD drive. The drive also checks the DVD "region", which is another whole ball of nonsense.)

After the content is decrypted, it has to be rendered. The MPEG4 data streams are decompressed and turned into a series of images, in effect.

Then those images are sent to the display device. In a computer, that means the playback software sends them to the video hardware, which then drives the display. (Sometimes the video hardware actually gets the MPEG4 data

and does the rendering, too.) With a standalone DVD player, it sends the images to the TV, using one of a number of kinds of connections.

Now, some of those connections between computer video output and display, or between DVD player and TV, can also be encrypted. The old-fashioned analog connections (with coax cables, or those cables you used to use for stereo components) don't. But the fancy new connection types like HDMI have provisions for digital rights management interactions between regular home A/V components, and they can actually encrypt the signals to prevent you from recording your DVD playback off the wire.

But capture software typically lives at the video-hardware-driver level. The typical capture software says, hey, I'm a video driver! Playback software, send your images to me, so I can render them and send them to the display! That's all decrypted content at that point.

> Do different screen capture programs involve significantly different
> methods of capturing screen and/or audio output?

I've seen a couple of approaches. Some screen-capture software pretends to be a video output device, as I described above. Some periodically reads the screen to see what's on it. Some intercepts operating-system instructions to see what programs are writing to the screen.

Probably only the first type would work for capturing video from DVD playback, though. Reading the screen would drop a lot of frames and produce noticeably blocky, jumpy video. And DVD playback doesn't go through the regular operating-system mechanisms for writing to the screen - it has to use special optimized mechanisms (eg DirectX in Windows) so it can pump all that data to the screen quickly.

> There was an example of screen capture software at the § 1201 hearings
> and some witnesses pointed out that the example presented revealed
> quality degradation, e.g., pixelation. Can capture software be
> adjusted in order to affect the quality of the reproduction of the
> video or audio captured? If so, how?

Yes, it typically can be adjusted, and there are other steps that a user can take (eg running a stripped-down system so other tasks aren't interfering with recording) to improve capture quality. There are limits, though.

With a system with sufficient resources, it should be possible to reproduce the original DVD video with very good fidelity, probably even with no loss of quality. But with the typical consumer system, I think you're always going to have some loss of quality, however you adjust it.

> Can the computer on which the capture software resides be adjusted to
> affect the quality of the output, i.e., by adjusting the settings of
> the operating system, video card or sound card software rather than
> the settings within the capture software itself?

Yes, but again only to a certain extent. Every system has finite resources, and exactly reproducing real-time video takes a lot of resources.

> It was claimed that screen and video capture technology does not work
> with Microsoft Vista. Is this true, and if so, why?

Not true, at least in general. Specific capture software might not work with Vista.

There may be some confusion here because of other DRM mechanisms that were implemented in Vista (and there's a fair bit of uncertainty around those) . . .

Some of the Palladium technologies reportedly made it into Vista. Some of them include ways in which Vista tries to detect if you've connected a recording device directly to the computer - for example, if you've hooked a VCR to the monitor port. If Vista decides you've done that, it degrades the video output. The idea is to make it harder to create a high-fidelity recording right from the computer's video output.

That doesn't affect screen-capture software, though.

It's worth noting that Vista actually includes screen-capture software, in effect - Microsoft's own Remote Desktop basically has to do what screen-capture software does. So does desktop sharing through Microsoft Windows Live Meeting. Those work fine with Vista.

> Are there other operating systems on which screen capture software
> will not operate?

There are a great many operating systems without screen capture software, but nothing that's likely to be used on a personal computer. For that matter, you can't play a DVD back on those OSes either. [End Quote]

[3] However, I am able to conduct this research if given two weeks before August 30, 2009 as well as an express exemption from 1201 for conducting the research.

[4] The Copyright Office could analyze and determine whether or not CSS is "primarily" a copy control by quantitatively analyzing its use and implementation as a copy control versus access control. These questions could be asked:

1. What technologies are in place other than CSS to protect access?
2. What technologies are in place other than CSS to prohibit copying?

By weighing and balancing the layers of technology at play here, the Copyright Office could determine whether or not CSS is really protecting access, or if access is indeed protected by other means as well.