Computers and the Law

Randy Canis

CLASS 11

DMCA
DMCA

- The DMCA is the Digital Millennium Copyright Act that was signed into law on October 28, 1998.
- The DMCA amended and augmented parts of the existing Copyright Act (i.e., Title 17).

Universal Studios v. Reimerdes

- Universal Studios et al. (P)
  - Eight major motion picture studios.
- Reimerdes (D)
  - Poster of DeCSS software program.
- Basis of Proceeding
  - Decision after preliminary injunction in favor of the P.

Universal Studios v. Reimerdes

- Why do the movie studios care about DeCSS and its progeny?
  - "First, the availability of DeCSS on the Internet effectively has compromised plaintiffs' system of copyright protection for DVDs, requiring them either to tolerate increased piracy or to expend resources to develop and implement a replacement system unless the availability of DeCSS is terminated."
  - "Second, the application of DeCSS to copy and distribute motion pictures on DVD, both on CD-ROMs and via the Internet, threatens to reduce the studios' revenue from the sale and rental of DVDs. It threatens also to impede new, potentially lucrative initiatives for the distribution of motion pictures in digital form, such as video-on-demand via the Internet."

Universal Studios v. Reimerdes

- The DMCA contains two principal anticircumvention provisions.
  - The first, Section 1201(a)(1), governs "the act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work," an act described by Congress as "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book."
  - The second, Section 1201(a)(2), which is the focus of this case, "supplements the prohibition against the act of circumvention in paragraph (a)(1) with prohibitions on creating and making available certain technologies developed or advertised to defeat technological protections against unauthorized access to a work."
  - As defendants are accused here only of posting and linking to other sites posting DeCSS, and not of using it themselves to bypass plaintiffs' access controls, it is principally the second of the anticircumvention provisions that is at issue in this case.
Universal Studios v. Reimerdes

(2) DeCSS Was Designed Primarily to Circumvent CSS

• "As CSS effectively controls access to plaintiffs’ copyrighted works, the only remaining question under Section 1201(a)(2)(A) is whether DeCSS was designed primarily to circumvent CSS. The ... answer is perfectly obvious. By the admission of both Jon Johansen, the programmer who principally wrote DeCSS, and defendant Corley, DeCSS was created solely for the purpose of decrypting CSS—that is all it does. ... Hence, absent satisfaction of a statutory exception, defendants clearly violated Section 1201(a)(2)(A) by posting DeCSS to their web site."

Universal Studios v. Reimerdes

Section 1201(a)(2)(B)

• As the only purpose or use of DeCSS is to circumvent CSS, the foregoing is sufficient to establish a prima facie violation of Section 1201(a)(2)(B) as well.

Universal Studios v. Reimerdes

Defense - The Linux Argument

• Perhaps the centerpiece of defendants’ statutory position is the contention that DeCSS was not created for the purpose of pirating copyrighted motion pictures. Rather, they argue, it was written to further the development of a DVD player that would run under the Linux operating system, as there allegedly were no Linux compatible players on the market at the time."

• Why didn’t this defense work?

Universal Studios v. Reimerdes

• First, Section 1201(f)(3) permits information acquired through reverse engineering to be made available to others only by the person who acquired the information. But these defendants did not do any reverse engineering. They simply took DeCSS off someone else's web site and posted it on their own. Defendants would be in no stronger position even if they had authored DeCSS. The right to make the information available extends only to dissemination "solely for the purpose" of achieving interoperability as defined in the statute. It does not apply to public dissemination of means of circumvention, as the legislative history confirms. These defendants, however, did not post DeCSS "solely" to achieve interoperability with Linux or anything else.

Universal Studios v. Reimerdes

• Fair use

• Finally, defendants rely on the doctrine of fair use. Stated in its most general terms, the doctrine, now codified in Section 107 of the Copyright Act, ... limits the exclusive rights of a copyright holder by permitting others to make limited use of portions of the copyrighted work, for appropriate purposes, free of liability for copyright infringement. For example, it is permissible for one other than the copyright owner to reprint or quote a suitable part of a copyrighted book or article in certain circumstances. The doctrine traditionally has facilitated literary and artistic criticism, teaching and scholarship, and other socially useful forms of expression. It has been viewed by courts as a safety valve that accommodates the exclusive rights conferred by copyright with the freedom of expression guaranteed by the First Amendment.
Universal Studios v. Reimerdes

• Defendants therefore argue that the DMCA cannot properly be construed to make it difficult or impossible to make any fair use of plaintiffs' copyrighted works and that the statute therefore does not reach their activities, which are simply a means to enable users of DeCSS to make such fair uses. Defendants have focused on a significant point. Access control measures such as CSS do involve some risk of preventing lawful as well as unlawful uses of copyrighted material. Congress, however, clearly faced up to and dealt with this question in enacting the DMCA.

Universal Studios v. Reimerdes

• “The Court begins its statutory analysis, as it must, with the language of the statute. Section 107 of the Copyright Act provides in critical part that certain uses of copyrighted works that otherwise would be wrongful are “not ... infringement[s] of copyright.” Defendants, however, are not here sued for copyright infringement. They are sued for offering and providing technology designed to circumvent technological measures that control access to copyrighted works and otherwise violating Section 1201(a)(2) of the Act. If Congress had meant the fair use defense to apply to such actions, it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate.”

Universal Studios v. Reimerdes

• “Defendants claim also that the possibility that DeCSS might be used for the purpose of gaining access to copyrighted works in order to make fair use of those works saves them under Sony Corp. v. Universal City Studios, Inc. But they are mistaken. Sony does not apply to the activities with which defendants here are charged. Even if it did, it would not govern here. Sony involved a construction of the Copyright Act that has been overruled by the later enactment of the DMCA to the extent of any inconsistency between Sony and the new statute.”
• What was the court’s justification for not applying Sony?

Universal Studios v. Reimerdes

• What about linking?
• Does it mean to provide or otherwise traffic in a violation of the DMCA?
• “[T]he anti-trafficking provision of the DMCA is implicated where one presents, holds out or makes a circumvention technology or device available, knowing its nature, for the purpose of allowing others to acquire it.”
• What was the ultimate ruling with regard to linking?

Universal Studios v. Reimerdes

• What about the First Amendment?
• Arguments
  – Computer code is protected free speech
  – DMCA is unconstitutionally overbroad
• Why do both arguments fail?

Universal Studios v. Reimerdes

• What happened after this case?
  – Appeal
  – 321 Studios case
Sony v. GameMasters

- Plaintiff: Sony
- Defendant: GameMasters
- Civil Action - trademark and copyright infringement, contributory trademark and contributory copyright infringement, violation of the Digital Millennium Copyright Act, and state and federal unfair competition laws.

Sony v. GameMasters

The Game Enhancer

- "The Game Enhancer is an external device manufactured by numerous companies which, when plugged into the PlayStation game console, performs at least two functions."
  - Modify the rules of a specific game.
  - Permit players to play games sold in Japan or Europe and intended by SCEA for use exclusively in Japanese or European PlayStation consoles. "The PlayStation console is designed to operate only when encrypted data is read from a CD-ROM that verifies that the CD is an authorized, legitimate SCEA product licensed for distribution in the same geographical territory of the console's sale. Games not licensed for distribution in the same territory as that of the console's sale cannot be played on the PlayStation without a device such as the Game Enhancer."

Sony v. GameMasters

- Did Sony win as a matter of law on:
  - contributory copyright, or
  - trademark infringement?

Sony v. GameMasters

- "The Digital Millennium Copyright Act, among other things, prohibits distribution of any product or device which:
  1) is primarily designed or produced for the purpose of circumventing a technological measure (or a protection afforded by a technological measure) that effectively controls access to a system protected by a registered copyright or effectively protects a right of a copyright owner in a registered work or portion thereof;
  2) has only limited commercially significant purpose or use other than to circumvent such a technological measure (or protection afforded by it); or
  3) is marketed for use in circumventing such a technological measure (or protection afforded by it)." 17 U.S.C. §§ 1201(a)(2)-(3) and (b)(1)-(2) (Public Law 105-304, October 28, 1998)."
Sony v. GameMasters

• “Section 1201 also prohibits manufacture or distribution of technologies, products and services used to circumvent technological measures which control access. The prohibition applies only if such circumventing technologies are primarily designed for this purpose, have only limited commercial purpose beyond such circumventing purpose, or are marketed for the prohibited purpose. This provision is immediately effective. …”

Sony v. GameMasters

• Defendant concedes in its opposition papers that “[t]he Game Enhancer makes temporary modifications to the [PlayStation] computer program … [c]hanging these codes with the Game Enhancer does not alter the underlying software made by SONY.” …

• What is the Game Enhancer distinguishing feature?

• What does the Game Enhancer circumvent?

• At this stage, the Game Enhancer appears to be a device whose primary function is to circumvent “a technological measure (or a protection afforded by a technological measure) that effectively controls access to a system protected by a registered copyright….” 17 U.S.C. § 1201(a)(2)(A).

Sony v. GameMasters

• “Plaintiff has demonstrated that it is likely to prevail upon the merits of its claim that defendant's sale of the Game Enhancer violates the Digital Millennium Copyright Act. Title 17 of the United States Code section 1203 authorizes this Court to issue a preliminary injunction to prevent violations of the Digital Millennium Copyright Act. 17 U.S.C. § 1203.”

Questions to Ponder

• Does this decision sit well with you?

• Do you think it is fair for consumers that they can be restricted by Sony from playing back-up copies of their games or import titles?

• What happened to consumers’ fair use?

Lexmark v. Static Control Components

• Who are the parties and what do they do?
  – Lexmark
  – Static Control Components (SCC)

• What are the functions of the programs?
  – Toner Loading Program - calculates toner level in printers manufactured by Lexmark
  – Printer Engine Program - controls various printer functions on Lexmark printers
Lexmark v. Static Control Components

Background of the Dispute

- Lexmark began selling discount toner cartridges for its printers that only Lexmark could refill and that contained a microchip designed to prevent Lexmark printers from functioning with toner cartridges that Lexmark had not re-filled. In an effort to support the market for competing toner cartridges, Static Control Components (SCC) mimicked Lexmark’s computer chip and sold it to companies interested in selling remanufactured toner cartridges.
- Lexmark brought this action to enjoin the sale of SCC’s computer chip and raised three theories of liability in doing so. Lexmark claimed that:
  - SCC’s chip copied the Toner Loading Program in violation of the federal copyright statute.
  - SCC’s chip violated the DMCA by circumventing a technological measure designed to control access to the Toner Loading Program.
  - SCC’s chip violated the DMCA by circumventing a technological measure designed to control access to the Printer Engine Program.

Lexmark v. Static Control Components

• What is the difference between prebate and nonprebate?
• What type of protection did Lexmark obtain on the programs?

Lexmark v. Static Control Components

- “Lexmark uses an ‘authentication sequence’ that performs a ‘secret handshake’ between each Lexmark printer and a microchip on each Lexmark toner cartridge. Both the printer and the chip employ a publicly available encryption algorithm known as ‘Secure Hash Algorithm-1’ or ‘SHA-1,’ which calculates a ‘Message Authentication Code’ based on data in the microchip’s memory. If the code calculated by the microchip matches the code calculated by the printer, the printer functions normally. If the two values do not match, the printer returns an error message and will not operate, blocking consumers from using toner cartridges that Lexmark has not authorized. …”
• What did SCC do?

Lexmark v. Static Control Components

- The parties also agree that Lexmark has registered the Toner Loading Program with the Copyright Office, which is an infringement suit prerequisite, see 17 U.S.C. § 411(a), and which constitutes prima facie evidence of the copyright’s validity, see id. §410(c). And the parties agree that SCC shoulders the burden of rebutting the presumptive validity of Lexmark’s copyright. …
• “The parties also share common ground when it comes to most of the general principles of copyright infringement applicable to this case…”

Entitlement to Copyright Protection

- “As this case comes to the court, the parties agree that computer programs may be entitled to copyright protection as ‘literary works’ under 17 U.S.C. §101 and may be protected from infringement under 17 U.S.C. §106. And that is true with respect to a computer program’s object code … and its source code …”
Lexmark v. Static Control Components

• Even if it is original under 102(a), what about 102(b)?

In ascertaining this 'elusive boundary line' between idea and expression, between process and non-functional expression, courts have looked to two other staples of copyright law — the doctrines of merger and scenes a faire.

• "Where the 'expression is essential to the statement of the idea,' ... or where there is only one way or very few ways of expressing the idea, ... the idea and expression are said to have 'merged.' In these instances, copyright protection does not exist because granting protection to the expressive component of the work necessarily would extend protection to the work's uncopyrightable ideas as well. ..."

• "... In the computer-software context, the [scenes a faire] doctrine means that the elements of a program dictated by practical realities -- e.g., by hardware standards and mechanical specifications, software standards and compatibility requirements, computer manufacturer design standards, target industry practices, and standard computer programming practices -- may not obtain protection. ..."

Lexmark v. Static Control Components

• "The statute first prohibits the circumvention of "a technological measure that effectively controls access to a work protected [by copyright]." 17 U.S.C. § 1201(a)(1). The statute then prohibits selling devices that circumvent access-control measures:
  – 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 copyrighted work;
    (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a copyrighted work; or
    (C) is marketed by that person or another acting in concert with that person's knowledge for use in circumventing a technological measure that effectively controls access to a copyrighted work.
  – Id. § 1201(a)(2). The statute finally bans devices that circumvent "technological measures" protecting "right[s] of the copyright owner." Id. §1201(b). The last provision prohibits devices aimed at circumventing technological measures that allow some forms of "access" but restrict other uses of the copyrighted work, such as viewing, streaming media, which permits users to view or watch a copyrighted work but prevents them from downloading a permanent copy of the work.

Reverse Engineering Defenses

• "The statute also contains three "reverse engineering" defenses. A person may circumvent an access control measure "for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to that person." 17 U.S.C. § 1201(f)(1). A person "may develop and employ technological means" that are "necessary" to enable interoperability. Id. §1201(f)(2). And these technological means may be made available to others "solely for the purpose of enabling interoperability of an independently created computer program with other programs." Id. §1201(f)(3). All three defenses apply only when traditional copyright infringement does not occur and only when the challenged actions (in the case of the third provision) would not violate other "applicable laws." ..."
Lexmark v. Static Control Components

• What did Lexmark argue in its complaint?
  
  "... It is not Lexmark’s authentication sequence that “controls access” to the Printer Engine Program. See 17 U.S.C. §1201(a)(2). It is the purchase of a Lexmark printer that allows “access” to the program. Anyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence, and the data from the program may be translated into readable source code after which copies may be freely distributed. ... No security device, in other words, protects access to the Printer Engine Program Code and no security device accordingly must be circumvented to obtain access to that program code."

Lexmark v. Static Control Components

Distinguish #1

• "In the essential setting where the DMCA applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation of the code's execution. ... [T]he DMCA applies in [] settings when the product manufacturer prevents all access to the copyrightable material and the alleged infringer responds by marketing a device that circumvents the technological measure designed to guard access to the copyrightable material."

Lexmark v. Static Control Components

Distinguish #2

• "The copyrightable expression in the Printer Engine Program, by contrast, operates on only one plane: in the literal elements of the program, its source and object code. Unlike the code underlying video games or DVDs, "using" or executing the Printer Engine Program does not in turn create any protected expression. ... And unlike the code underlying video games or DVDs, no encryption or other technological measure prevents access to the Printer Engine Program. Presumably, it is precisely because the Printer Engine Program is not a conduit to protectable expression that explains why Lexmark (or any other printer company) would not block access to the computer software that makes the printer work. Because Lexmark's authentication sequence does not restrict access to this literal code, the DMCA does not apply."

Lexmark v. Static Control Components

• Legislative History
  
  "Nowhere in its deliberations over the DMCA did Congress express an interest in creating liability for the circumvention of technological measures designed to prevent consumers from using consumer goods while leaving the copyrightable content of a work unprotected. ..."

DMCA Rulemaking

• DMCA Rulemaking establishes exemptions in 2000, 2003, 2006, and 2010
  
  • Rule makings conducted in
  
  • Current rulemaking (2012) is located here:
Current Exemptions

a) Literary Works Distributed Electronically—Assistive Technologies
b) Wireless Telephone Handsets—Software Interoperability
c) Wireless Telephone Handsets—Interoperability With Alternative Networks
d) Motion Picture Excerpts—Commentary, Criticism, and Educational Uses
e) Motion Pictures and Other Audiovisual Works—Captioning and Descriptive Audio

Exemptions Considered but Not Implemented

a) Literary Works in the Public Domain—Digital Access
b) Video Game Consoles—Software Interoperability
c) Personal Computing Devices—Software Interoperability
d) Motion Pictures and Other Works on DVDs and Other Media—Space Shifting

Part 2

• Limitations on liability relating to material online §512

Background of “Hypothetical Dispute”

• CS317-ISP (i.e., the client) recently provided us (client’s counsel) with an e-mail it received from NetPD (enforcer of copyrights). In the e-mail, NetPD advised CS317-ISP that a digital audio file in which one of its clients (computer user) has rights was located on one of CS317-ISP’s servers and that the e-mail should be construed as notice under the Digital Millennium Copyright Act (“DMCA”) and requested that certain actions should be taken by CS317-ISP. We have been asked by CS317-ISP to determine how it should respond to this message.

ISPs and the DMCA

• Internet Service Providers (ISPs) are concerned with their liability for subscribers who use their resources to commit unlawful acts. The greatest concern has been liability for copyright infringement, as their users transmit a vast amount of material through the Internet and it is impractical to screen out infringing material. The law was unprepared for the wealth and speed of material available on the Internet and, as a result, legal reform was necessary to protect ISPs from liability from actions taken by their subscribers.

ISPs and the DMCA

• Congress responded to the plight of ISPs by introducing legislation that would provide them with “safe harbors” (i.e., exemptions) that would shield them from liability in certain circumstances. In 1998, the Online Copyright Infringement Liability Limitation Act (OCILLA) was signed into law as part of the Digital Millennium Copyright Act and provided safe harbors to protect ISPs in four distinct circumstances: (a) transitory digital network communications, (b) system caching, (c) information residing on systems or networks at direction of users, and (d) information location tools. OCILLA was written into law as 17 U.S.C. §512, which appears in its entirety in the Appendix.
Introduction

Various prerequisites are necessary for ISPs to take advantage of some of the safe harbors including designating an agent with the Copyright Office to receive service, receiving sufficient notice from a copyright owner to react in the prescribed statutory manner, complying with standard technical measures, and having an anti-infringement policy in effect. Below we determine whether or not CS317-ISP has met the prerequisites to take advantage of any safe harbors.

**Prerequisites**

**Designated Agent**
- CS317-ISP must have registered a designated agent with the Copyright Office pursuant to §512(c)(2) to take advantage of the safe harbor for information residing on systems or networks at direction of users (i.e., §512(c)). We have reviewed the Service Provider Agent List at the Copyright Office and CS317-ISP is not listed.
- Without designating an agent, CS317-ISP is unable to receive the exemption for information residing on systems or networks at direction of users with the present matter. However, as will be further explained below, this exemption is immaterial with respect to the present notice received from NetPD as the notice relates to the exemption for transitory digital network communications (i.e., §512(a)).

**Sufficiency of Notice Provided by NetPD**
- The e-mail received from NetPD states that its letter “constitutes notice to [CS317-ISP] that [the indicated] site operator maybe be liable for the infringing activity occurring on [CS317-ISP’s] server.” Therefore, we consider the implications of the e-mail and whether (i) CS317-ISP has received "sufficient notice" such it will be deemed to have knowledge of infringing material on its system, and (ii) the effect, if any, of receiving actual knowledge of the infringing material on its system.

**CS317-ISP Must Not Interfere with Standard Technical Measures**
- Pursuant to §512(i)(1)(B), CS317-ISP must accommodate and not interfere with “standard technical measures”. In the future, it is intended that standard technical measures will be used by copyright owners to identify or protect their copyrighted works. However, this is not at issue at the present time because there is yet to be a standard means for protecting copyrighted works. We should re-evaluate this factor when there is a general consensus as to what are standard technical measures.
Prerequisites

CS317-ISP Must Have an Anti-Infringement Policy in Effect

- For CS317-ISP to use the OCILLA exemptions, under §512(i)(1)(A) it must have adopted and reasonably implemented "a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers." We are unaware of how CS317-ISP informs its subscribers and account holders of its AUP.

Prerequisites

- However, CS317-ISP should adopt the following means of notifying its subscribers of the AUP:
  1. E-mail subscribers when the AUP has been modified;
  2. Create a version number and last updated date for the AUP so subscribers to view the AUP online will know whether it has changed since the last time they reviewed it;
  3. Provide a link to the AUP on an easily locatable section of the website (e.g., such as the front page of the website); and
  4. Make sure that before users gain access to CS317-ISP’s system (i.e., by becoming subscribers) that they agree to the AUP such as through a click wrap agreement.

- By following steps 1-4 above, CS317-ISP will more clearly comply with this prerequisite as well as follow better internet practices by effectively alerting its subscribers of its policies currently in effect.

Prerequisites

• Next, we consider whether CS317-ISP’s AUP complies with the requirements of OCILLA. Sections 8.1 of the AUP allows CS317-ISP to “deny [a] subscriber access to all or part of [CS317-ISP] service without notice if [the] subscriber engages in any conduct or activities that [CS317-ISP] in its sole discretion believes violates any of the terms and conditions in this AUP.”

• Thus, pursuant to Section 8.1, CS317-ISP can terminate a subscriber who, according to Section 1.1, “posts, transmits, re-transmits or stores material on or through [the CS317-ISP] system services or products that: (i) is in violation of any local, state, federal or non-United law or regulation; (ii) threatening, obscene, indecent, defamatory or that otherwise could adversely affect any individual, group or entity (collectively, “Persons”); or (iii) violates the rights of any person including rights protected by copyright, trade secret, patent or other intellectual property or similar laws or regulations including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by [subscriber].” Therefore, it appears as though CS317-ISP has met the anti-infringement requirement.

Summary of the Safe Harbors

• OCILLA provides safe harbors to ISPs in four distinct circumstances: transitory digital network communications (i.e., §512(a)), system caching (i.e., §512(b)), information residing on systems or networks at direction of users (i.e., §512(c)), and information location tools (i.e., §512(d)). It is not necessary to obtain all four safe harbors to avoid liability.

• Rather, when the behavior of an ISP falls within a particular safe harbor, that behavior will be exempted harbor if the ISP meets the prerequisites for obtaining the safe harbor as well as the particular requirements of the specific safe harbor.

• Below we review whether CS317-ISP’s behavior falls within any of the safe harbors and whether the safe harbors are met.

SAFE HARBOR 512(a): Transitory Digital Network Communications

Background

• As discussed above, CS317-ISP has met the prerequisites to take advantage of the safe harbor for transitory digital network communications. We must consider whether the complained of behavior falls within this particular exemption for transitory digital network communications, and whether CS317-ISP has met the requirements to take advantage of this exemption.
SAFE HARBOR 512(a): Transitory Digital Network Communications

Requirement #1: CS317-ISP Must Be A “Service Provider”
- The first requirement for CS317-ISP to qualify as a "service provider" under 512(k)(1)(A) is that it must be an "entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user’s choosing, without modification to the content of the material as sent or received.” CS317-ISP provides the services listed above and is a service provider with respect to this exemption.

SAFE HARBOR 512(a): Transitory Digital Network Communications

Requirement #2: Transmission of Material Through CS317-ISP’s System
- The second requirement for CS317-ISP to fall within the transitory digital network communications exemption is that its subscriber’s behavior must stem from CS317-ISP providing services for the "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections.” With respect to the message received from NetPD, the subscriber was using CS317-ISP’s Internet Access to connect to the Internet and thus was "provided a connection" by CS317-ISP. The subscriber transferred the MP3 file by using its connection provided by CS317-ISP. Therefore, CS317-ISP’s relation to the subscriber’s behavior falls within this exemption.

SAFE HARBOR 512(a): Transitory Digital Network Communications

Requirement #3: Transmission Must Be Eligible
- The third and final requirement for CS317-ISP to obtain the transitory digital network communications exemption is the “transmission” part of §512(a): (1) the transmission of the material was initiated by or at the direction of a person other than the service provider; (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider; (3) the service provider does not select the recipients of the material except as an automatic response to the request of another person; (4) no copy of the material made in intermediate or transient storage in a manner that is ordinarily accessible to anyone other than anticipated recipients, nor does it maintain a copy of material on a system or network in a manner ordinarily accessible to anyone other than anticipated recipients, for does it maintain a copy of material on its system for a longer period than is reasonably necessary for a transmission. Finally, the material is transmitted through CS317-ISP’s system without modification. Therefore, CS317-ISP has complied with the above five elements with respect to the transmission of the allegedly infringing MP3 file.

SAFE HARBOR 512(a): Transitory Digital Network Communications

Safe Harbor is Met
- CS317-ISP has met the necessary requirements of the transitory digital network communications exemption because it is a service provider, the material was transmitted through its system and the transmission is eligible. Therefore, CS317-ISP is not liable for monetary relief (including without limitation damages, costs and attorneys’ fees) for the actions taken by its subscriber while using Aimster.

SAFE HARBOR 512(b): System Caching

Background
- The second safe harbor (i.e., 512(b)) is for “system caching” and limits the liability for copyright infringement of a service provider by reason of the immediate and temporary storage of material on a system or network controlled or operated by or for the service provider…
SAFE HARBOR 512(b): System Caching

Safe Harbor is Not Relevant

• NetPD has not complained about CS317-ISP’s system caching but rather has complained of the behavior of a CS317-ISP subscriber with respect to one of its copyrighted MP3 digital audio files. Thus, as CS317-ISP’s behavior does not fall within this safe harbor, this exemption will not shield CS317-ISP from liability from the complained of activity and therefore will not be further considered herein. However, we recommend that CS317-ISP provide us with a written description of its policy of system caching so that we can compare it against this exemption as a prophylactic measure against a possible future system caching complaint.

SAFE HARBOR 512(c): Information Residing on Systems or Networks at Direction of Users

Safe Harbor is Not Relevant

• NetPD’s message seems to complain of a file stored on CS317-ISP system. However, as outlined above, the file was not stored on CS317-ISP’s system but was rather transferred through CS317-ISP’s system. Therefore, the exemption for information residing on systems or networks at direction of users is not relevant to the message received from NetPD.

SAFE HARBOR 512(d): Information Location Tools

Background

• The fourth and final safe harbor (i.e., 512(d)) is for “information location tools” and limits the liability for copyright infringement of a service provider by reason of it “referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link.”

SAFE HARBOR 512(c): Information Residing on Systems or Networks at Direction of Users

Important Safe Harbor Note

• A future analysis under 512(c) will be vastly different from 512(a) and it will be necessary to prepare a different response to both the subscriber and the copyright owner. CS317-ISP should consider providing us with a copy of any such notices it receives so that we can make a determination as to what action should be taken.
Injunctive Relief for NetPD

- We have concluded that under the exemption for transitory digital network communications, CS317-ISP is not monetarily liable for the behavior of CS317-ISP’s subscriber. However, we have not addressed the issue of injunctive relief.
- Under §502 of the Copyright Act, courts can grant temporary and final injunctions to prevent or restrain infringement of copyrights. However, §512(i)(B) of the DMCA limits the injunctive relief available to copyright owners when a service provider qualifies for the transitory digital network communications exemption.
- With appropriate court action, NetPD could potentially obtain an order restraining CS317-ISP from providing access to the subscriber who transmitted the infringing file by ordering CS317-ISP to terminate its subscriber’s account.
- Therefore, if CS317-ISP refuses to comply with NetPD’s demands, NetPD could take CS317-ISP to court to force the termination of the subscriber’s Internet access.

CS317-ISP’s Actions Against the Subscriber

Determine the Identity of the Subscriber

- CS317-ISP should review the necessary information such as server logs to determine the subscriber responsible for transferring the allegedly infringing file. If the subscriber can be identified, this subscriber’s account information and the notice received from the copyright owner should be stored in a special file and retained indefinitely.

Provide the Subscriber With Notice

- Once the subscriber is identified, CS317-ISP should send a warning notice to the subscriber advising him or her of the message received from NetPD. If CS317-ISP receives such a notice, it will need to expeditiously disclose to NetPD the information required by the subpoena. If CS317-ISP receives such a notice, it should contact us immediately.

Future Infringement by the Subscriber

- We propose the following plan for reprimanding “repeat infringers.” If the subscriber is cited a third time for copyright infringement within a twelve-month period, CS317-ISP should suspend the subscriber’s account for a period of thirty days. If the subscriber is cited a fourth time for copyright infringement during a twelve-month period, the subscriber can be identified, this subscriber’s account information and the notice received from the copyright owner should be stored in a special file and retained indefinitely.

- As previously mentioned, NetPD has requested that CS317-ISP should adopt the above-mentioned plan or something similar to it for reprimanding repeat infringers. If CS317-ISP does not take significant action against subscribers who are repeat infringers, under §512(e)(4)(A) it could lose its ability to take advantage of the safe harbors contained in §512.

Receiving Subpoena from NetPD

- Under §512(h), NetPD could request a district court to issue a subpoena to CS317-ISP to identify an alleged infringer. Should CS317-ISP receive such a subpoena, it will need to confirm with NetPD the information required by the subpoena. If CS317-ISP receives such a notice, it should contact us immediately.

CS317-ISP’s Response to NetPD

- With respect to the first request, CS317-ISP should send a warning notice to the subscriber advising him or her of the message received from NetPD. With respect to the second request, CS317-ISP should send a warning notice to the subscriber advising him or her of the message received from NetPD. With respect to the third request, CS317-ISP should not confirm whether the infringing activity has ceased.
- With respect to the first request, CS317-ISP should not confirm whether the infringing activity has ceased.
- With respect to the second request, CS317-ISP can confirm that it has notified the subscriber of its infringing activity. Finally, with respect to the third request, CS317-ISP should not confirm whether the infringing activity has ceased.
Conclusion

- We believe under the safe harbor for transitory digital network communications (i.e., 512(a)) that CS317-ISP is not liable for the behavior of one of its subscribers with respect to his or her transferring of a digital MP3 sound file using the Aimster protocol. We have also prepared a warning notice for CS317-ISP to send to the infringer, along with a proposed response that we wish to send on CS317-ISP's behalf to NetPD. With respect to future notices received by copyrights owners, we strongly urge CS317-ISP to provide us with a copy of the notice received so that we determine an appropriate response.

UMG v. Shelter Capital Partners

- Veoh
  - website that enables users to share videos
  - implemented various procedures to prevent copyright infringement through its system
- Universal Music Group (UMG)
  - recorded music and music publishing

UMG v. Shelter Capital Partners

- Background
  - users in the past have downloaded videos without UMG's authorization that include UMG songs
  - UMG sued for direct and secondary copyright infringement
  - DC ruled in favor of Veoh under DMCA 512(c)

UMG v. Shelter Capital Partners

- How does Veoh work?
  - View videos uploaded by users and partner content
  - Content viewed through standalone software application or Veoh website
  - Veoh makes money through advertising
- What kind of agreements must the User agree to before sharing material?

UMG v. Shelter Capital Partners

- What happens when a video is uploaded?
  - transcoding
  - extraction of metadata
  - assignment of a web address
- Do Veoh employees review videos before they are made publically available?
UMG v. Shelter Capital Partners

• How are videos made available?
  – streaming
  – downloading

• How is copyright infringement automatically prevented?
  – hash filtering
  – audio fingerprinting

• Veoh filtered backlog of content with audio fingerprinting and removed 60K files

UMG v. Shelter Capital Partners

• Who else did UMG sue?
  – Three of Veoh’s investors as defendants on theories of secondary liability

UMG v. Shelter Capital Partners

• 512(c)
  (1) In general. — A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if
  • (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
  • (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or
  • (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

• (B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

• (C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

UMG v. Shelter Capital Partners

• What are UMG’s arguments?
  1. the alleged infringing activities do not fall within the plain meaning of "infringement of copyright by reason of the storage [of material] at the direction of a user"
  2. genuine issues of fact remain about whether Veoh had actual knowledge of infringement, or was "aware of facts or circumstances from which infringing activity [was] apparent"
  3. Veoh "receive[d] a financial benefit directly attributable to . . . infringing activity" that it had the right and ability to control under § 512(c)(1)(B).
UMG v. Shelter Capital Partners

- Do the functions of Veoh’s software destroy storage at the direction of users?
  - No, because by reason of storage and the infringer does not have to conduct the storage
- “We hold that the language and structure of the statute, as well as the legislative intent that motivated its enactment, clarify that § 512(c) encompasses the access-facilitating processes that automatically occur when a user uploads a video to Veoh.”

UMG v. Shelter Capital Partners

- What about actual knowledge?
  - UMG argues that Veoh had knowledge or awareness of other infringing videos that it did not remove
  - UMG failed to rebut Veoh’s showing “that when it did acquire knowledge of allegedly infringing material — whether from DMCA notices, informal notices, or other means — it expeditiously removed such material.”
  - “We therefore hold that merely hosting a category of copyrightable content, such as music videos, with the general knowledge that one’s services could be used to share infringing material, is insufficient to meet the actual knowledge requirement under § 512(c)(1)(A)(i).”
- “[W]e hold that Veoh’s general knowledge that it hosted copyrightable material and that its services could be used for infringement is insufficient to constitute a red flag.”

UMG v. Shelter Capital Partners

- What about financial benefit directly attributable to an infringing activity?
- “[W]e hold that the ‘right and ability to control’ under § 512(c) requires control over specific infringing activity the provider knows about. A service provider’s general right and ability to remove materials from its services is, alone, insufficient. Of course, a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge.”

Capitol Records, Inc. v. MP3Tunes

- Case History
- S.D.NY
  - October 25, 2011 order
  - Reconsideration of order
- “EMI’s motion is granted in part and denied in part and Robertson’s motions are granted in part and denied in part.”

Capitol Records, Inc. v. MP3Tunes

- Willful blindness
- “In Viacom, the Second Circuit considered the ‘application of the common law willful blindness doctrine in the DMCA context’ as an issue of first impression and held that ‘the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA.’ … Thus, where a service provider is ‘aware of a high probability of the fact [of infringement] and consciously avoid[s] confirming that fact,’ that provider is willfully blind to infringement and may lose the protections of the safe harbor.”
Capitol Records, Inc. v. MP3Tunes

- "Red Flag" Knowledge of Infringement
  - Service providers can lose the protection of the DMCA safe harbors if they have actual or apparent (also called 'red flag') knowledge of infringing content.
  - Formal take down notices only, or internal and third-party communications regarding the content?

Capitol Records, Inc. v. MP3Tunes

- Not through general awareness of infringement occurring
  - "Subjective/Objective" standard - "the actual knowledge provision turns on whether the provider actually or 'subjectively' knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."

Capitol Records, Inc. v. MP3Tunes

- "This Court is aware of no authority for the proposition that the DMCA safe harbor is per se unavailable in an inducement claim, or that evidence of inducement would obviate the requirement to prove actual or red flag knowledge of infringement."

Capitol Records, Inc. v. MP3Tunes

- "In Viacom, the Second Circuit concluded that the § 512(c) safe harbor 'is clearly meant to cover more than mere electronic storage lockers.' ... Rather, its protections 'extend[] to software functions performed for the purpose of facilitating access to user-stored material'".
  - "This Court declines to rule that MP3tunes' cover art algorithm is shielded by the § 512(c) safe harbor."

Program Completed

All course materials - Copyright 2000-14 Randy L. Canis, Esq.