INTERNET LAW: SPRING 2010
PROFESSOR GRIMMELMANN
NEW YORK LAW SCHOOL

READING PACKET 6

COPYRIGHT AND NETWORK NEUTRALITY

Contents

United States Code, Selected Sections **4**

17 U.S.C. § 106 4
17 U.S.C. § 107 4
17 U.S.C. § 512 4
17 U.S.C. § 1201 8

Class 23: Copyright Principles **10**

Copyright primer 11
MAI Sys. Corp. v. Peak Computer, Inc. 13
Perfect 10, Inc. v. Amazon.com, Inc. 15
A & M Records, Inc. v. Napster, Inc. 21

Class 24: Secondary Liability **26**

A & M Records, Inc. v. Napster, Inc. 27
VISA problem 36
Rip-Mix-Burn problem 37

Class 25: Open Source and Anti-Circumvention **38**

ISC License 39
GNU General Public License (GPL) 39
Jacobsen v. Katzer 41
Universal City Studios, Inc. v. Corley 46
Universal City Studios, Inc. v. Reimerdes 49

Class 26: Section 512 ..... **55**

Lenz v. Universal Music Corp. 56
Perfect 10, Inc. v. CCBill LLC 59
Section 512 problems 70

Class 27: Network Neutrality **72**

In re Formal Complaint of Free Press and Public Knowledge 72
Network Management problem 79
iPhone problem 80

17 U.S.C. § 106
Exclusive rights in copyrighted works

Subject to sections 107 through 122, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following:

(1) to reproduce the copyrighted work in copies or phonorecords; ...

(3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;

(4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;

(5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; ...

17 U.S.C. § 107
Limitations on exclusive rights: Fair use

Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.

17 U.S.C. § 512
Limitations on liability relating to material online

(a) Transitory Digital Network Communications.— A service provider shall not be liable ... for infringement of copyright by reason of the provider's 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, if [the transmission is initiated by a user, automatic, sent to recipients selected by the user, made accessible only to recipients and deleted promptly from the provider's system, and unmodified]. ...

(c) Information Residing on Systems or Networks At Direction of Users.—

(1) In general.— A service provider shall not be liable ... 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 the service provider—

(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. ...

(3) Elements of notification.—

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed. ...

(d) Information Location Tools.— 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 provider 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, if the service provider [compiles with the procedures given in subsection (c), above]. ...

(f) Misrepresentations.— Any person who knowingly materially misrepresents under this section—

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

(g) Replacement of Removed or Disabled Material and Limitation on Other Liability.—

(1) No liability for taking down generally.— Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

(2) Exception.— Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider—

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will replace the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice,

unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) Contents of counter notification.— To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on other liability.— A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(i) Conditions for Eligibility.—

(1) Accommodation of technology.— The limitations on liability established by this section shall apply to a service provider only if the service provider—

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, 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; and

(B) accommodates and does not interfere with standard technical measures. ...

(k) Definitions.—

(1) Service provider.—

(A) As used in subsection (a), the term "service provider" means 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.

(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A). ...

(l) Other Defenses Not Affected.— The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

17 U.S.C. § 1201
Circumvention of copyright protection systems

(a) Violations Regarding Circumvention of Technological Measures.—

(1)

(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

...

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection—

(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; and

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

CLASS 23: COPYRIGHT PRINCIPLES

Out of all our topics in this course, copyright on the Internet is the one that could most easily be a course unto itself. Almost every facet of copyright doctrine (which was complicated to begin with) has been challenged by the Internet. We can't possibly hope to cover all of these twists and turns. Instead, our tour of digital copyright will focus on giving you the basic framework and introducing you to the defining issues of the last decade.

Preparation questions

(1) Start by reading the copyright primer. It omits most of the details, but it shows you the basic framework for copyright analysis. The first task is to assign responsibility for any direct infringements. *MAI* starts that process off by helping us consider what activities raise atcopyright issue at all. After *MAI*, which of the following could be a "reproduction" that infringes copyright, and which could not?

- Reading a book?
- Photocopying a chapter from a textbook?
- Singing a song in the shower?
- Running a computer program?
- Burning a set of MP3s to a CD?
- Ripping a CD to a computer?
- Downloading (using right-click "save as") a video file?
- Browsing to a web page that contains pictures?

(2) Note that "reproduction" is not the only way to be a direct infringer. You can also infringe, *inter alia*, by engaging in public performance, public display, or public distribution without necessarily "reproducing" anything. Whichever of these exclusive rights is at stake, the mere fact that a reproduction or a performance (or etc.) has taken place doesn't necessarily tell us *who* has engaged in it, and is thus the direct infringer. The first part of *Perfect 10* gives us a cut at this question. The works here are pornographic images copyrighted by Perfect 10. How did the alleged infringement of *thumbnail* images take place? Who is a direct infringer: Google, the user, or both? Next, how did the alleged infringement of the *full-size* images take place? Draw a picture. What's the role of the bootleg web sites, users, and Google in this process? What's Perfect 10's theory of Google's liability, and why does the court reject it? Are the bootleg web sites direct infringers? What about the users?

(3) A finding of direct infringement can be negated if the defendant shows that her use is a *fair use*. This complicated, vexing, indispensable doctrine may take some time to wrap your head around. It's case-by-case, and not all successful fair use defenses look the same. We'll talk about two general species. One—also considered in *Perfect 10*—protects socially useful "transformative" uses. The idea that a search engine could make a transformative use when it shows thumbnails would have shocked a previous generation of copyright lawyers. But it seems to be taking tentative hold in the courts, with *Perfect 10* its high-water mark thus far. Why does Google win on this issue? Are you convinced that this is a "transformative" use

entitled to the law's special solicitude? What about the harm to Perfect 10's marketing of its works?

(4) Another, important face of fair use is personal uses. In the landmark *Sony* case, the Supreme Court held that noncommercial taping an over-the-air television program for later viewing is a fair use. In the *Napster* opinion, the Ninth Circuit rejects *Sony*-style arguments made by Napster. (We'll talk about Napster's liability vis-a-vis its users next time, as it requires some architectural details. For the time being, treat the opinion purely as a question of whether the users are infringers or not.) Napster provides two major proposed fair uses: sampling and space-shifting. How does the court distinguish those uses from the time-shifting held to be a fair use in *Sony*?

Copyright primer

Even more so than elsewhere in the course, almost everything in this primer is a deliberate over-simplification. There are almost always complications and exceptions. The goal here is to show you how all the various tests and doctrines fit together. Understand that when you confront these issues in practice, you'll care about details barely even hinted at here.

Copyright starts from the axiom that *original works of authorship* are copyrightable. 17 U.S.C. § 102. We won't unpack what "original" or "authorship" means. For our purposes, the key distinction is between significantly creative "works"—novels, songs, and sculptures, for example—and facts that no one creates, like the temperature in Times Square at 5:30 PM on March 15, 1994. The former are copyrightable, the latter aren't.

Once a work is copyrighted, the copyright owner has a set of six exclusive rights spelled out in 17 U.S.C. § 106. "Use" is not one of them; it has never been copyright infringement to read a book. Instead, an infringer is one who violates one or more of the exclusive rights. The first and easiest-to-understand is the *reproduction* right: to "reproduce the copyrighted work in copies." 17 U.S.C. § 106(1). We'll also be concerned with the *public distribution*, *public display*, and *public performance* rights. 17 U.S.C. § 106(3)–(5). Note that the statutory language of all three includes the words "to the public" or "publicly." Purely private distributions, displays, and performances are not infringements. Here's how the Copyright Act explains the difference:

> To perform or display a work "publicly" means—
>
> (1) to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered; or
>
> (2) to transmit or otherwise communicate a performance or display of the work to a place specified by clause (1) or to the public, by means of any device or process ...

To analyze an infringement case, start by asking whether you can find a *direct infringer*, i.e., someone who personally does something prohibited by one of the exclusive rights. The prototypical direct infringer is the pirate publisher: someone who prints and sells thousands of unauthorized copies of a book. The printing is an infringement of the reproduction right, regardless of whether the copies are sold; the sales are a infringement of the distribution right.

At this stage, you should be checking whether the alleged direct infringer has any valid defenses. Obviously, permission of the copyright holder is a complete defense. In copyright terms, the copyright owner's permission is a *license* to engage in acts that would otherwise constitute infringement. Licenses can be explicit or implicit.

Another common defense is *fair use*, a complex and very case-specific defense that requires the court to balance four statutory factors. 17 U.S.C. § 107. These factors tend to favor certain kinds of defendants, such as reviewers who quote from the book they're discussing in their reviews.

A third defense to consider is *first sale*: once the copyright owner has legitimately sold a copy of a work, she has no further right to restrict the distribution of *that copy*. Thus, the owner of the copy is free to sell it, give it away, lend it, etc.

If there's a direct infringer, next you need to consider whether anyone else is a *secondary infringer*. Four doctrines make these secondary infringers jointly and severally liable with the primary infringers:

- One, so invisible that courts and lawyers rarely mention it, is *respondeat superior*. Employers are liable for the torts committed by their employees within the scope of their employment. Courts also implicitly apply this rule to computer systems. If you r company owns a computer and your employees program the computer to make infringing copies, the company is liable.

- A *vicarious* infringer (a) has the *right and ability to control* the infringing acts and (b) stands to gain a *direct financial benefit* from the infringement. This doctrine is an extension of *respondeat superior*, but it can cover cases in which there's no employment relationship. The classic cases here are the "dance hall cases," in which a nightclub hires a band that includes infringing songs in its set. The nightclub could have supervised the band more closely, and the nightclub profited because people came to see the band play.

- A *contributory* infringer (a) *materially contributes* to the infringement and (b) had *knowledge* of the infringement. A classic example of a contributory infringer is a store that rents high-speed audio cassette duplicating machines and sells large numbers of blank cassettes pre-timed to be the exact same length as particular major-label albums. The store is directly helping its customers make unauthorized copies, and clearly knows that that's what they're up to. We will talk, in some detail, about what "knowledge" means or might mean here.

- An *inducing* infringer distributes a device (a) with the *object of promoting infringement* (b) as shown by *clear expression or other affirmative steps* taken to foster infringement. This is a souped-up version of contributory infringement (so some courts and commentators treat it as a subset of contributory infringement). This is the most recent of these three doctrines, and the least well fleshed-out.

As these doctrines have developed, contributory infringement—but *not* vicarious or inducement infringement—has been subject to the *substantial non-infringing uses* (or *Sony*) defense. One who merely supplies a device is not liable for the resulting infringements, so long as the device is capable substantial non-infringing uses. To understand this defense, think about the cassette store, above. The high-speed tape duplicators have substantial non-infringing uses (e.g. a motivational speaker trying to self-distribute her talks). The pre-cut cassette tapes don't; they're designed to be useful for copying popular albums, and nothing else.

There will be more, but that's enough to start with ...

MAI Sys. Corp. v. Peak Computer, Inc.
991 F. 2d 511 (9th Cir. 1993)

MAI Systems Corp., until recently, manufactured computers and designed software to run those computers. The company continues to service its computers and the software necessary to operate the computers. MAI software includes operating system software, which is necessary to run any other program on the computer.

Peak Computer, Inc. is a company organized in 1990 that maintains computer systems for its clients. Peak maintains MAI computers for more than one hundred clients in Southern California. This accounts for between fifty and seventy percent of Peak's business.

Peak's service of MAI computers includes routine maintenance and emergency repairs. Malfunctions often are related to the failure of circuit boards inside the computers, and it may be necessary for a Peak technician to operate the computer and its operating system software in order to service the machine. ...

IV. COPYRIGHT INFRINGEMENT

The district court granted summary judgment in favor of MAI on its claims of copyright infringement and issued a permanent injunction against Peak on these claims. The alleged copyright violations include: (1) Peak's running of MAI software licenced to Peak customers; (2) Peak's use of unlicensed software at its headquarters; and, (3) Peak's loaning of MAI computers and software to its customers. Each of these alleged violations must be considered separately.

A. Peak's running of MAI software licenced to Peak customers

To prevail on a claim of copyright infringement, a plaintiff must prove ownership of a copyright and a "'copying' of protectable expression" beyond the scope of a license. *S.O.S., Inc. v. Payday, Inc.*, 886 F.2d 1081, 1085 (9th Cir.1989).

MAI software licenses allow MAI customers to use the software for their own internal information processing. This allowed use necessarily includes the loading of the software into the computer's random access memory ("RAM") by a MAI customer. However, MAI software licenses do not allow for the use or copying of MAI software by third parties such as Peak. Therefore, any "copying" done by Peak is "beyond the scope" of the license.

It is not disputed that MAI owns the copyright to the software at issue here, however, Peak vigorously disputes the district court's conclusion that a "copying" occurred under the Copyright Act.

The Copyright Act defines "copies" as:

> material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device.

17 U.S.C. § 101.

The Copyright Act then explains:

> A work is "fixed" in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.

17 U.S.C. § 101.

The district court's grant of summary judgment on MAI's claims of copyright infringement reflects its conclusion that a "copying" for purposes of copyright law occurs when a computer program is transferred from a permanent storage device to a computer's RAM. This conclusion is consistent with its finding, in granting the preliminary injunction, that: "the loading of copyrighted computer software from a storage medium (hard disk, floppy disk, or read only memory) into the memory of a central processing unit ("CPU") causes a copy to be made. In the absence of ownership of the copyright or express permission by license, such acts constitute copyright infringement." We find that this conclusion is supported by the record and by the law.

Peak concedes that in maintaining its customer's computers, it uses MAI operating software "to the extent that the repair and maintenance process necessarily involves turning on the computer to make sure it is functional and thereby running the operating system." It is also uncontroverted that when the computer is turned on the operating system is loaded into the computer's RAM. As part of diagnosing a computer problem at the customer site, the Peak technician runs the computer's operating system software, allowing the technician to view the systems error log, which is part of the operating system, thereby enabling the technician to diagnose the problem.

Peak argues that this loading of copyrighted software does not constitute a copyright violation because the "copy" created in RAM is not "fixed." However, by showing that Peak loads the software into the RAM and is then able to view the system error log and diagnose the problem with the computer, MAI has adequately shown that the representation created in the RAM is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration."

After reviewing the record, we find no specific facts (and Peak points to none) which indicate that the copy created in the RAM is not fixed. ...

The law also supports the conclusion that Peak's loading of copyrighted software into RAM creates a "copy" of that software in violation of the Copyright Act. In *Apple Computer, Inc. v. Formula Int'l, Inc.*, 594 F. Supp. 617, 621 (C.D.Cal.1984), the district court ... stated:

> RAM can be simply defined as a computer component in which data and computer programs can be temporarily recorded. Thus, the purchaser of [software] desiring to utilize all of the programs on the diskette could arrange to copy [the software] into RAM. This would only be a temporary fixation. It is a property of RAM that when the computer is turned off, the copy of the program recorded in RAM is lost.

Apple Computer at 622.

While we recognize that this language is not dispositive, it supports the view that the copy made in RAM is "fixed" and qualifies as a copy under the Copyright Act.

We have found no case which specifically holds that the copying of software into RAM creates a "copy" under the Copyright Act. However, it is generally accepted that the loading of software into a computer constitutes the creation of a copy under the Copyright Act. *See e.g. Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255, 260 (5th Cir.1988) ("the act of loading a program from a medium of storage into a computer's memory creates a copy of the program"); 2 Nimmer on Copyright, § 8.08 at 8-105 (1983) ("Inputting a computer program entails the preparation of a copy."); Final Report of the National Commission on the New Technological Uses of Copyrighted Works, at 13 (1978) ("the placement of a work into a computer is the preparation of a copy"). We recognize that these authorities are somewhat troubling since they do not specify that a copy is created regardless of whether the software is loaded into the RAM, the hard disk or the read only memory ("ROM"). However, since we find that the copy created in the RAM can be "perceived, reproduced, or otherwise communicated," we hold that the loading of software into the RAM creates a copy under the Copyright Act. 17 U.S.C. § 101. We affirm the district court's grant of summary judgment as well as the permanent injunction as it relates to this issue. ...

Perfect 10, Inc. v. Amazon.com, Inc.
487 F.3d 701 (9th Cir. 2007)

IKUTA, Circuit Judge.

In this appeal, we consider a copyright owner's efforts to stop an Internet search engine from facilitating access to infringing images. Perfect 10, Inc. sued Google Inc., for infringing Perfect 10's copyrighted photographs of nude models, among other claims. ... The district court preliminarily enjoined Google from creating and publicly displaying thumbnail versions of Perfect 10's images, *Perfect 10 v. Google, Inc.*, 416 F. Supp. 2d 828 (C.D.Cal.2006), but did not enjoin Google from linking to third-party websites that display infringing full-size versions of Perfect 10's images. ... Perfect 10 and Google both appeal the district court's order.

I

Background

...

Google operates a search engine, a software program that automatically accesses thousands of websites (collections of webpages) and indexes them within a database stored on Google's computers. When a Google user accesses the Google website and types in a search query, Google's software searches its database for websites responsive to that search query. Google then sends relevant information from its index of websites to the user's computer. Google's search engines can provide results in the form of text, images, or videos.

The Google search engine that provides responses in the form of images is called "Google Image Search." In response to a search query, Google Image Search identifies text in its database responsive to the query and then communicates to users the images associated with the relevant text. Google's software cannot recognize and index the images themselves. Google Image Search provides search results as a webpage of small images called "thumbnails," which are stored in Google's servers. The thumbnail images are reduced, lower-resolution versions of full-sized images stored on third-party computers.

When a user clicks on a thumbnail image, the user's browser program interprets HTML instructions on Google's webpage. These HTML instructions direct the user's browser to cause a rectangular area (a "window") to appear on the user's computer screen. The window has two separate areas of information. The browser fills the top section of the screen with information from the Google webpage, including the thumbnail image and text. The HTML instructions also give the user's browser the address of the website publisher's computer that stores the full-size version of the thumbnail. By following the HTML instructions to access the third-party webpage, the user's browser connects to the website publisher's computer, downloads the full-size image, and makes the image appear at the bottom of the window on the user's screen. Google does not store the images that fill this lower part of the window and does not communicate the images to the user; Google simply provides HTML instructions directing a user's browser to access a third-party website. However, the top part of the window (containing the information from the Google webpage) appears to frame and comment on the bottom part of the window. Thus, the user's window appears to be filled with a single integrated presentation of the full-size image, but it is actually an image from a third-party website framed by information from Google's website. The process by which the webpage directs a user's browser to incorporate content from different computers into a single window is referred to as "in-line linking." The term "framing" refers to the process by which information from one computer appears to frame and annotate the in-line linked content from another computer. ...

Perfect 10 markets and sells copyrighted images of nude models. Among other enterprises, it operates a subscription website on the Internet. Subscribers pay a monthly fee to view Perfect10 images in a "members' area" of the site. Subscribers must use a password to log into the members' area. Google does not include these password-protected images from the members' area in Google's index or database. Perfect 10 has also licensed Fonestarz Media Limited to sell and distribute Perfect 10's reduced-size copyrighted images for download and use on cell phones.

Some website publishers republish Perfect 10's images on the Internet without authorization. Once this occurs, Google's search engine may automatically index the webpages containing these images and provide thumbnail versions of images in response to user inquiries. When a user clicks on the thumbnail image returned by Google's search engine, the user's browser accesses the third-party webpage and in-line links to the full-sized infringing image stored on the website publisher's computer. This image appears, in its original context, on the lower portion of the window on the user's computer screen framed by information from Google's webpage. ...

III

Direct Infringement

Perfect 10 claims that Google's search engine program directly infringes two exclusive rights granted to copyright holders: its display rights and its distribution rights. Plaintiffs must satisfy two requirements to present a prima facie case of direct infringement: (1) they must show ownership of the allegedly infringed material and (2) they must demonstrate that the alleged infringers violate at least one exclusive right granted to copyright holders under 17 U.S.C. § 106. Even if a plaintiff satisfies these two requirements and makes a prima facie case of direct infringement, the defendant may avoid liability if it can establish that its use of the images is a "fair use" as set forth in 17 U.S.C. § 107.

Perfect 10's ownership of at least some of the images at issue is not disputed.

The district court held that Perfect 10 was likely to prevail in its claim that Google violated Perfect 10's display right with respect to the infringing thumbnails. However, the district court concluded that Perfect 10 was not likely to prevail on its claim that Google violated either Perfect 10's display or distribution right with respect to its full-size infringing images. We review these rulings for an abuse of discretion.

A. Display Right

...

We have not previously addressed the question when a computer displays a copyrighted work for purposes of section 106(5). Section 106(5) states that a copyright owner has the exclusive right "to display the copyrighted work publicly." The Copyright Act explains that "display" means "to show a copy of it, either directly or by means of a film, slide, television image, or any other device or process. . . ." 17 U.S.C. § 101. Section 101 defines "copies" as "material objects, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." *Id.* Finally, the Copyright Act provides that "[a] work is 'fixed' in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." *Id.*

We must now apply these definitions to the facts of this case. A photographic image is a work that is "'fixed' in a tangible medium of expression," for purposes of the Copyright Act, when embodied (i.e., stored) in a computer's server (or hard disk, or other storage device). The image stored in the computer is the "copy" of the work for purposes of copyright law. *See MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 517-18 (9th Cir.1993). The computer owner shows a copy "by means of a . . . device or process" when the owner uses the computer to fill the computer screen with the photographic image stored on that computer, or by communicating the stored image electronically to another person's computer. 17 U.S.C. § 101. In sum, based on the plain language of the statute, a person displays a photographic image by using a computer to fill a computer screen with a copy of the photographic image fixed in the computer's memory. There is no dispute that Google's computers store thumbnail versions of Perfect 10's copyrighted images and communicate copies of those thumbnails to Google's users. Therefore, Perfect10 has made a prima facie case that Google's communication of its stored thumbnail images directly infringes Perfect 10's display right.

Google does not, however, display a copy of full-size infringing photographic images for purposes of the Copyright Act when Google frames in-line linked images that appear on a user's computer screen. Because Google's computers do not store the photographic images, Google does not have a copy of the images for purposes of the Copyright Act. In other words, Google does not have any "material objects . . . in which a work is fixed . . . and from which the work can be perceived, reproduced, or otherwise communicated" and thus cannot communicate a copy. 17 U.S.C. § 101.

Instead of communicating a copy of the image, Google provides HTML instructions that direct a user's browser to a website publisher's computer that stores the full-size photographic

image. Providing these HTML instructions is not equivalent to showing a copy. First, the HTML instructions are lines of text, not a photographic image. Second, HTML instructions do not themselves cause infringing images to appear on the user's computer screen. The HTML merely gives the address of the image to the user's browser. The browser then interacts with the computer that stores the infringing image. It is this interaction that causes an infringing image to appear on the user's computer screen. Google may facilitate the user's access to infringing images. However, such assistance raises only contributory liability issues and does not constitute direct infringement of the copyright owner's display rights.

Perfect 10 argues that Google displays a copy of the full-size images by framing the full-size images, which gives the impression that Google is showing the image within a single Google webpage. While in-line linking and framing may cause some computer users to believe they are viewing a single Google webpage, the Copyright Act, unlike the Trademark Act, does not protect a copyright holder against acts that cause consumer confusion. ...

B. Distribution Right

The district court also concluded that Perfect 10 would not likely prevail on its claim that Google directly infringed Perfect 10's right to distribute its full-size images. The district court reasoned that distribution requires an "actual dissemination" of a copy. Because Google did not communicate the full-size images to the user's computer, Google did not distribute these images.

Again, the district court's conclusion on this point is consistent with the language of the Copyright Act. Section 106(3) provides that the copyright owner has the exclusive right "to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending." 17 U.S.C. § 106(3). As noted, "copies" means "material objects . . . in which a work is fixed." 17 U.S.C. § 101. The Supreme Court has indicated that in the electronic context, copies may be distributed electronically. Google's search engine communicates HTML instructions that tell a user's browser where to find full-size images on a website publisher's computer, but Google does not itself distribute copies of the infringing photographs. It is the website publisher's computer that distributes copies of the images by transmitting the photographic image electronically to the user's computer. ...

Accordingly, the district court correctly concluded that Perfect 10 does not have a likelihood of success in proving that Google violates Perfect 10's distribution rights with respect to full-size images.

C. Fair Use Defense

Although Perfect 10 has succeeded in showing it would prevail in its prima facie case that Google's thumbnail images infringe Perfect 10's display rights, Perfect 10 must still show a likelihood that it will prevail against Google's affirmative defense. Google contends that its use of thumbnails is a fair use of the images and therefore does not constitute an infringement of Perfect 10's copyright. *See* 17 U.S.C. § 107.

The fair use defense permits the use of copyrighted works without the copyright owner's consent under certain situations. The defense encourages and allows the development of new ideas that build on earlier ones, thus providing a necessary counterbalance to the copyright law's goal of protecting creators' work product. "From the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's

very purpose. . . ." *Campbell*, 510 U.S. at 575, 114 S.Ct. 1164. "The fair use doctrine thus 'permits [and requires] courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster.'" *Id.* at 577, 114 S.Ct. 1164 (*quoting Stewart v. Abend*, 495 U.S. 207, 236, 110 S.Ct. 1750, 109 L.Ed.2d 184 (1990)) (alteration in original). ...

In applying the fair use analysis in this case, we are guided by *Kelly v. Arriba Soft Corp.*,which considered substantially the same use of copyrighted photographic images as is at issue here. In *Kelly*, a photographer brought a direct infringement claim against Arriba, the operator of an Internet search engine. The search engine provided thumbnail versions of the photographer's images in response to search queries. We held that Arriba's use of thumbnail images was a fair use primarily based on the transformative nature of a search engine and its benefit to the public. We also concluded that Arriba's use of the thumbnail images did not harm the photographer's market for his image.

In this case, the district court determined that Google's use of thumbnails was not a fair use and distinguished Kelly. We consider these distinctions in the context of the four-factor fair use analysis, remaining mindful that Perfect 10 has the burden of proving that it will successfully challenge any evidence Google presents to support its affirmative defense.

Purpose and character of the use. The first factor, 17 U.S.C. § 107(1), requires a court to consider "the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes." The central purpose of this inquiry is to determine whether and to what extent the new work is "transformative." *Campbell*, 510 U.S. at 579. A work is "transformative" when the new work does not merely supersede the objects of the original creation but rather adds something new, with a further purpose or different character, altering the first with new expression, meaning, or message. Conversely, if the new work supersedes the use of the original, the use is likely not a fair use.

As noted in *Campbell*, a "transformative work" is one that alters the original work "with new expression, meaning, or message." A use is considered transformative only where a defendant changes a plaintiff's copyrighted work or uses the plaintiff's copyrighted work in a different context such that the plaintiff's work is transformed into a new creation.

Google's use of thumbnails is highly transformative. In *Kelly*, we concluded that Arriba's use of thumbnails was transformative because "Arriba's use of the images serve[d] a different function than Kelly's use—improving access to information on the [I]nternet versus artistic expression." *Kelly*, 336 F.3d at 819. Although an image may have been created originally to serve an entertainment, aesthetic, or informative function, a search engine transforms the image into a pointer directing a user to a source of information. Just as a "parody has an obvious claim to transformative value" because "it can provide social benefit, by shedding light on an earlier work, and, in the process, creating a new one," *Campbell*, 510 U.S. at 579, 114 S.Ct. 1164, a search engine provides social benefit by incorporating an original work into a new work, namely, an electronic reference tool. Indeed, a search engine may be more transformative than a parody because a search engine provides an entirely new use for the original work, while a parody typically has the same entertainment purpose as the original work. In other words, a search engine puts images "in a different context" so that they are "transformed into a new creation." *Wall Data*, 447 F.3d at 778.

The fact that Google incorporates the entire Perfect 10 image into the search engine results does not diminish the transformative nature of Google's use. As the district court correctly noted, we determined in *Kelly* that even making an exact copy of a work may be transformative so long as the copy serves a different function than the original work. ...

We conclude that the significantly transformative nature of Google's search engine, particularly in light of its public benefit, outweighs Google's superseding and commercial uses of the thumbnails in this case. ...

The nature of the copyrighted work. With respect to the second factor, "the nature of the copyrighted work," 17 U.S.C. § 107(2), our decision in *Kelly* is directly on point. There we held that the photographer's images were "creative in nature" and thus "closer to the core of intended copyright protection than are more fact-based works." *Kelly*, 336 F.3d at 820 (internal quotation omitted). However, because the photos appeared on the Internet before Arriba used thumbnail versions in its search engine results, this factor weighed only slightly in favor of the photographer.

Here, the district court found that Perfect 10's images were creative but also previously published. ... Once Perfect 10 has exploited this commercially valuable right of first publication by putting its images on the Internet for paid subscribers, Perfect 10 is no longer entitled to the enhanced protection available for an unpublished work. Accordingly the district court did not err in holding that this factor weighed only slightly in favor of Perfect 10.

The amount and substantiality of the portion used. "The third factor asks whether the amount and substantiality of the portion used in relation to the copyrighted work as a whole . . . are reasonable in relation to the purpose of the copying." *Campbell*, 510 U.S. at 586, 114 S.Ct. 1164 (internal quotation omitted); *see also* 17 U.S.C. § 107(3). In *Kelly*, we held Arriba's use of the entire photographic image was reasonable in light of the purpose of a search engine. Specifically, we noted, "[i]t was necessary for Arriba to copy the entire image to allow users to recognize the image and decide whether to pursue more information about the image or the originating [website]. If Arriba only copied part of the image, it would be more difficult to identify it, thereby reducing the usefulness of the visual search engine." *Id.* Accordingly, we concluded that this factor did not weigh in favor of either party. Because the same analysis applies to Google's use of Perfect 10's image, the district court did not err in finding that this factor favored neither party.

Effect of use on the market. The fourth factor is "the effect of the use upon the potential market for or value of the copyrighted work." 17 U.S.C. § 107(4). In Kelly, we concluded that Arriba's use of the thumbnail images did not harm the market for the photographer's full-size images. *See Kelly*, 336 F.3d at 821-22. We reasoned that because thumbnails were not a substitute for the full-sized images, they did not harm the photographer's ability to sell or license his full-sized images. *Id.* The district court here followed Kelly's reasoning, holding that Google's use of thumbnails did not hurt Perfect 10's market for full-size images. *See Perfect10*, 416 F. Supp. 2d at 850-51.

Perfect 10 argues that the district court erred because the likelihood of market harm may be presumed if the intended use of an image is for commercial gain. However, this presumption does not arise when a work is transformative because "market substitution is at least less certain, and market harm may not be so readily inferred." ...

Perfect 10 also has a market for reduced-size images, an issue not considered in Kelly. The district court held that "Google's use of thumbnails likely does harm the potential market for the

downloading of [Perfect 10's] reduced-size images onto cell phones." *Perfect 10*, 416 F. Supp. 2d at 851 (emphasis omitted). The district court reasoned that persons who can obtain Perfect 10 images free of charge from Google are less likely to pay for a download, and the availability of Google's thumbnail images would harm Perfect 10's market for cell phone downloads. As we discussed above, the district court did not make a finding that Google users have downloaded thumbnail images for cell phone use. This potential harm to Perfect10's market remains hypothetical. We conclude that this factor favors neither party.

Having undertaken a case-specific analysis of all four factors, we now weigh these factors together "in light of the purposes of copyright." *Campbell*, 510 U.S. at 578, 114 S.Ct. 1164; *see also Kelly*, 336 F.3d at 818 ("We must balance [the section 107] factors in light of the objectives of copyright law, rather than view them as definitive or determinative tests."). We note that Perfect 10 has the burden of proving that it would defeat Google's affirmative fair use defense, *see supra* Section II. In this case, Google has put Perfect 10's thumbnail images (along with millions of other thumbnail images) to a use fundamentally different than the use intended by Perfect 10. In doing so, Google has provided a significant benefit to the public. Weighing this significant transformative use against the unproven use of Google's thumbnails for cell phone downloads, and considering the other fair use factors, all in light of the purpose of copyright, we conclude that Google's use of Perfect 10's thumbnails is a fair use. ...

A & M Records, Inc. v. Napster, Inc.
239 F. 3d 1004 (9th Cir. 2001)

... In 1987, the Moving Picture Experts Group set a standard file format for the storage of audio recordings in a digital format called MPEG-3, abbreviated as "MP3." Digital MP3 files are created through a process colloquially called "ripping." Ripping software allows a computer owner to copy an audio compact disk ("audio CD") directly onto a computer's hard drive by compressing the audio information on the CD into the MP3 format. The MP3's compressed format allows for rapid transmission of digital audio files from one computer ...

Napster facilitates the transmission of MP3 files between and among its users. Through a process commonly called "peer-to-peer" file sharing, Napster allows its users to: (1) make MP3 music files stored on individual computer hard drives available for copying by other Napster users; (2) search for MP3 music files stored on other users' computers; and (3) transfer exact copies of the contents of other users' MP3 files from one computer to another via the Internet. These functions are made possible by Napster's MusicShare software, available free of charge from Napster's Internet site, and Napster's network servers and server-side software. ...

A. Accessing the System

In order to copy MP3 files through the Napster system, a user must first access Napster's Internet site and download the MusicShare software to his individual computer. Once the software is installed, the user can access the Napster system. A first-time user is required to register with the Napster system by creating a "user name" and password.

B. Listing Available Files

If a registered user wants to list available files stored in his computer's hard drive on Napster for others to access, he must first create a "user library" directory on his computer's hard drive.

The user then saves his MP3 files in the library directory, using self-designated file names. He next must log into the Napster system using his user name and password. His MusicShare software then searches his user library and verifies that the available files are properly formatted. If in the correct MP3 format, the names of the MP3 files will be uploaded from the user's computer to the Napster servers. The content of the MP3 files remains stored in the user's computer.

Once uploaded to the Napster servers, the user's MP3 file names are stored in a server-side "library" under the user's name and become part of a "collective directory" of files available for transfer during the time the user is logged onto the Napster system. The collective directory is fluid; it tracks users who are connected in real time, displaying only file names that are immediately accessible.

C. Searching For Available Files

Napster allows a user to locate other users' MP3 files in two ways: through Napster's search function and through its "hotlist" function.

Software located on the Napster servers maintains a "search index" of Napster's collective directory. To search the files available from Napster users currently connected to the network servers, the individual user accesses a form in the MusicShare software stored in his computer and enters either the name of a song or an artist as the object of the search. The form is then transmitted to a Napster server and automatically compared to the MP3 file names listed in the server's search index. Napster's server compiles a list of all MP3 file names pulled from the search index which include the same search terms entered on the search form and transmits the list to the searching user. The Napster server does not search the contents of any MP3 file; rather, the search is limited to "a text search of the file names indexed in a particular cluster. Those file names may contain typographical errors or otherwise inaccurate descriptions of the content of the files since they are designated by other users." *Napster*, 114 F. Supp. 2d at 906.

To use the "hotlist" function, the Napster user creates a list of other users' names from whom he has obtained MP3 files in the past. When logged onto Napster's servers, the system alerts the user if any user on his list (a "hotlisted user") is also logged onto the system. If so, the user can access an index of all MP3 file names in a particular hotlisted user's library and request a file in the library by selecting the file name. The contents of the hotlisted user's MP3 file are not stored on the Napster system.

D. Transferring Copies of an MP3 file

To transfer a copy of the contents of a requested MP3 file, the Napster server software obtains the Internet address of the requesting user and the Internet address of the "host user" (the user with the available files). The Napster servers then communicate the host user's Internet address to the requesting user. The requesting user's computer uses this information to establish a connection with the host user and downloads a copy of the contents of the MP3 file from one computer to the other over the Internet, "peer-to-peer." A downloaded MP3 file can be played directly from the user's hard drive using Napster's MusicShare program or other software. The file may also be transferred back onto an audio CD if the user has access to equipment designed for that purpose. In both cases, the quality of the original sound recording is slightly diminished by transfer to the MP3 format.

...

Napster contends that its users do not directly infringe plaintiffs' copyrights because the users are engaged in fair use of the material. *See* 17 U.S.C. § 107 ("[T]he fair use of a copyrighted work . . . is not an infringement of copyright."). Napster identifies three specific alleged fair uses: sampling, where users make temporary copies of a work before purchasing; space-shifting, where users access a sound recording through the Napster system that they already own in audio CD format; and permissive distribution of recordings by both new and established artists.

The district court considered factors listed in 17 U.S.C. § 107, which guide a court's fair use determination. These factors are: (1) the purpose and character of the use; (2) the nature of the copyrighted work; (3) the "amount and substantiality of the portion used" in relation to the work as a whole; and (4) the effect of the use upon the potential market for the work or the value of the work. *See* 17 U.S.C. § 107. The district court first conducted a general analysis of Napster system uses under § 107, and then applied its reasoning to the alleged fair uses identified by Napster. The district court concluded that Napster users are not fair users.

We agree. We first address the court's overall fair use analysis.

1. Purpose and Character of the Use

This factor focuses on whether the new work merely replaces the object of the original creation or instead adds a further purpose or different character. In other words, this factor asks "whether and to what extent the new work is 'transformative.'" *See Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 579 (1994).

... Courts have been reluctant to find fair use when an original work is merely retransmitted in a different medium. *See*, *e.g.*, *Infinity Broadcast Corp. v. Kirkwood*, 150 F.3d 104, 108 (2d Cir.1998) (concluding that retransmission of radio broadcast over telephone lines is not transformative); *UMG Recordings, Inc. v. MP3.com, Inc.*, 92 F. Supp. 2d 349, 351 (S.D.N.Y.) (finding that reproduction of audio CD into MP3 format does not "transform" the work), *certification denied*, 2000 WL 710056 (S.D.N.Y. June 1, 2000) ("Defendant's copyright infringement was clear, and the mere fact that it was clothed in the exotic webbing of the Internet does not disguise its illegality.").

This "purpose and character" element also requires the district court to determine whether the allegedly infringing use is commercial or noncommercial. *See Campbell*, 510 U.S. at 584-85. A commercial use weighs against a finding of fair use but is not conclusive on the issue. *Id.* The district court determined that Napster users engage in commercial use of the copyrighted materials largely because (1) "a host user sending a file cannot be said to engage in a personal use when distributing that file to an anonymous requester" and (2) "Napster users get for free something they would ordinarily have to buy." *Napster*, 114 F. Supp. 2d at 912. The district court's findings are not clearly erroneous. ...

2. The Nature of the Use

Works that are creative in nature are closer to the core of intended copyright protection"than are more fact-based works. The district court determined that plaintiffs' "copyrighted musical compositions and sound recordings are creative in nature . . . which cuts against a finding of fair use under the second factor." Napster, 114 F. Supp. 2d at 913. We find no error in the district court's conclusion.

3. The Portion Used

While wholesale copying does not preclude fair use *per se*, copying an entire work militates against a finding of fair use. The district court determined that Napster users engage in "wholesale copying" of copyrighted work because file transfer necessarily "involves copying the entirety of the copyrighted work." *Napster*, 114 F. Supp. 2d at 913. We agree. ...

4. Effect of Use on Market

Fair use, when properly applied, is limited to copying by others which does not materially impair the marketability of the work which is copied. The importance of this [fourth] factor will vary, not only with the amount of harm, but also with the relative strength of the showing on the other factors. ...

Addressing this factor, the district court concluded that Napster harms the market in "at least" two ways: it reduces audio CD sales among college students and it "raises barriers to plaintiffs' entry into the market for the digital downloading of music." *Napster*, 114 F. Supp. 2d at 913. ...

5. Identified Uses

Napster maintains that its identified uses of sampling and space-shifting were wrongly excluded as fair uses by the district court.

a. Sampling

Napster contends that its users download MP3 files to "sample" the music in order to decide whether to purchase the recording. ...

Plaintiffs have established that they are likely to succeed in proving that even authorized temporary downloading of individual songs for sampling purposes is commercial in nature. ... The record supports a finding that free promotional downloads are highly regulated by the record company plaintiffs and that the companies collect royalties for song samples available on retail Internet sites. Evidence relied on by the district court demonstrates that the free downloads provided by the record companies consist of thirty-to-sixty second samples or are full songs programmed to "time out," that is, exist only for a short time on the downloader's computer. In comparison, Napster users download a full, free and permanent copy of the recording. ...

[O]verall, Napster has an adverse impact on the audio CD and digital download markets. Contrary to Napster's assertion that the district court failed to specifically address the market impact of sampling, the district court determined that "[e]ven if the type of sampling supposedly done on Napster were a non-commercial use, plaintiffs have demonstrated a substantial likelihood that it would adversely affect the potential market for their copyrighted works if it became widespread." The record supports the district court's preliminary determinations that: (1) the more music that sampling users download, the less likely they are to eventually purchase the recordings on audio CD; and (2) even if the audio CD market is not harmed, Napster has adverse effects on the developing digital download market.

Napster further argues that the district court erred in rejecting its evidence that the users' downloading of "samples" increases or tends to increase audio CD sales. The district court, however, correctly noted that "any potential enhancement of plaintiffs' sales . . . would not tip the fair use analysis conclusively in favor of defendant." *Id.* at 914. We agree that increased sales of copyrighted material attributable to unauthorized use should not deprive the copyright holder of the right to license the material. Nor does positive impact in one market, here the audio CD

market, deprive the copyright holder of the right to develop identified alternative markets, here the digital download market.

We find no error in the district court's factual findings or abuse of discretion in the court's conclusion that plaintiffs will likely prevail in establishing that sampling does not constitute a fair use.

b. Space-Shifting

Napster also maintains that space-shifting is a fair use. Space-shifting occurs when a Napster user downloads MP3 music files in order to listen to music he already owns on audio CD. Napster asserts that we have already held that space-shifting of musical compositions and sound recordings is a fair use. *See Recording Indus. Ass'n of Am. v. Diamond Multimedia Sys., Inc.*, 180 F.3d 1072, 1079 (9th Cir.1999) ("Rio [a portable MP3 player] merely makes copies in order to render portable, or 'space-shift,' those files that already reside on a user's hard drive. . . . Such copying is a paradigmatic noncommercial personal use."). *See also generally Sony*, 464 U.S. at 423, 104 S.Ct. 774 (holding that "time-shifting," where a video tape recorder owner records a television show for later viewing, is a fair use).

Both *Diamond* and *Sony* are inapposite because the methods of shifting in these cases did not also simultaneously involve distribution of the copyrighted material to the general public; the time or space-shifting of copyrighted material exposed the material only to the original user. In *Diamond*, for example, the copyrighted music was transferred from the user's computer hard drive to the user's portable MP3 player. So too *Sony*, where "the majority of VCR purchasers . . . did not distribute taped television broadcasts, but merely enjoyed them at home." *Napster*, 114 F. Supp. 2d at 913. Conversely, it is obvious that once a user lists a copy of music he already owns on the Napster system in order to access the music from another location, the song becomes "available to millions of other individuals," not just the original CD owner. ...

... We find no error in the district court's determination that plaintiffs will likely succeed in establishing that Napster users do not have a fair use defense.

CLASS 24: SECONDARY LIABILITY

Now for the dense stuff. Once you've figured out who's a direct infringer, it's time to decide whether anyone else should also be held secondarily liable for the infringements. You need to master four doctrines here: vicarious infringement, contributory infringement, the *Sony* defense to contributory infringement, and inducement infringement.

Preparation questions

(1) Napster (a continuation of the same case you read for last time) provides an introduction to contributory and vicarious infringement. I'd actually like to start with a question not fully considered last time: why isn't Napster *directly* liable for copyright infringement? Until you can answer this question, you haven't fully grasped Napster's architecture. Go back and read the facts from last time's portion of the case. Pin down how Napster's design meant that it couldn't be directly liable—but left it open to suit for the infringements of its users.

(2) Now, let's take up the vicarious infringement liability, analysis in Part V of the court's opinion. How is it that a company with no revenue to speak of could have a "direct financial interest" in anything? Similarly, walk through the court's reasoning on the "right and ability to control." Note that Napster users aren't employees. How is it that Napster could still have the "right and ability" to control what they do? Would Sony, back in the 1980s, have had the "right and ability" to control VCR users? What accounts for the difference?

(3) The interesting (and tricky) part of the contributory infringement analysis in Part IV centers on the relationship of knowledge to the *Sony* defense. (I think material contribution is easy; why?) You may find it helpful to go back to the *eBay* case from trademark, and distinguish specific (or "actual") knowledge from general (or "constructive") knowledge of infringement. Which of these does Napster have? Why? Do you think that Napster was capable of substantial noninfringing uses? If so, why doesn't *Sony* shield it from liability?

(4) Grokster was the next step in the copyright wars after the Napster litigation saga. Read the Supreme Court's description of how the Gnutella network (which is fairly typical of these second-generation peer-to-peer services) works. The Supreme Court doesn't discuss it, but could Morpheus and StreamCast have been held liable on a vicarious liability theory? If you understand why the answer is probably "no," then you understand the important technical point. Reread the facts of how Gnutella and Napster operate until you see the difference. Diagrams may be helpful.

(5) Given the unavailability of a vicarious infringement theory, the copyright-owner plaintiffs pushed hard on the contributory infringement theory. In light of the key architectural difference between Napster and these second-generation networks (no central directory), revisit the *Napster* analysis. Does StreamCast have the right kind of knowledge of infringement to be held liable? Can it raise a *Sony* defense?

(6) In the face of the Ninth Circuit's conclusion that *Sony* applied, the copyright owners shifted their focus to the question of what counts as a a "significant" noninfringing use. They argued that the peer-to-peer networks were so overwhelmingly used for infringement that the noninfinging uses were insignificant in comparison. The defendants, along with numerous academic and activist amici, argued instead that these uses were indeed significant and becoming more so. (What kinds of legitimate uses might peer-to-peer technology have?)

Or, interpreted differently, they were disputing what the legal threshold ought to be. Do you see why this could be regarded either as a factual or as a legal issue? Each side convinced three Supreme Court justices of its position (in separate concurrences not reproduced here). The Court as a whole, however, sidestepped the issue. How is the "inducement" standard something of a cop-out?

(7) The inducement standard itself seems simple enough. What did Morpheus and StreamCast do wrong? Do you agree that it was wrong? How reliable a test does it provide to distinguish good actors from bad?

A & M Records, Inc. v. Napster, Inc.
239 F. 3d 1004 (9th Cir. 2001)

[See the previous class for the facts of this case. Having held that Napster's users are direct infringers and do not have a fair use defense, the court now considers whether Napster can be held secondarily liable for their infringements.]

IV.

We first address plaintiffs' claim that Napster is liable for contributory copyright infringement. Traditionally, "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a `contributory' infringer." *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162 (2d Cir.1971); see also *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 264 (9th Cir.1996). Put differently, liability exists if the defendant engages in "personal conduct that encourages or assists the infringement." *Matthew Bender & Co. v. West Publ'g Co.*, 158 F.3d 693, 706 (2d Cir.1998).

The district court determined that plaintiffs in all likelihood would establish Napster's liability as a contributory infringer. The district court did not err; Napster, by its conduct, knowingly encourages and assists the infringement of plaintiffs' copyrights.

A. Knowledge

Contributory liability requires that the secondary infringer know or have reason to know of direct infringement. The district court found that Napster had both actual and constructive knowledge that its users exchanged copyrighted music. The district court also concluded that the law does not require knowledge of "specific acts of infringement" and rejected Napster's contention that because the company cannot distinguish infringing from noninfringing files, it does not "know" of the direct infringement.

It is apparent from the record that Napster has knowledge, both actual and constructive,of direct infringement. Napster claims that it is nevertheless protected from contributory liability by the teaching of *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984). We disagree. We observe that Napster's actual, specific knowledge of direct infringement renders Sony's holding of limited assistance to Napster. We are compelled to make a clear distinction between the architecture of the Napster system and Napster's conduct in relation to the operational capacity of the system.

The *Sony* Court refused to hold the manufacturer and retailers of video tape recorders liable for contributory infringement despite evidence that such machines could be and were used to

infringe plaintiffs' copyrighted television shows. Sony stated that if liability "is to be imposed on petitioners in this case, it must rest on the fact that they have sold equipment with constructive knowledge of the fact that their customers may use that equipment to make unauthorized copies of copyrighted material." *Id.* at 439, 104 S.Ct. 774 (emphasis added). The Sony Court declined to impute the requisite level of knowledge where the defendants made and sold equipment capable of both infringing and "substantial noninfringing uses." *Id.* at 442 (adopting a modified "staple article of commerce" doctrine from patent law).

We are bound to follow *Sony*, and will not impute the requisite level of knowledge to Napster merely because peer-to-peer file sharing technology may be used to infringe plaintiffs' copyrights. ... Regardless of the number of Napster's infringing versus noninfringing uses, the evidentiary record here supported the district court's finding that plaintiffs would likely prevail in establishing that Napster knew or had reason to know of its users' infringement of plaintiffs' copyrights.

This analysis is similar to that of *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*, which suggests that in an online context, evidence of actual knowledge of specific acts of infringement is required to hold a computer system operator liable for contributory copyright infringement. 907 F.Supp. at 1371. Netcom considered the potential contributory copyright liability of a computer bulletin board operator whose system supported the posting of infringing material. Id. at 1374. The court, in denying Netcom's motion for summary judgment of noninfringement and plaintiff's motion for judgment on the pleadings, found that a disputed issue of fact existed as to whether the operator had sufficient knowledge of infringing activity. Id. at 1374-75.

The court determined that for the operator to have sufficient knowledge, the copyright holder must "provide the necessary documentation to show there is likely infringement." 907 F. Supp. at 1374. If such documentation was provided, the court reasoned that Netcom would be liable for contributory infringement because its failure to remove the material "and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation" in distribution of copyrighted material. *Id.*

We agree that if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement. See *Netcom*, 907 F.Supp. at 1374. Conversely, absent any specific information which identifies infringing activity, a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material. See *Sony*, 464 U.S. at 436, 442-43, 104 S.Ct. 774. To enjoin simply because a computer network allows for infringing use would, in our opinion, violate Sony and potentially restrict activity unrelated to infringing use.

We nevertheless conclude that sufficient knowledge exists to impose contributory liability when linked to demonstrated infringing use of the Napster system. The record supports the district court's finding that Napster has actual knowledge that specific infringing material is available using its system, that it could block access to the system by suppliers of the infringing material, and that it failed to remove the material.

B. Material Contribution

Under the facts as found by the district court, Napster materially contributes to the infringing activity. Relying on *Fonovisa*, the district court concluded that "[w]ithout the support services defendant provides, Napster users could not find and download the music they want with the ease of which defendant boasts." *Napster*, 114 F.Supp.2d at 919-20. We agree that Napster provides "the site and facilities" for direct infringement. See *Fonovisa*, 76 F.3d at 264; cf. *Netcom*, 907 F.Supp. at 1372 ("Netcom will be liable for contributory infringement since its failure to cancel [a user's] infringing message and thereby stop an infringing copy from being distributed worldwide constitutes substantial participation."). The district court correctly applied the reasoning in *Fonovisa*, and properly found that Napster materially contributes to direct infringement. ...

V.

We turn to the question whether Napster engages in vicarious copyright infringement. Vicarious copyright liability is an "outgrowth" of respondeat superior. *Fonovisa*, 76 F.3d at 262. In the context of copyright law, vicarious liability extends beyond an employer/employee relationship to cases in which a defendant "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities." Id. (quoting *Gershwin*, 443 F.2d at 1162.

Before moving into this discussion, we note that *Sony*'s "staple article of commerce" analysis has no application to Napster's potential liability for vicarious copyright infringement. ....

A. Financial Benefit

The district court determined that plaintiffs had demonstrated they would likely succeed in establishing that Napster has a direct financial interest in the infringing activity. *Napster*, 114 F. Supp.2d at 921-22. We agree. Financial benefit exists where the availability of infringing material "acts as a `draw' for customers." *Fonovisa*, 76 F.3d at 263-64 (stating that financial benefit may be shown "where infringing performances enhance the attractiveness of a venue"). Ample evidence supports the district court's finding that Napster's future revenue is directly dependent upon "increases in userbase." More users register with the Napster system as the "quality and quantity of available music increases." 114 F.Supp.2d at 902. We conclude that the district court did not err in determining that Napster financially benefits from the availability of protected works on its system.

B. Supervision

The district court determined that Napster has the right and ability to supervise its users' conduct. *Napster*, 114 F.Supp.2d at 920-21 (finding that Napster's representations to the court regarding "its improved methods of blocking users about whom rights holders complain . . . is tantamount to an admission that defendant can, and sometimes does, police its service"). We agree in part.

The ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise. See *Fonovisa*, 76 F.3d at 262 ("Cherry Auction had the right to terminate vendors for any reason whatsoever and through that right had the ability to control the activities of vendors on the premises."); cf. *Netcom*, 907 F.Supp. at 1375-76 (indicating that plaintiff raised a genuine issue of fact regarding ability to supervise by presenting evidence that an electronic bulletin board service can suspend subscriber's accounts). Here, plaintiffs have

demonstrated that Napster retains the right to control access to its system. Napster has an express reservation of rights policy, stating on its website that it expressly reserves the "right to refuse service and terminate accounts in [its] discretion, including, but not limited to, if Napster believes that user conduct violates applicable law . . . or for any reason in Napster's sole discretion, with or without cause."

To escape imposition of vicarious liability, the reserved right to police must be exercised to its fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability. See, e.g., *Fonovisa*, 76 F.3d at 261 ("There is no dispute for the purposes of this appeal that Cherry Auction and its operators were aware that vendors in their swap meets were selling counterfeit recordings."); see also *Gershwin*, 443 F.2d at 1161-62 (citing Shapiro, Bernstein & Co. v. H.L. Green Co., 316 F.2d 304 (2d Cir.1963), for the proposition that "failure to police the conduct of the primary infringer" leads to imposition of vicarious liability for copyright infringement).

The district court correctly determined that Napster had the right and ability to police its system and failed to exercise that right to prevent the exchange of copyrighted material. The district court, however, failed to recognize that the boundaries of the premises that Napster "controls and patrols" are limited. See, e.g., *Fonovisa*, 76 F.3d at 262-63 (in addition to having the right to exclude vendors, defendant "controlled and patrolled" the premises); see also *Polygram*, 855 F.Supp. at 1328-29 (in addition to having the contractual right to remove exhibitors, trade show operator reserved the right to police during the show and had its "employees walk the aisles to ensure `rules compliance'"). Put differently, Napster's reserved "right and ability" to police is cabined by the system's current architecture. As shown by the record, the Napster system does not "read" the content of indexed files, other than to check that they are in the proper MP3 format.

Napster, however, has the ability to locate infringing material listed on its search indices, and the right to terminate users' access to the system. The file name indices, therefore, are within the "premises" that Napster has the ability to police. We recognize that the files are user-named and may not match copyrighted material exactly (for example, the artist or song could be spelled wrong). For Napster to function effectively, however, file names must reasonably or roughly correspond to the material contained in the files, otherwise no user could ever locate any desired music. As a practical matter, Napster, its users and the record company plaintiffs have equal access to infringing material by employing Napster's "search function."

Our review of the record requires us to accept the district court's conclusion that plaintiffs have demonstrated a likelihood of success on the merits of the vicarious copyright infringement claim. Napster's failure to police the system's "premises," combined with a showing that Napster financially benefits from the continuing availability of infringing files on its system, leads to the imposition of vicarious liability. ...

Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.

545 U.S. 913 (2005)

JUSTICE SOUTER delivered the opinion of the Court.

The question is under what circumstances the distributor of a product capable of both lawful and unlawful use is liable for acts of copyright infringement by third parties using the product. We hold that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement.

I.

A.

Respondents, Grokster, Ltd., and StreamCast Networks, Inc., defendants in the trial court, distribute free software products that allow computer users to share electronic files through peer-to-peer networks, so called because users' computers communicate directly with each other, not through central servers. The advantage of peer-to-peer networks over information networks of other types shows up in their substantial and growing popularity. Because they need no central computer server to mediate the exchange of information or files among users, the high-bandwidth communications capacity for a server may be dispensed with, and the need for costly server storage space is eliminated. Since copies of a file (particularly a popular one) are available on many users' computers, file requests and retrievals may be faster than on other types of networks, and since file exchanges do not travel through a server, communications can take place between any computers that remain connected to the network without risk that a glitch in the server will disable the network in its entirety. Given these benefits in security, cost, and efficiency, peer-to-peer networks are employed to store and distribute electronic files by universities, government agencies, corporations, and libraries, among others.

Other users of peer-to-peer networks include individual recipients of Grokster's and StreamCast's software, and although the networks that they enjoy through using the software can be used to share any type of digital file, they have prominently employed those networks in sharing copyrighted music and video files without authorization. A group of copyright holders (MGM for short, but including motion picture studios, recording companies, songwriters, and music publishers) sued Grokster and StreamCast for their users' copyright infringements, alleging that they knowingly and intentionally distributed their software to enable users to reproduce and distribute the copyrighted works in violation of the Copyright Act. MGM sought damages and an injunction.

[The Court detailed StreamCast's architecture, which was more complex than Morpheus's in ways not material here.]

In the Gnutella network made available by Morpheus, ... peer computers using the protocol communicate directly with each other. When a user enters a search request into the Morpheus software, it sends the request to computers connected with it, which in turn pass the request along to other connected peers. The search results are communicated to the requesting computer, and the user can download desired files directly from peers' computers. As this description indicates, Grokster and StreamCast use no servers to intercept the content of the search requests or to mediate the file transfers conducted by users of the software, there being no central point through which the substance of the communications passes in either direction.

Although Grokster and StreamCast do not therefore know when particular files are copied, a few searches using their software would show what is available on the networks the software reaches. MGM commissioned a statistician to conduct a systematic search, and his study showed

that nearly 90% of the files available for download on the FastTrack system were copyrighted works. Grokster and StreamCast dispute this figure, raising methodological problems and arguing that free copying even of copyrighted works may be authorized by the rightholders. They also argue that potential noninfringing uses of their software are significant in kind, even if infrequent in practice. Some musical performers, for example, have gained new audiences by distributing their copyrighted works for free across peer-to-peer networks, and some distributors of unprotected content have used peer-to-peer networks to disseminate files, Shakespeare being an example. Indeed, StreamCast has given Morpheus users the opportunity to download the briefs in this very case, though their popularity has not been quantified.

As for quantification, the parties' anecdotal and statistical evidence entered thus far to show the content available on the FastTrack and Gnutella networks does not say much about which files are actually downloaded by users, and no one can say how often the software is used to obtain copies of unprotected material. But MGM's evidence gives reason to think that the vast majority of users' downloads are acts of infringement, and because well over 100 million copies of the software in question are known to have been downloaded, and billions of files are shared across the FastTrack and Gnutella networks each month, the probable scope of copyright infringement is staggering. ...

B.

After discovery, the parties on each side of the case crossmoved for summary judgment.

The District Court [ruled in favor of Grokster and StreamCast].

The Court of Appeals affirmed. In the court's analysis, a defendant was liable as a contributory infringer when it had knowledge of direct infringement and materially contributed to the infringement. But the court read *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U. S. 417 (1984), as holding that distribution of a commercial product capable of substantial noninfringing uses could not give rise to contributory liability for infringement unless the distributor had actual knowledge of specific instances of infringement and failed to act on that knowledge. The fact that the software was capable of substantial noninfringing uses in the Ninth Circuit's view meant that Grokster and StreamCast were not liable, because they had no such actual knowledge, owing to the decentralized architecture of their software. ...

The Ninth Circuit also considered whether Grokster and StreamCast could be liable under a theory of vicarious infringement. The court held against liability because the defendants did not monitor or control the use of the software, had no agreed-upon right or current ability to supervise its use, and had no independent duty to police infringement. We granted certiorari.

II.

...

Despite the currency of these principles of secondary liability, this Court has dealt with secondary copyright infringement in only one recent case, and because MGM has tailored its principal claim to our opinion there, a look at our earlier holding is in order. In *Sony Corp. v. Universal City Studios*, supra, this Court addressed a claim that secondary liability for infringement can arise from the very distribution of a commercial product. There, the product, novel at the time, was what we know today as the videocassette recorder or VCR. ...

On those facts, with no evidence of stated or indicated intent to promote infringing uses, the only conceivable basis for imposing liability was on a theory of contributory infringement arising from its sale of VCRs to consumers with knowledge that some would use them to infringe. But because the VCR was "capable of commercially significant noninfringing uses," we held the manufacturer could not be faulted solely on the basis of its distribution.. ...

In sum, where an article is good for nothing else but infringement, there is no legitimate public interest in its unlicensed availability, and there is no injustice in presuming or imputing an intent to infringe. Conversely, the doctrine absolves the equivocal conduct of selling an item with substantial lawful as well as unlawful uses, and limits liability to instances of more acute fault than the mere understanding that some of one's products will be misused. It leaves breathing room for innovation and a vigorous commerce.

The parties and many of the amici in this case think the key to resolving it is the Sony rule and, in particular, what it means for a product to be "capable of commercially significant noninfringing uses." *Sony Corp. v. Universal City Studios*, supra, at 442. MGM advances the argument that granting summary judgment to Grokster and StreamCast as to their current activities gave too much weight to the value of innovative technology, and too little to the copyrights infringed by users of their software, given that 90% of works available on one of the networks was shown to be copyrighted. Assuming the remaining 10% to be its noninfringing use, MGM says this should not qualify as "substantial," and the Court should quantify *Sony* to the extent of holding that a product used "principally" for infringement does not qualify. As mentioned before, Grokster and StreamCast reply by citing evidence that their software can be used to reproduce public domain works, and they point to copyright holders who actually encourage copying. Even if infringement is the principal practice with their software today, they argue, the noninfringing uses are significant and will grow. ...

Because Sony did not displace other theories of secondary liability, and because we find below that it was error to grant summary judgment to the companies on MGM's inducement claim, we do not revisit *Sony* further, as MGM requests, to add a more quantified description of the point of balance between protection and commerce when liability rests solely on distribution with knowledge that unlawful use will occur. It is enough to note that the Ninth Circuit's judgment rested on an erroneous understanding of *Sony* and to leave further consideration of the *Sony* rule for a day when that may be required.

C.

Sony's rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product. But nothing in *Sony* requires courts to ignore evidence of intent if there is such evidence, and the case was never meant to foreclose rules of fault-based liability derived from the common law. Thus, where evidence goes beyond a product's characteristics or the knowledge that it may be put to infringing uses, and shows statements or actions directed to promoting infringement, *Sony*'s staple-article rule will not preclude liability. ...

For the same reasons that *Sony* took the staple-article doctrine of patent law as a model for its copyright safe-harbor rule, the inducement rule, too, is a sensible one for copyright. We adopt it here, holding that one who distributes a device with the object of promoting its use to infringe copyright, as shown by clear expression or other affirmative steps taken to foster infringement, is liable for the resulting acts of infringement by third parties. We are, of course, mindful of the

need to keep from trenching on regular commerce or discouraging the development of technologies with lawful and unlawful potential. Accordingly, just as *Sony* did not find intentional inducement despite the knowledge of the VCR manufacturer that its device could be used to infringe, mere knowledge of infringing potential or of actual infringing uses would not be enough here to subject a distributor to liability. Nor would ordinary acts incident to product distribution, such as offering customers technical support or product updates, support liability in themselves. The inducement rule, instead, premises liability on purposeful, culpable expression and conduct, and thus does nothing to compromise legitimate commerce or discourage innovation having a lawful promise.

III.

A.

The only apparent question about treating MGM's evidence as sufficient to withstand summary judgment under the theory of inducement goes to the need on MGM's part to adduce evidence that StreamCast and Grokster communicated an inducing message to their software users. The classic instance of inducement is by advertisement or solicitation that broadcasts a message designed to stimulate others to commit violations. MGM claims that such a message is shown here. It is undisputed that StreamCast beamed onto the computer screens of users of Napster-compatible programs ads urging the adoption of its OpenNap program, which was designed, as its name implied, to invite the custom of patrons of Napster, then under attack in the courts for facilitating massive infringement. Those who accepted StreamCast's OpenNap program were offered software to perform the same services, which a factfinder could conclude would readily have been understood in the Napster market as the ability to download copyrighted music files. Grokster distributed an electronic newsletter containing links to articles promoting its software's ability to access popular copyrighted music. And anyone whose Napster or free file-sharing searches turned up a link to Grokster would have understood Grokster to be offering the same file-sharing ability as Napster, and to the same people who probably used Napster for infringing downloads; that would also have been the understanding of anyone offered Grokster's suggestively named Swaptor software, its version of OpenNap. And both companies communicated a clear message by responding affirmatively to requests for help in locating and playing copyrighted materials.

In StreamCast's case, of course, the evidence just described was supplemented by other unequivocal indications of unlawful purpose in the internal communications and advertising designs aimed at Napster users ("When the lights went off at Napster . . . where did the users go?"). Whether the messages were communicated is not to the point on this record. The function of the message in the theory of inducement is to prove by a defendant's own statements that his unlawful purpose disqualifies him from claiming protection (and incidentally to point to actual violators likely to be found among those who hear or read the message). Proving that a message was sent out, then, is the preeminent but not exclusive way of showing that active steps were taken with the purpose of bringing about infringing acts, and of showing that infringing acts took place by using the device distributed. Here, the summary judgment record is replete with other evidence that Grokster and StreamCast, unlike the manufacturer and distributor in *Sony*, acted with a purpose to cause copyright violations by use of software suitable for illegal use.

Three features of this evidence of intent are particularly notable. First, each company showed itself to be aiming to satisfy a known source of demand for copyright infringement, the

market comprising former Napster users. StreamCast's internal documents made constant reference to Napster, it initially distributed its Morpheus software through an OpenNap program compatible with Napster, it advertised its OpenNap program to Napster users, and its Morpheus software functions as Napster did except that it could be used to distribute more kinds of files, including copyrighted movies and software programs. Grokster's name is apparently derived from Napster, it too initially offered an OpenNap program, its software's function is likewise comparable to Napster's, and it attempted to divert queries for Napster onto its own Web site. Grokster and StreamCast's efforts to supply services to former Napster users, deprived of a mechanism to copy and distribute what were overwhelmingly infringing files, indicate a principal, if not exclusive, intent on the part of each to bring about infringement.

Second, this evidence of unlawful objective is given added significance by MGM's showing that neither company attempted to develop filtering tools or other mechanisms to diminish the infringing activity using their software. While the Ninth Circuit treated the defendants' failure to develop such tools as irrelevant because they lacked an independent duty to monitor their users' activity, we think this evidence underscores Grokster's and StreamCast's intentional facilitation of their users' infringement.

Third, there is a further complement to the direct evidence of unlawful objective. It is useful to recall that StreamCast and Grokster make money by selling advertising space, by directing ads to the screens of computers employing their software. As the record shows, the more the software is used, the more ads are sent out and the greater the advertising revenue becomes. Since the extent of the software's use determines the gain to the distributors, the commercial sense of their enterprise turns on high-volume use, which the record shows is infringing. This evidence alone would not justify an inference of unlawful intent, but viewed in the context of the entire record its import is clear.

The unlawful objective is unmistakable.

B.

In addition to intent to bring about infringement and distribution of a device suitable for infringing use, the inducement theory of course requires evidence of actual infringement by recipients of the device, the software in this case. As the account of the facts indicates, there is evidence of infringement on a gigantic scale, and there is no serious issue of the adequacy of MGM's showing on this point in order to survive the companies' summary judgment requests. Although an exact calculation of infringing use, as a basis for a claim of damages, is subject to dispute, there is no question that the summary judgment evidence is at least adequate to entitle MGM to go forward with claims for damages and equitable relief.

* * *

In sum, this case is significantly different from *Sony* and reliance on that case to rule in favor of StreamCast and Grokster was error. Sony dealt with a claim of liability based solely on distributing a product with alternative lawful and unlawful uses, with knowledge that some users would follow the unlawful course. The case struck a balance between the interests of protection and innovation by holding that the product's capability of substantial lawful employment should bar the imputation of fault and consequent secondary liability for the unlawful acts of others.

MGM's evidence in this case most obviously addresses a different basis of liability for distributing a product open to alternative uses. Here, evidence of the distributors' words and deeds going beyond distribution as such shows a purpose to cause and profit from third-party acts of copyright infringement. If liability for inducing infringement is ultimately found, it will not be on the basis of presuming or imputing fault, but from inferring a patently illegal objective from statements and actions showing what that objective was.

There is substantial evidence in MGM's favor on all elements of inducement, and summary judgment in favor of Grokster and StreamCast was error. On remand, reconsideration of MGM's motion for summary judgment will be in order.

The judgment of the Court of Appeals is vacated, and the case is remanded for further proceedings consistent with this opinion.

VISA problem

The following is taken from the statement of facts in *Perfect 10, Inc. v. Visa Intern. Service Ass'n,* 494 F. 3d 788 (9th Cir. 2007):

> Perfect 10 publishes the magazine "PERFECT10" and operates the subscription website www.perfect10.com, both of which "feature tasteful copyrighted images of the world's most beautiful natural models." Perfect 10 claims copyrights in the photographs published in its magazine and on its website, federal registration of the "PERFECT 10" trademark and blanket publicity rights for many of the models appearing in the photographs. Perfect 10 alleges that numerous websites based in several countries have stolen its proprietary images, altered them, and illegally offered them for sale online.
>
> Instead of suing the direct infringers in this case, Perfect 10 sued Defendants, financial institutions that process certain credit card payments to the allegedly infringing websites. The Visa and Master-Card entities are associations of member banks that issue credit cards to consumers, automatically process payments to merchants authorized to accept their cards, and provide information to the interested parties necessary to settle the resulting debits and credits. Defendants collect fees for their services in these transactions. Perfect 10 alleges that it sent Defendants repeated notices specifically identifying infringing websites and informing Defendants that some of their consumers use their payment cards to purchase infringing images. Defendants admit receiving some of these notices, but they took no action in response to the notices after receiving them.

The District Court has dismissed Perfect 10's copyright-infringement suit for failure to state a claim under Fed. R. Civ. Proc. 12(b)(6). You represent Perfect 10. Advise your client whether to appeal. (Given the citation above, in real life Perfect 10 clearly did choose to appeal. But should it have?)

Rip-Mix-Burn problem

Apple's Mac computers have CD drives which can read and write CDs. Apple's iTunes software, which ships pre-installed on every Mac, has features that can "rip" a CD into MP3 files stored on a user's hard drive and can "burn" a playlist of MP3s to a CD. You are Associate General Counsel at Apple, with responsibility for approving any marketing materials released by the company. Your advertising agency has proposed the following print ad to run in large-circulation magazines throughout the U.S. What's your call on it?

CLASS 25: OPEN SOURCE AND ANTI-CIRCUMVENTION

Today's class offers what may seem like an unusual pairing of topics: open-source software and the anti-circumvention rules of the Digital Millennium Copyright Act. Actually, they have more in common than one might expect.

Preparation questions

(1) Corley and *Remeirdes* are the same case. I've given you the facts from the Court of Appeals because its version was shorter. And I've given you the decision from the District Court because the defendants dropped their statutory argument on appeal. They should be read as a single case. Your first task is to understand the purpose of the DMCA, from the copyright owners' perspective. The key here is "digital rights management" or DRM: technological controls on copyrighted content, of which CSS is a great example. Why would a copyright owner slap DRM on an e-book, or a music file, or a movie? What business models does that enable? What other examples of DRM can you think of that you've come across in your daily life?

(2) DMCA Section 1201 is best understood as a DRM-protection law. [Section 1201 refers to "technological measures," but the concept is the same.] What kind of threats does the circumvention of DRM pose to copyright owners? (DeCSS is an example here. What does its existence do to the DVD business model?) Why, from a copyright owner's point of view, was pre-1998 copyright law insufficient to deal with this threat?

(3) Now, let's change gears and talk about open-source software. Read the ISC license, the GPL, and *Jacobsen*. Why would a programmer choose to give away her software voluntarily and for free? (There are multiple motivations here, so take a moment to brainstorm different ones.) How will a larger project that requires hundreds of programmers to collaborate—like the Linux operating system or the Firefox web browser—ever get written if the program is available to anyone for free? Does this tell us anything about Wikipedia? About YouTube? About other web sites?

(4) Note that both the ISC and GPL require that anyone who receives the software and distributes it in unmodified form keep intact the copyright notice and the license text. Why? How does that advance the goals of giving the software away?

(5) When it comes to *modified* software, however, they take different views. The ISC license is extremely permissive. If I receive software under the ISC license, I'm free to *change* it, then start selling copies of the software as though it had been proprietary, copyrighted software from the start. In contrast, the GPL is apparently more restrictive. It imposes two stringent conditions on the recipient who modifies the software and then starts distributing it. How does Clause 2 ensure that the software stays legally free, even as I make changes to it? And how does Clause 3 ensure that the software stays technically free, even as I make changes to it? The result is that the GPL is more restrictive on what recipients of the software can do, but more protective of third parties. Explain why. Is the Artistic license considered in *Jacobsen* more like the ISC license or the GPL?

(6) Of course, all of this licensing machinery is useless if you can't get a court to enforce your license conditions. *Jacobsen* is about the question of whether these terms are contractual covenants or conditions that limit the scope of a copyright license. Why does this matter?

What would the remedies be for breach of a contractual covenant? How about for copying the software beyond the scope of the license? How does *Jacobsen* answer this question? How would open source programmers feel about this decision? How do you think commercial developers—like, oh, say, the creators of CSS—feel about this decision?

(7) Now, we're ready to bring everything together. *Corley/Remeirdes* shows us the collision of two worlds: the copyright industries with their DRM, and hackers with their open-source software. But DRM and open-source software are deeply incompatible. Why? Similarly, the cultural values of the copyright industries and of hackers are deeply incompatible. Why? What happened when they collided?

ISC License

Copyright (c) Year(s), Company or Person's Name <E-mail address>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

GNU General Public License (GPL)
Version 2

PREAMBLE

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. ...

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". ...

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
>
> c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.) ...

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. ...

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License. ...

Jacobsen v. Katzer
535 F.3d 1373 (2008)

HOCHBERG, District Judge.

We consider here the ability of a copyright holder to dedicate certain work to free public use and yet enforce an "open source" copyright license to control the future distribution and modification of that work. Appellant Robert Jacobsen ("Jacobsen") appeals from an order denying a motion for preliminary injunction. Jacobsen holds a copyright to computer programming code. He makes that code available for public download from a website without a financial fee pursuant to the Artistic License, an "open source" or public license. Appellees Matthew Katzer and Kamind Associates, Inc. (collectively "Katzer/Kamind") develop commercial software products for the model train industry and hobbyists. Jacobsen accused Katzer/Kamind of copying certain materials from Jacobsen's website and incorporating them into one of Katzer/Kamind's software packages without following the terms of the Artistic License. Jacobsen brought an action for copyright infringement and moved for a preliminary injunction.

The District Court held that the open source Artistic License created an "intentionally broad" nonexclusive license which was unlimited in scope and thus did not create liability for copyright infringement. The District Court reasoned:

> The plaintiff claimed that by modifying the software the defendant had exceeded the scope of the license and therefore infringed the copyright. Here, however, the JMRI Project license provides that a user may copy the files verbatim or may otherwise modify the material in any way, including as part of a larger, possibly commercial software distribution. The license explicitly gives the users of the material, any member of the public, "the right to use and distribute the [material] in a more-or-less customary fashion, plus the right to make reasonable accommodations." The scope of the nonexclusive license is, therefore, intentionally broad. The condition that the user insert a prominent notice of attribution does not limit the scope of the license. Rather, Defendants' alleged violation of the conditions of the license may have constituted a breach of the nonexclusive license, but does not create liability for copyright infringement where it would not otherwise exist.

On this basis, the District Court denied the motion for a preliminary injunction. We vacate and remand.

I.

Jacobsen manages an open source software group called Java Model Railroad Interface ("JMRI"). Through the collective work of many participants, JMRI created a computer programming application called DecoderPro, which allows model railroad enthusiasts to use their computers to program the decoder chips that control model trains. DecoderPro files are available for download and use by the public free of charge from an open source incubator website called SourceForge; Jacobsen maintains the JMRI site on SourceForge. The downloadable files contain copyright notices and refer the user to a "COPYING" file, which clearly sets forth the terms of the Artistic License.

Katzer/Kamind offers a competing software product, Decoder Commander, which is also used to program decoder chips. During development of Decoder Commander, one of Katzer/ Kamind's predecessors or employees is alleged to have downloaded the decoder definition files from DecoderPro and used portions of these files as part of the Decoder Commander software. The Decoder Commander software files that used DecoderPro definition files did not comply with the terms of the Artistic License. Specifically, the Decoder Commander software did not include (1) the author' names, (2) JMRI copyright notices, (3) references to the COPYING file, (4) an identification of SourceForge or JMRI as the original source of the definition files, and (5) a description of how the files or computer code had been changed from the original source code. The Decoder Commander software also changed various computer file names of Decoder-Pro files without providing a reference to the original JMRI files or information on where to get the Standard Version.

Jacobsen moved for a preliminary injunction, arguing that the violation of the terms of the Artistic License constituted copyright infringement and that, under Ninth Circuit law, irreparable harm could be presumed in a copyright infringement case. The District Court reviewed the Artistic License and determined that "Defendants' alleged violation of the conditions of the license may have constituted a breach of the nonexclusive license, but does not create liability for copyright infringement where it would not otherwise exist." The District Court found that Jacobsen had a cause of action only for breach of contract, rather than an action for copyright infringement based on a breach of the conditions of the Artistic License. Because a breach of

contract creates no presumption of irreparable harm, the District Court denied the motion for a preliminary injunction. ...

II.

[A]n order granting or denying a preliminary injunction will be reversed only if the district court relied on an erroneous legal premise or abused its discretion. A district court's order denying a preliminary injunction is reversible for factual error only when the district court rests its conclusions on clearly erroneous findings of fact.

... Thus, for a preliminary injunction to issue, Jacobsen must either show (1) a likelihood of success on the merits of his copyright infringement claim from which irreparable harm is presumed; or (2) a fair chance of success on the merits and a clear disparity in the relative hardships that tips sharply in his favor.

A.

Public licenses, often referred to as "open source" licenses, are used by artists, authors, educators, software developers, and scientists who wish to create collaborative projects and to dedicate certain works to the public. Several types of public licenses have been designed to provide creators of copyrighted materials a means to protect and control their copyrights. Creative Commons, one of the amici curiae, provides free copyright licenses to allow parties to dedicate their works to the public or to license certain uses of their works while keeping some rights reserved.

Open source licensing has become a widely used method of creative collaboration that serves to advance the arts and sciences in a manner and at a pace that few could have imagined just a few decades ago. For example, the Massachusetts Institute of Technology ("MIT") uses a Creative Commons public license for an OpenCourseWare project that licenses all 1800 MIT courses. Other public licenses support the GNU/Linux operating system, the Perl programming language, the Apache web server programs, the Firefox web browser, and a collaborative web-based encyclopedia called Wikipedia. Creative Commons notes that, by some estimates, there are close to 100,000,000 works licensed under various Creative Commons licenses. The Wikimedia Foundation, another of the amici curiae, estimates that the Wikipedia website has more than 75,000 active contributors working on some 9,000,000 articles in more than 250 languages.

Open Source software projects invite computer programmers from around the world to view software code and make changes and improvements to it. Through such collaboration, software programs can often be written and debugged faster and at lower cost than if the copyright holder were required to do all of the work independently. In exchange and in consideration for this collaborative work, the copyright holder permits users to copy, modify and distribute the software code subject to conditions that serve to protect downstream users and to keep the code accessible. By requiring that users copy and restate the license and attribution information, a copyright holder can ensure that recipients of the redistributed computer code know the identity of the owner as well as the scope of the license granted by the original owner. The Artistic License in this case also requires that changes to the computer code be tracked so that downstream users know what part of the computer code is the original code created by the copyright holder and what part has been newly added or altered by another collaborator.

Traditionally, copyright owners sold their copyrighted material in exchange for money. The lack of money changing hands in open source licensing should not be presumed to mean that there is no economic consideration, however. There are substantial benefits, including economic benefits, to the creation and distribution of copyrighted works under public licenses that range far beyond traditional license royalties. For example, program creators may generate market share for their programs by providing certain components free of charge. Similarly, a programmer or company may increase its national or international reputation by incubating open source projects. Improvement to a product can come rapidly and free of charge from an expert not even known to the copyright holder. ...

B.

The parties do not dispute that Jacobsen is the holder of a copyright for certain materials distributed through his website. Katzer/Kamind also admits that portions of the DecoderPro software were copied, modified, and distributed as part of the Decoder Commander software. Accordingly, Jacobsen has made out a prima facie case of copyright infringement. Katzer/Kamind argues that they cannot be liable for copyright infringement because they had a license to use the material. Thus, the Court must evaluate whether the use by Katzer/Kamind was outside the scope of the license. The copyrighted materials in this case are downloadable by any user and are labeled to include a copyright notification and a COPYING file that includes the text of the Artistic License.

The Artistic License grants users the right to copy, modify, and distribute the software:

> provided that [the user] insert a prominent notice in each changed file stating how and when [the user] changed that file, and provided that [the user] do at least ONE of the following:
>
> a) place [the user's] modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as ftp.uu.net, or by allowing the Copyright Holder to include [the user's] modifications in the Standard Version of the Package.
>
> b) use the modified Package only within [the user's] corporation or organization.
>
> c) rename any non-standard executables so the names do not conflict with the standard executables, which must also be provided, and provide a separate manual page for each nonstandard executable that clearly documents how it differs from the Standard Version, or
>
> d) make other distribution arrangements with the Copyright Holder.

The heart of the argument on appeal concerns whether the terms of the Artistic License are conditions of, or merely covenants to, the copyright license. Generally, a copyright owner who grants a nonexclusive license to use his copyrighted material waives his right to sue the licensee for copyright infringement and can sue only for breach of contract. If, however, a license is limited in scope and the licensee acts outside the scope, the licensor can bring an action for copyright infringement.

Thus, if the terms of the Artistic License allegedly violated are both covenants and conditions, they may serve to limit the scope of the license and are governed by copyright law. If

they are merely covenants, by contrast, they are governed by contract law. The District Court did not expressly state whether the limitations in the Artistic License are independent covenants or, rather, conditions to the scope; its analysis, however, clearly treated the license limitations as contractual covenants rather than conditions of the copyright license.

Jacobsen argues that the terms of the Artistic License define the scope of the license and that any use outside of these restrictions is copyright infringement. Katzer/Kamind argues that these terms do not limit the scope of the license and are merely covenants providing contractual terms for the use of the materials, and that his violation of them is neither compensable in damages nor subject to injunctive relief. ...

III.

The Artistic License states on its face that the document creates conditions: "The intent of this document is to state the conditions under which a Package may be copied." (Emphasis added.) The Artistic License also uses the traditional language of conditions by noting that the rights to copy, modify, and distribute are granted "provided that" the conditions are met. Under California contract law, "provided that" typically denotes a condition.

The conditions set forth in the Artistic License are vital to enable the copyright holder to retain the ability to benefit from the work of downstream users. By requiring that users who modify or distribute the copyrighted material retain the reference to the original source files, downstream users are directed to Jacobsen's website. Thus, downstream users know about the collaborative effort to improve and expand the SourceForge project once they learn of the "upstream" project from a "downstream" distribution, and they may join in that effort.

The District Court interpreted the Artistic License to permit a user to "modify the material in any way" and did not find that any of the "provided that" limitations in the Artistic License served to limit this grant. The District Court's interpretation of the conditions of the Artistic License does not credit the explicit restrictions in the license that govern a downloader's right to modify and distribute the copyrighted work. The copyright holder here expressly stated the terms upon which the right to modify and distribute the material depended and invited direct contact if a downloader wished to negotiate other terms. These restrictions were both clear and necessary to accomplish the objectives of the open source licensing collaboration, including economic benefit. ...

Copyright holders who engage in open source licensing have the right to control the modification and distribution of copyrighted material. ... Copyright licenses are designed to support the right to exclude; money damages alone do not support or enforce that right. The choice to exact consideration in the form of compliance with the open source requirements of disclosure and explanation of changes, rather than as a dollar-denominated fee, is entitled to no less legal recognition. Indeed, because a calculation of damages is inherently speculative, these types of license restrictions might well be rendered meaningless absent the ability to enforce through injunctive relief.

In this case, a user who downloads the JMRI copyrighted materials is authorized to make modifications and to distribute the materials "provided that" the user follows the restrictive terms of the Artistic License. A copyright holder can grant the right to make certain modifications, yet retain his right to prevent other modifications. Indeed, such a goal is exactly the purpose of adding conditions to a license grant. The Artistic License, like many other common copyright

licenses, requires that any copies that are distributed contain the copyright notices and the COPYING file.

It is outside the scope of the Artistic License to modify and distribute the copyrighted materials without copyright notices and a tracking of modifications from the original computer files. If a down loader does not assent to these conditions stated in the COPYING file, he is instructed to "make other arrangements with the Copyright Holder." Katzer/Kamind did not make any such "other arrangements." The clear language of the Artistic License creates conditions to protect the economic rights at issue in the granting of a public license. These conditions govern the rights to modify and distribute the computer programs and files included in the downloadable software package. The attribution and modification transparency requirements directly serve to drive traffic to the open source incubation page and to inform downstream users of the project, which is a significant economic goal of the copyright holder that the law will enforce. Through this controlled spread of information, the copyright holder gains creative collaborators to the open source project; by requiring that changes made by downstream users be visible to the copyright holder and others, the copyright holder learns about the uses for his software and gains others' knowledge that can be used to advance future software releases.

IV.

For the aforementioned reasons, we vacate and remand. While Katzer/Kamind appears to have conceded that they did not comply with the aforedescribed conditions of the Artistic License, the District Court did not make factual findings on the likelihood of success on the merits in proving that Katzer/Kamind violated the conditions of the Artistic License. Having determined that the terms of the Artistic License are enforceable copyright conditions, we remand to enable the District Court to determine whether Jacobsen has demonstrated (1) a likelihood of success on the merits and either a presumption of irreparable harm or a demonstration of irreparable harm; or (2) a fair chance of success on the merits and a clear disparity in the relative hardships and tipping in his favor.

Universal City Studios, Inc. v. Corley
273 F. 3d 429 (2d Cir. 2001)

Background

For decades, motion picture studios have made movies available for viewing at home in what is called "analog" format. Movies in this format are placed on videotapes, which can be played on a video cassette recorder ("VCR"). In the early 1990s, the studios began to consider the possibility of distributing movies in digital form as well. Movies in digital form are placed on discs, known as DVDs, which can be played on a DVD player (either a stand-alone device or a component of a computer). DVDs offer advantages over analog tapes, such as improved visual and audio quality, larger data capacity, and greater durability. However, the improved quality of a movie in a digital format brings with it the risk that a virtually perfect copy, i.e., one that will not lose perceptible quality in the copying process, can be readily made at the click of a computer control and instantly distributed to countless recipients throughout the world over the Internet. This case arises out of the movie industry's efforts to respond to this risk by invoking the anti-trafficking provisions of the DMCA.

I. CSS

The movie studios were reluctant to release movies in digital form until they were confident they had in place adequate safeguards against piracy of their copyrighted movies. The studios took several steps to minimize the piracy threat. First, they settled on the DVD as the standard digital medium for home distribution of movies. The studios then sought an encryption scheme to protect movies on DVDs. They enlisted the help of members of the consumer electronics and computer industries, who in mid-1996 developed the Content Scramble System ("CSS"). CSS is an encryption scheme that employs an algorithm configured by a set of "keys" to encrypt a DVD's contents. The algorithm is a type of mathematical formula for transforming the contents of the movie file into gibberish; the "keys" are in actuality strings of 0's and 1's that serve as values for the mathematical formula.

Decryption in the case of CSS requires a set of "player keys" contained in compliant DVD players, as well as an understanding of the CSS encryption algorithm. Without the player keys and the algorithm, a DVD player cannot access the contents of a DVD. With the player keys and the algorithm, a DVD player can display the movie on a television or a computer screen, but does not give a viewer the ability to use the copy function of the computer to copy the movie or to manipulate the digital content of the DVD.

The studios developed a licensing scheme for distributing the technology to manufacturers of DVD players. Player keys and other information necessary to the CSS scheme were given to manufacturers of DVD players for an administrative fee. In exchange for the licenses, manufacturers were obliged to keep the player keys confidential. Manufacturers were also required in the licensing agreement to prevent the transmission of "CSS data" (a term undefined in the licensing agreement) from a DVD drive to any "internal recording device," including, presumably, a computer hard drive.

With encryption technology and licensing agreements in hand, the studios began releasing movies on DVDs in 1997, and DVDs quickly gained in popularity, becoming a significant source of studio revenue. In 1998, the studios secured added protection against DVD piracy when Congress passed the DMCA, which prohibits the development or use of technology designed to circumvent a technological protection measure, such as CSS. The pertinent provisions of the DMCA are examined in greater detail below.

II. DeCSS

In September 1999, Jon Johansen, a Norwegian teenager, collaborating with two unidentified individuals he met on the Internet, reverse-engineered a licensed DVD player designed to operate on the Microsoft operating system, and culled from it the player keys and other information necessary to decrypt CSS. The record suggests that Johansen was trying to develop a DVD player operable on Linux, an alternative operating system that did not support any licensed DVD players at that time. In order to accomplish this task, Johansen wrote a decryption program executable on Microsoft's operating system. That program was called, appropriately enough, "DeCSS."

If a user runs the DeCSS program (for example, by clicking on the DeCSS icon on a Microsoft operating system platform) with a DVD in the computer's disk drive, DeCSS will decrypt the DVD's CSS protection, allowing the user to copy the DVD's files and place the copy on the user's hard drive. The result is a very large computer file that can be played on a non-

CSS-compliant player and copied, manipulated, and transferred just like any other computer file. [5] DeCSS comes complete with a fairly user-friendly interface that helps the user select from among the DVD's files and assign the decrypted file a location on the user's hard drive. The quality of the resulting decrypted movie is "virtually identical" to that of the encrypted movie on the DVD. And the file produced by DeCSS, while large, can be compressed to a manageable size by a compression software called "DivX," available at no cost on the Internet. This compressed file can be copied onto a DVD, or transferred over the Internet (with some patience).

Johansen posted the executable object code, but not the source code, for DeCSS on his web site. The distinction between source code and object code is relevant to this case, so a brief explanation is warranted. A computer responds to electrical charges, the presence or absence of which is represented by strings of 1's and 0's. Strictly speaking, "object code" consists of those 1's and 0's. While some people can read and program in object code, it would be inconvenient, inefficient and, for most people, probably impossible to do so. Computer languages have been written to facilitate program writing and reading. A program in such a computer language — BASIC, C, and Java are examples — is said to be written in "source code." Source code has the benefit of being much easier to read (by people) than object code, but as a general matter, it must be translated back to object code before it can be read by a computer. This task is usually performed by a program called a compiler. Since computer languages range in complexity, object code can be placed on one end of a spectrum, and different kinds of source code can be arrayed across the spectrum according to the ease with which they are read and understood by humans. Within months of its appearance in executable form on Johansen's web site, DeCSS was widely available on the Internet, in both object code and various forms of source code.

In November 1999, [defendant Eric] Corley wrote and placed on his web site, 2600.com, an article about the DeCSS phenomenon. His web site is an auxiliary to the print magazine, 2600: The Hacker Quarterly, which Corley has been publishing since 1984. As the name suggests, the magazine is designed for "hackers," as is the web site. While the magazine and the web site cover some issues of general interest to computer users — such as threats to online privacy — the focus of the publications is on the vulnerability of computer security systems, and more specifically, how to exploit that vulnerability in order to circumvent the security systems. Representative articles explain how to steal an Internet domain name and how to break into the computer systems at Federal Express.

Corley's article about DeCSS detailed how CSS was cracked, and described the movie industry's efforts to shut down web sites posting DeCSS. It also explained that DeCSS could be used to copy DVDs. At the end of the article, the Defendants posted copies of the object and source code of DeCSS. In Corley's words, he added the code to the story because "in a journalistic world, ... [y]ou have to show your evidence ... and particularly in the magazine that I work for, people want to see specifically what it is that we are referring to," including "what evidence ... we have" that there is in fact technology that circumvents CSS. Writing about DeCSS without including the DeCSS code would have been, to Corley, "analogous to printing a story about a picture and not printing the picture." Corley also added to the article links that he explained would take the reader to other web sites where DeCSS could be found.

2600.com was only one of hundreds of web sites that began posting DeCSS near the end of 1999. The movie industry tried to stem the tide by sending cease-and-desist letters to many of

these sites. These efforts met with only partial success; a number of sites refused to remove DeCSS. In January 2000, the studios filed this lawsuit. ...

Universal City Studios, Inc. v. Reimerdes
111 F. Supp. 2d 294 (S.D.N.Y. 2000)

II. The Digital Millennium Copyright Act

A. Background and Structure of the Statute

In December 1996, the World Intellectual Property Organization ("WIPO"), held a diplomatic conference in Geneva that led to the adoption of two treaties. Article 11 of the relevant treaty, the WIPO Copyright Treaty, provides in relevant part that contracting states "shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorized by the authors concerned or permitted by law."

The adoption of the WIPO Copyright Treaty spurred continued Congressional attention to the adaptation of the law of copyright to the digital age. Lengthy hearings involving a broad range of interested parties both preceded and succeeded the Copyright Treaty. As noted above, a critical focus of Congressional consideration of the legislation was the conflict between those who opposed anti-circumvention measures as inappropriate extensions of copyright and impediments to fair use and those who supported them as essential to proper protection of copyrighted materials in the digital age. The DMCA was enacted in October 1998 as the culmination of this process.

The DMCA contains two principal anti-circumvention provisions. The first, Section 1201(a)(1), governs "[t]he 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.

B. Posting of DeCSS

1. Violation of Anti-Trafficking Provision

Section 1201(a)(2) of the Copyright Act, part of the DMCA, provides that:

> "No person shall ... offer to the public, provide or otherwise traffic in any technology ... that —
>
> "(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act];

"(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under [the Copyright Act]; or

"(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act]."

In this case, defendants concededly offered and provided and, absent a court order, would continue to offer and provide DeCSS to the public by making it available for download on the 2600.com web site. DeCSS, a computer program, unquestionably is "technology" within the meaning of the statute. "[C]ircumvent a technological measure" is defined to mean descrambling a scrambled work, decrypting an encrypted work, or "otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner," so DeCSS clearly is a means of circumventing a technological access control measure. In consequence, if CSS otherwise falls within paragraphs (A), (B) or (C) of Section 1201(a)(2), and if none of the statutory exceptions applies to their actions, defendants have violated and, unless enjoined, will continue to violate the DMCA by posting DeCSS.

a. Section 1201(a)(2)(A)

(1) CSS Effectively Controls Access to Copyrighted Works

During pretrial proceedings and at trial, defendants attacked plaintiffs' Section 1201(a)(2)(A) claim, arguing that CSS, which is based on a 40-bit encryption key, is a weak cipher that does not "effectively control" access to plaintiffs' copyrighted works. They reasoned from this premise that CSS is not protected under this branch of the statute at all. Their post-trial memorandum appears to have abandoned this argument. In any case, however, the contention is indefensible as a matter of law.

First, the statute expressly provides that "a technological measure `effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information or a process or a treatment, with the authority of the copyright owner, to gain access to a work." One cannot gain access to a CSS-protected work on a DVD without application of the three keys that are required by the software. One cannot lawfully gain access to the keys except by entering into a license with the DVD CCA under authority granted by the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to such a license. In consequence, under the express terms of the statute, CSS "effectively controls access" to copyrighted DVD movies. It does so, within the meaning of the statute, whether or not it is a strong means of protection.

This view is confirmed by the legislative history, which deals with precisely this point. The House Judiciary Committee section-by-section analysis of the House bill, which in this respect was enacted into law, makes clear that a technological measure "effectively controls access" to a copyrighted work if its function is to control access:

"The bill does define the functions of the technological measures that are covered — that is, what it means for a technological measure to `effectively control access to a work' ... and to `effectively protect a right of a copyright owner under this title' .... The practical, common-sense approach taken by H.R.2281 is that if, in the ordinary course

> of its operation, a technology actually works in the defined ways to control access to a work ... then the `effectiveness' test is met, and the prohibitions of the statute are applicable. This test, which focuses on the function performed by the technology, provides a sufficient basis for clear interpretation."

Further, the House Commerce Committee made clear that measures based on encryption or scrambling "effectively control" access to copyrighted works, although it is well known that what may be encrypted or scrambled often may be decrypted or unscrambled. As CSS, in the ordinary course of its operation — that is, when DeCSS or some other decryption program is not employed — "actually works" to prevent access to the protected work, it "effectively controls access" within the contemplation of the statute.

Finally, the interpretation of the phrase "effectively controls access" offered by defendants at trial — viz., that the use of the word "effectively" means that the statute protects only successful or efficacious technological means of controlling access — would gut the statute if it were adopted. If a technological means of access control is circumvented, it is, in common parlance, ineffective. Yet defendants' construction, if adopted, would limit the application of the statute to access control measures that thwart circumvention, but withhold protection for those measures that can be circumvented. In other words, defendants would have the Court construe the statute to offer protection where none is needed but to withhold protection precisely where protection is essential. The Court declines to do so. Accordingly, the Court holds that CSS effectively controls access to plaintiffs' copyrighted works.

(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.

b. 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.

c. 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. The argument plays itself out in various ways as different elements of the DMCA come into focus. But it perhaps is useful to address the point at its most general level in order to place the preceding discussion in its fullest context.

As noted, Section 1201(a) of the DMCA contains two distinct prohibitions. Section 1201(a)(1), the so-called basic provision, "aims against those who engage in unauthorized circumvention of technological measures.... [It] focuses directly on wrongful conduct, rather than on those who facilitate wrongful conduct...." Section 1201(a)(2), the anti-trafficking provision at issue in this

case, on the other hand, separately bans offering or providing technology that may be used to circumvent technological means of controlling access to copyrighted works. If the means in question meets any of the three prongs of the standard set out in Section 1201(a)(2)(A), (B), or (C), it may not be offered or disseminated.

As the earlier discussion demonstrates, the question whether the development of a Linux DVD player motivated those who wrote DeCSS is immaterial to the question whether the defendants now before the Court violated the anti-trafficking provision of the DMCA. The inescapable facts are that (1) CSS is a technological means that effectively controls access to plaintiffs' copyrighted works, (2) the one and only function of DeCSS is to circumvent CSS, and (3) defendants offered and provided DeCSS by posting it on their web site. Whether defendants did so in order to infringe, or to permit or encourage others to infringe, copyrighted works in violation of other provisions of the Copyright Act simply does not matter for purposes of Section 1201(a)(2). The offering or provision of the program is the prohibited conduct — and it is prohibited irrespective of why the program was written, except to whatever extent motive may be germane to determining whether their conduct falls within one of the statutory exceptions. ...

d. 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.

The use of technological means of controlling access to a copyrighted work may affect the ability to make fair uses of the work. Focusing specifically on the facts of this case, the application of CSS to encrypt a copyrighted motion picture requires the use of a compliant DVD player to view or listen to the movie. Perhaps more significantly, it prevents exact copying of either the video or the audio portion of all or any part of the film. This latter point means that certain uses that might qualify as "fair" for purposes of copyright infringement — for example, the preparation by a film studies professor of a single CD-ROM or tape containing two scenes from different movies in order to illustrate a point in a lecture on cinematography, as opposed to showing relevant parts of two different DVDs — would be difficult or impossible absent circumvention of the CSS encryption. 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.

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.

Congress was well aware during the consideration of the DMCA of the traditional role of the fair use defense in accommodating the exclusive rights of copyright owners with the legitimate interests of noninfringing users of portions of copyrighted works. It recognized the contention, voiced by a range of constituencies concerned with the legislation, that technological controls on access to copyrighted works might erode fair use by preventing access even for uses that would be deemed "fair" if only access might be gained. And it struck a balance among the competing interests.

The first element of the balance was the careful limitation of Section 1201(a)(1)'s prohibition of the act of circumvention to the act itself so as not to "apply to subsequent actions of a person once he or she has obtained authorized access to a copy of a [copyrighted] work...." By doing so, it left "the traditional defenses to copyright infringement, including fair use, ... fully applicable" provided "the access is authorized." ...

Third, it created a series of exceptions to aspects of Section 1201(a) for certain uses that Congress thought "fair," including reverse engineering, security testing, good faith encryption research, and certain uses by nonprofit libraries, archives and educational institutions. ...

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. ...

When *Sony* was decided, the only question was whether the manufacturers could be held liable for infringement by those who purchased equipment from them in circumstances in which there were many noninfringing uses for their equipment. But that is not the question now before this Court. The question here is whether the possibility of noninfringing fair use by someone who gains access to a protected copyrighted work through a circumvention technology distributed by the defendants saves the defendants from liability under Section 1201. But nothing in Section 1201 so suggests. By prohibiting the provision of circumvention technology, the DMCA fundamentally altered the landscape. A given device or piece of technology might have "a substantial noninfringing use, and hence be immune from attack under *Sony*'s construction of the Copyright Act — but nonetheless still be subject to suppression under Section 1201."Indeed, Congress explicitly noted that Section 1201 does not incorporate *Sony*.

The policy concerns raised by defendants were considered by Congress. Having considered them, Congress crafted a statute that, so far as the applicability of the fair use defense to Section 1201(a) claims is concerned, is crystal clear. In such circumstances, courts may not undo what Congress so plainly has done by "construing" the words of a statute to accomplish a result that Congress rejected. The fact that Congress elected to leave technologically unsophisticated

persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so is a matter for Congress unless Congress' decision contravenes the Constitution, a matter to which the Court turns below. Defendants' statutory fair use argument therefore is entirely without merit.

[The court concluded that Section 1201 does not unconstitutionally abridge free speech rights.]

CLASS 26: SECTION 512

Today we take up the statutory provision commonly known as "section 512." Technically, it's the Online Copyright Infringement Liability Limitation Act, which was Title II of the DMCA, and which added section 512 to Title 17 of the U.S. Code. But people will make fun of you if you insist on these details, and with good reason. So "section 512" it is. In basic form, it provides protection for various online intermediaries from copyright liability.

The motivation for such a statute should be fairly clear at this point. Suppose that Irene Infringer uploads a copyrighted MP3 to her personal web site on a server operated by Epitome Hosting, and that Doug Downloader downloads it via his Ultraband cable Internet service. *Sony* will presumably supply a defense to the manufacturers of the server, the cable modem, and the various network cables. But what about Epitome and Ultraband, who provide services? Epitome's servers made a reproduction and publicly distributed the MP3, and Ultraband used its cables and routers to transmit the MP3, which is arguably a reproduction, a distribution, and/or a performance. You don't even need to get into the *Napster* analysis: based on what we've studied, this looks like direct infringement.

Congress dealt with this situation in section 512. It gives Epitome, Ultraband, and other "service providers" immunity from copyright liability provided they comply with various threshold conditions. The basic structure is that Congress provides four independent immunities in clauses (a) through (d), each of which covers a different aspect of a service provider's operations. Each then comes with its own laundry list of conditions. Most notably, the immunity applicable to Epitome—the "hosting" immunity under 512(c)—includes an obligation known as "notice and takedown." The immunity vanishes if the copyright owner sends a specially formatted notice of infringement to the service provider, unless the service provider takes the allegedly infringing material down.

Today's material is dense. Here's how I recommend you prepare. Start by skimming the statute, included at the start of this packet. Then skim through the two assigned cases, noting briefly the issues they raise and the context in which those issues arise. Then flip back here and work through the preparation questions, referring to the statute as needed and reading, in detail, the relevant sections of the cases.

Preparation questions:

(1) Let's start by thinking about how the notice and takedown process works with reference to *Lenz*. YouTube, like Epitome, depends on the 512(c) immunity for "storage [of infringing material] at the direction of a user." But notice that 512(c)(1)(C) conditions that immunity on taking prompt action when it receives a notice of claimed infringement. What's the statutory language that tells us what YouTube must do? If YouTube receives a "DMCA notice," as they're called, and does nothing, what result? If the video clip was a fair use and YouTube does nothing, is YouTube liable for its inaction? What do you think YouTube will *actually* do when it receives a DMCA notice? Compare this legal regime to section 230 and to the common-law trademark regime applied in *Tiffany v. eBay*.

(2) Congress responded to the risk of overly aggressive DMCA notices with two provisions, both of which you see at work in *Lenz*. One, codified in 512(g), is generally called "counter-notice and putback." Why? How does it work? How quickly? What do you think YouTube actually does when it receives one? Does the copyright owner have any recourse if the

alleged infringer files a counter-notice? Read the statute before you answer. The other, codified in 512(f), gives a civil cause of action against anyone who makes knowing material misrepresentations in sending takedown notices. Reading through *Lenz*, how easy do you think it is for victims of mistaken takedowns to win these suits? Overall, does 512(c) favor copyright owners or users?

(3) Now, let's turn to the threshold issues. *CCBill* (the third in Perfect 10's war-on-the-Internet litigation campaign) will be our text here. First, note that the defendants raise defenses under 512(a), 512(c), and 512(d). Read the statute and the discussion in *CCBill* and try to explain what distinguishes these three safe-harbors. It's best to think of each safe-harbor as covering different activities; it's possible for a defendant to be immune under one for certain activities (e.g. hosting content at YouTube.com) and under another for different ones (e.g. providing a search engine at Google.com). Note that 512(d) imposes a similar notice-and-takedown regime to 512(c), but that 512(a) doesn't. Why not?

(4) The next common source of section 512 litigation is the "repeat infringer" policy provision in 512(i). What obligations does this requirement impose on service providers? One of the questions the *CCBill* court considers is how CCBill and CWIE are supposed to decide who is a "repeat infringer." What sources of information is a hosting provider supposed to look to? Must it investigate its service searching for infringing materials, and if so, how aggressively? What role do DMCA notices play in this process? What about things that are kind of like DMCA notices but fail one or more of the statutory requirements?

(5) 512(c) imposes two further threshold tests for a hosting provider to qualify for the safe harbor. The first, codified in 512(c)(1)(A), requires that the service provider "not have actual knowledge that the material ... is infringing; is not aware of facts or circumstances from which infringing activity is apparent; or upon obtaining such knowledge or awareness acts expeditiously to remove, or disable access to, the material." Does this remind you of anything we've studied? The second, codified in 512(c)(1)(B), requires that the service provider "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." Does that remind you of anything we've studied?

Lenz v. Universal Music Corp.
572 F. Supp. 2d 1150 (N.D. Cal. 2008)

JEREMY FOGEL, District Judge. ...

I. BACKGROUND

On February 7, 2007, Plaintiff Stephanie Lenz ("Lenz") videotaped her young children dancing in her family's kitchen. The song "Let's Go Crazy" by the artist professionally known as Prince ("Prince") played in the background. The video is twenty nine seconds in length, and "Let's Go Crazy" can be heard for approximately twenty seconds, albeit with difficulty given the poor sound quality of the video. The audible portion of the song includes the lyrics, "C'mon baby let's get nuts" and the song's distinctive guitar solo. Lenz is heard asking her son, "what do you think of the music?" On February 8, 2007, Lenz titled the video "Let's Go Crazy # 1" and uploaded it to YouTube.com ("YouTube"), a popular Internet video hosting site, for the alleged

purpose of sharing her son's dancing with friends and family. YouTube provides "video sharing" or "user generated content." The video was available to the public at http://www.youtube.com/watch?v=N1KfJHFW1hQ [and it still is].

Universal owns the copyright to "Let's Go Crazy." On June 4, 2007, Universal sent YouTube a takedown notice pursuant to Title II of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512 (2000). The notice was sent to YouTube's designated address for receiving DMCA notices, "copyright@youtube.com," and demanded that YouTube remove Lenz's video from the site because of a copyright violation. YouTube removed the video the following day and sent Lenz an email notifying her that it had done so in response to Universal's accusation of copyright infringement. YouTube's email also advised Lenz of the DMCA's counter-notification procedures and warned her that any repeated incidents of copyright infringement could lead to the deletion of her account and all of her videos. After conducting research and consulting counsel, Lenz sent YouTube a DMCA counter-notification pursuant to 17 U.S.C. § 512(g) on June 27, 2007. Lenz asserted that her video constituted fair use of "Let's Go Crazy" and thus did not infringe Universal's copyrights. Lenz demanded that the video be re-posted. YouTube re-posted the video on its website about six weeks later. As of the date of this order, the "Let's Go Crazy # 1" video has been viewed on YouTube more than 593,000 times.

In September 2007, Prince spoke publicly about his efforts "to reclaim his art on the internet" and threatened to sue several internet service providers for alleged infringement of his music copyrights. Lenz alleges that Universal issued the removal notice only to appease Prince because Prince "is notorious for his efforts to control all uses of his material on and off the Internet." In an October 2007 statement to ABC News, Universal made the following comment:

> Prince believes it is wrong for YouTube, or any other user-generated site, to appropriate his music without his consent. That position has nothing to do with any particular video that uses his songs. It's simply a matter of principle. And legally, he has the right to have his music removed. We support him and this important principle. That's why, over the last few months, we have asked You-Tube to remove thousands of different videos that use Prince music without his permission.

Lenz asserts in her complaint that "Prince himself demanded that Universal seek the removal of the ["Let's Go Crazy # 1"] video ... [and that] Universal sent the DMCA notice at Prince's behest, based not on the particular characteristics of [the video] or any good-faith belief that it actually infringed a copyright but on its belief that, as 'a matter of principle' Prince 'has the right to have his music removed.'"

On July 24, 2007, Lenz filed suit against Universal alleging misrepresentation pursuant to 17 U.S.C. § 512(f) and tortious interference with her contract with YouTube. ...

III. DISCUSSION

The DMCA requires that copyright owners provide the following information in a takedown notice:

> ...
>
> (v) *A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.*

> (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

17 U.S.C. § 512(c)(3)(A) (emphasis added). Here, the parties do not dispute that Lenz used copyrighted material in her video or that Universal is the true owner of Prince's copyrighted music. Thus the question in this case is whether 17 U.S.C. § 512(c)(3)(A)(v) requires a copyright owner to consider the fair use doctrine in formulating a good faith belief that "use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law."

Universal contends that copyright owners cannot be required to evaluate the question of fair use prior to sending a takedown notice because fair use is merely an excused infringement of a copyright rather than a use authorized by the copyright owner or by law. Universal emphasizes that Section 512(c)(3)(A) does not even mention fair use, let alone require a good faith belief that a given use of copyrighted material is not fair use. Universal also contends that even if a copyright owner were required by the DMCA to evaluate fair use with respect to allegedly infringing material, any such duty would arise only after a copyright owner receives a counternotice and considers filing suit. *See* 17 U.S.C. § 512(g)(2)(C).

Lenz argues that fair use is an authorized use of copyrighted material, noting that the fair use doctrine itself is an express component of copyright law. Indeed, Section 107 of the Copyright Act of 1976 provides that "[n]otwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work ... is not an infringement of copyright." 17 U.S.C. § 107. Lenz asserts in essence that copyright owners cannot represent in good faith that material infringes a copyright without considering all authorized uses of the material, including fair use. ...

A. Fair Use and 17 U.S.C. § 512(c)(3)(A)(v).

... Though Congress did not expressly mention the fair use doctrine in the DMCA, the Copyright Act provides explicitly that "the fair use of a copyrighted work ... is not an infringement of copyright." 17 U.S.C. § 107. Even if Universal is correct that fair use only excuses infringement, the fact remains that fair use is a lawful use of a copyright. Accordingly, in order for a copyright owner to proceed under the DMCA with "a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law," the owner must evaluate whether the material makes fair use of the copyright. 17 U.S.C. § 512(c)(3)(A)(v). An allegation that a copyright owner acted in bad faith by issuing a takedown notice without proper consideration of the fair use doctrine thus is sufficient to state a misrepresentation claim pursuant to Section 512(f) of the DMCA. Such an interpretation of the DMCA furthers both the purposes of the DMCA itself and copyright law in general. In enacting the DMCA, Congress noted that the "provisions in the bill balance the need for rapid response to potential infringement with the end-users [sic] legitimate interests in not having material removed without recourse."

Universal suggests that copyright owners may lose the ability to respond rapidly to potential infringements if they are required to evaluate fair use prior to issuing takedown notices. Universal also points out that the question of whether a particular use of copyrighted material constitutes fair use is a fact-intensive inquiry, and that it is difficult for copyright owners to predict whether a court eventually may rule in their favor. However, while these concerns are

understandable, their actual impact likely is overstated. Although there may be cases in which such considerations will arise, there are likely to be few in which a copyright owner's determination that a particular use is not fair use will meet the requisite standard of subjective bad faith required to prevail in an action for misrepresentation under 17 U.S.C. § 512(f). *See Rossi v. Motion Picture Ass'n of America, Inc.*, 391 F.3d 1000, 1004 (9th Cir.2004) (holding that "the 'good faith belief requirement in § 512(c)(3)(A)(v) encompasses a subjective, rather than objective, standard'").[1] ...

Undoubtedly, some evaluations of fair use will be more complicated than others. But in the majority of cases, a consideration of fair use prior to issuing a takedown notice will not be so complicated as to jeopardize a copyright owner's ability to respond rapidly to potential infringements. The DMCA already requires copyright owners to make an initial review of the potentially infringing material prior to sending a takedown notice; indeed, it would be impossible to meet any of the requirements of Section 512(c) without doing so. A consideration of the applicability of the fair use doctrine simply is part of that initial review. As the Ninth Circuit observed in *Rossi*, a full investigation to verify the accuracy of a claim of infringement is not required.

The purpose of Section 512(f) is to prevent the abuse of takedown notices. If copyright owners are immune from liability by virtue of ownership alone, then to a large extent Section 512(f) is superfluous. As Lenz points out, the unnecessary removal of non-infringing material causes significant injury to the public where time-sensitive or controversial subjects are involved and the counter-notification remedy does not sufficiently address these harms. A good faith consideration of whether a particular use is fair use is consistent with the purpose of the statute. Requiring owners to consider fair use will help "ensure[] that the efficiency of the Internet will continue to improve and that the variety and quality of services on the Internet will expand" without compromising "the movies, music, software and literary works that are the fruit of American creative genius." Sen. Rep. No. 105-190 at 2 (1998). ...

Perfect 10, Inc. v. CCBill LLC
488 F.3d 1102 (9th Cir. 2007)

MILAN D. SMITH, JR., Circuit Judge:

Perfect 10, the publisher of an adult entertainment magazine and the owner of the subscription website perfect10.com, alleges that CCBill and CWIE violated copyright, trademark, and state unfair competition, false advertising and right of publicity laws by providing services to websites that posted images stolen from Perfect 10's magazine and website. Perfect 10 appeals the district court's finding that CCBill and CWIE qualified for certain statutory safe harbors from copyright infringement liability under the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 512, and that CCBill and CWIE were immune from liability for state law unfair competition and false advertising claims based on the Communications Decency Act

---

[1] One might imagine a case in which an alleged infringer uses copyrighted material in a manner that unequivocally qualifies as fair use, and in addition there is evidence that the copyright owner deliberately has invoked the DMCA not to protect its copyright but to prevent such use. *See*, *e.g.*, *Online Policy Group v. Diebold, Inc.*, 337 F.Supp.2d 1195, 1204-05 (N.D.Cal.2004) (suggesting that the copyright owner sought to use the DMCA "as a sword to suppress publication of embarrassing content rather than as a shield to protect its intellectual property").

("CDA"), 47 U.S.C. § 230(c)(1). CCBill and CWIE cross-appeal, arguing that the district court erred in holding that the CDA does not provide immunity against Perfect 10's right of publicity claims and in denying their requests for costs and attorney's fees under the Copyright Act.

We have jurisdiction pursuant to 28 U.S.C. § 1291. We affirm in part, reverse in part, and remand.

BACKGROUND

Perfect 10 is the publisher of the eponymous adult entertainment magazine and the owner of the website, perfect10.com. Perfect10.com is a subscription site where consumers pay a membership fee in order to gain access to content on the website. Perfect 10 has created approximately 5,000 images of models for display in its website and magazine. Many of the models in these images have signed releases assigning their rights of publicity to Perfect 10. Perfect 10 also holds registered U.S. copyrights for these images and owns several related, registered trademark and service marks.

CWIE provides webhosting and related Internet connectivity services to the owners of various websites. For a fee, CWIE provides "ping, power, and pipe," services to their clients by ensuring the "box" or server is on, ensuring power is provided to the server and connecting the client's service or website to the Internet via a data center connection. CCBill allows consumers to use credit cards or checks to pay for subscriptions or memberships to e-commerce venues.

Beginning August 10, 2001, Perfect 10 sent letters and emails to CCBill and CWIE stating that CCBill and CWIE clients were infringing Perfect 10 copyrights. Perfect 10 directed these communications to Thomas A. Fisher, the designated agent to receive notices of infringement. Fisher is also the Executive Vice-President of both CCBill and CWIE. Representatives of celebrities who are not parties to this lawsuit also sent notices of infringement to CCBill and CWIE. On September 30, 2002, Perfect 10 filed the present action alleging copyright and trademark violations, state law claims of violation of right of publicity, unfair competition, false and misleading advertising, as well as RICO claims.

STANDARDS OF REVIEW

We review a district court's grant of summary judgment de novo. Viewing the evidence in the light most favorable to the nonmoving party, we must determine whether there are any genuine issues of material fact and whether the district court correctly applied the relevant substantive law. The district court's interpretations of the Copyright Act are also reviewed de novo.

We review a district court's decision to grant or deny attorney's fees under the Copyright Act for abuse of discretion.

DISCUSSION

I. SECTION 512 SAFE HARBORS

The DMCA established certain safe harbors to "provide protection from liability for: (1) transitory digital network communications; (2) system caching; (3) information residing on systems or networks at the direction of users; and (4) information location tools." *Ellison*, 357 F.3d at 1076-77 (citing 17 U.S.C. §§ 512(a)-(d)) (footnotes omitted). These safe harbors limit liability but "do not affect the question of ultimate liability under the various doctrines of direct,

vicarious, and contributory liability," *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1174 (C.D. Cal. 2002) (citing H.R. Rep. 105-551 (II), at 50 (1998) ("H.R. Rep."), and "nothing in the language of *§ 512* indicates that the limitation on liability described therein is exclusive." *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 552 (4th Cir. 2004).

A. Reasonably Implemented Policy: § 512(i)(1)(A)

To be eligible for any of the four safe harbors at §§ 512(a)-(d), a service provider must first meet the threshold conditions set out in § 512(i), including the requirement that the service provider:

> [H]as adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, 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.

Section 512(i)(1)(A); *Ellison*, 357 F.3d at 1080.

The statute does not define "reasonably implemented." We hold that a service provider "implements" a policy if it has a working notification system, a procedure for dealing with DMCA-compliant notifications, and if it does not actively prevent copyright owners from collecting information needed to issue such notifications. The statute permits service providers to implement a variety of procedures, but an implementation is reasonable if, under "appropriate circumstances," the service provider terminates users who repeatedly or blatantly infringe copyright.

1. "Implementation"

Perfect 10 argues that there is a genuine issue of material fact whether CCBill and CWIE prevented the implementation of their policies by failing to keep track of repeatedly infringing webmasters. The district court found that there was not, and we agree.

In *Ellison*, Stephen Robertson posted copies of Harlan Ellison's copyrighted short stories on Internet newsgroups available through USENET servers. 357 F.3d at 1075. Ellison asserted that America Online, Inc. ("AOL") had infringed his copyright by providing access to the USENET servers. *Id.* Based on evidence that AOL changed its contact email address for copyright infringement notices from copyright@aol.com to aolcopyright@aol.com in the fall of 1999, but neglected to register the change with the U.S. Copyright Office until April 2000, we held that the district court erred in concluding on summary judgment that AOL satisfied the requirements of § 512(i). *Id.* at 1077. Even though Ellison did not learn of the infringing activity until after AOL had notified the U.S. Copyright Office of the correct email address, we found that "AOL allowed notices of potential copyright infringement to fall into a vacuum and go unheeded; that fact is sufficient for a reasonable jury to conclude that AOL had not reasonably implemented its policy against repeat infringers." *Id.* at 1080.

Similarly, the *Aimster* cases hold that a repeat infringer policy is not implemented under § 512 (i)(1)(A) if the service provider prevents copyright holders from providing DMCA-compliant notifications. In *Aimster*, the district court held that Aimster did not reasonably implement its stated repeat infringer policy because "the encryption on Aimster renders it impossible to ascertain which users are transferring which files." 252 F. Supp. 2d at 659. The court found that "[a]dopting a repeat infringer policy and then purposely eviscerating any hope that such a policy

could ever be carried out is not an 'implementation' as required by § 512(i)." *Id.* The Seventh Circuit affirmed, finding that Aimster did not meet the requirement of § 512(i)(1)(A) because, in part, "by teaching its users how to encrypt their unlawful distribution of copyrighted materials [Aimster] disabled itself from doing anything to prevent infringement." *In re Aimster Copyright Litig.*, 334 F.3d 643, 655 (7th Cir. 2003).

Based on *Ellison* and the *Aimster* cases, a substantial failure to record webmasters associated with allegedly infringing websites may raise a genuine issue of material fact as to the implementation of the service provider's repeat infringer policy. In this case, however, the record does not reflect such a failure. Perfect 10 references a single page from CCBill and CWIE's "DMCA Log." Although this page shows some empty fields in the spreadsheet column labeled "Webmasters [sic] Name," Perfect 10's conclusion that the DMCA Log thus "does not reflect any effort to track notices of infringements received by webmaster identity" is not supported by evidence in the record. The remainder of the DMCA Log indicates that the email address and/or name of the webmaster is routinely recorded in CCBill and CWIE's DMCA Log. CCBill's interrogatory responses dated December 11, 2003 also contain a chart indicating that CCBill and CWIE largely kept track of the webmaster for each website.

Unlike *Ellison* and *Aimster*, where the changed email address and the encryption system ensured that *no* information about the repeat infringer was collected, it is undisputed that CCBill and CWIE recorded most webmasters. The district court properly concluded that the DMCA Log does not raise a triable issue of fact that CCBill and CWIE did not implement a repeat infringer policy.

2. Reasonableness

A service provider reasonably implements its repeat infringer policy if it terminates users when "appropriate." *See Corbis*, 351 F. Supp. 2d at 1104. Section 512(i) itself does not clarify when it is "appropriate" for service providers to act. It only requires that a service provider terminate users who are "repeat infringers."

To identify and terminate repeat infringers, a service provider need not affirmatively police its users for evidence of repeat infringement. Section 512(c) states that "[a] service provider shall not be liable for monetary relief" if it does not know of infringement. A service provider is also not liable under § 512(c) if it acts "expeditiously to remove, or disable access to, the material" when it (1) has actual knowledge, (2) is aware of facts or circumstances from which infringing activity is apparent, or (3) has received notification of claimed infringement meeting the requirements of § 512(c)(3). Were we to require service providers to terminate users under circumstances other than those specified in § 512(c), § 512(c)'s grant of immunity would be meaningless. This interpretation of the statute is supported by legislative history. *See* H.R. Rep., at 61 (Section 512(i) is not intended "to undermine the . . . knowledge standard of [§ 512](c).").

Perfect 10 claims that CCBill and CWIE unreasonably implemented their repeat infringer policies by tolerating flagrant and blatant copyright infringement by its users despite notice of infringement from Perfect 10, notice of infringement from copyright holders not a party to this litigation and "red flags" of copyright infringement.

a. Perfect 10's Claimed Notice of Infringement

Perfect 10 argues that CCBill and CWIE implemented their repeat infringer policy in an unreasonable manner because CCBill and CWIE received notices of infringement from Perfect 10, and yet the infringement identified in these notices continued. The district court found that Perfect 10 did not provide notice that substantially complied with the requirements of § 512(c)(3),[2] and thus did not raise a genuine issue of material fact as to whether CCBill and CWIE reasonably implemented their repeat infringer policy. We agree.

Compliance is not "substantial" if the notice provided complies with only some of the requirements of § 512(c)(3)(A). Section 512(c)(3)(B)(ii) explains that a service provider will not be deemed to have notice of infringement when "the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A)" so long as the service provider responds to the inadequate notice and explains the requirements for substantial compliance. The statute thus signals that substantial compliance means substantial compliance with *all* of *§ 512(c)(3)*'s clauses, not just some of them. *See* H.R. Rep., at 56 (A communication substantially complies even if it contains technical errors such as misspellings or outdated information.). *See also Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs., Inc.*, 359 U.S. App. D.C. 85, 351 F.3d 1229, 1236 (D.C. Cir. 2003) (citing H.R. Rep., at 56).

Perfect 10 claims that it met the requirements of § 512(c)(3) through a combination of three sets of documents. The first set of documents is a 22,185 page bates-stamped production on October 16, 2002 that includes pictures with URLs of Perfect 10 models allegedly posted on CCBill or CWIE client websites. The October 16, 2002 production did not contain a statement under penalty of perjury that the complaining party was authorized to act, as required by § 512(c)(3)(A)(vi). The second set of documents was also not sworn to, and consisted of a spreadsheet emailed to Fisher on July 14, 2003 identifying the Perfect 10 models in the October 16, 2002 production by bates number. On December 2, 2003, Perfect 10 completed interrogatory responses which were signed under penalty of perjury. These responses incorporated the July 14, 2003 spreadsheet by reference.

---

[2] Section 512(c)(3) reads:

> (A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:
>
> (i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
>
> (ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.
>
> (iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.
>
> (iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.
>
> (v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.
>
> (vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Taken individually, Perfect 10's communications do not substantially comply with the requirements of § 512(c)(3). Each communication contains more than mere technical errors; often one or more of the required elements are entirely absent. *See Perfect 10, Inc. v. CCBill, LLC*, 340 F. Supp. 2d 1077, 1100-01 (C.D. Cal. 2004) ("Order"). In order to substantially comply with § 512(c)(3)'s requirements, a notification must do more than identify infringing files. The DMCA requires a complainant to declare, under penalty of perjury, that he is authorized to represent the copyright holder, and that he has a good-faith belief that the use is infringing. This requirement is not superfluous. Accusations of alleged infringement have drastic consequences: A user could have content removed, or may have his access terminated entirely. If the content infringes, justice has been done. But if it does not, speech protected under the First Amendment could be removed. We therefore do not require a service provider to start potentially invasive proceedings if the complainant is unwilling to state under penalty of perjury that he is an authorized representative of the copyright owner, and that he has a good-faith belief that the material is unlicensed.

Permitting a copyright holder to cobble together adequate notice from separately defective notices also unduly burdens service providers. Indeed, the text of § 512(c)(3) requires that the notice be "*a* written communication." (Emphasis added). Again, this requirement is not a mere technicality. It would have taken Fisher substantial time to piece together the relevant information for each instance of claimed infringement. To do so, Fisher would have to first find the relevant line in the spreadsheet indicating ownership information, then comb the 22,185 pages provided by Perfect 10 in order to find the appropriate image, and finally copy into a browser the location printed at the top of the page -- a location which was, in some instances, truncated. The DMCA notification procedures place the burden of policing copyright infringement -- identifying the potentially infringing material and adequately documenting infringement -- squarely on the owners of the copyright. We decline to shift a substantial burden from the copyright owner to the provider; Perfect 10's separate communications are inadequate.

Since Perfect 10 did not provide effective notice, knowledge of infringement may not be imputed to CCBill or CWIE based on Perfect 10's communications. Perfect 10's attempted notice does not raise a genuine issue of material fact that CCBill and CWIE failed to reasonably implement a repeat infringer policy within the meaning of § 512(i)(1)(A).

b. Non-Party Notices

Perfect 10 also cites to notices of infringement by other copyright holders, and argues that CCBill and CWIE did not reasonably implement their repeat infringer policies because they continued to provide services for websites that infringed non-party copyrights. The district court expressly declined to consider evidence of notices provided by any party other than Perfect 10 on the basis that these notices were irrelevant to Perfect 10's claims. We disagree.

CCBill and CWIE's actions towards copyright holders who are not a party to the litigation are relevant in determining whether CCBill and CWIE reasonably implemented their repeat infringer policy. Section 512(i)(1)(A) requires an assessment of the service provider's "policy," not how the service provider treated a particular copyright holder. *See Ellison*, 357 F.3d at 1080 (AOL's repeat infringer policy was not reasonably implemented because copyright holders other than Ellison could have attempted to notify AOL during the time that AOL's email address was incorrectly listed.). Thus, CCBill and CWIE's response to adequate non-party notifications is

relevant in determining whether they reasonably implemented their policy against repeat infringers.

A policy is unreasonable only if the service provider failed to respond when it had knowledge of the infringement. The district court in this case did not consider any evidence relating to copyright holders other than Perfect 10. We remand for determination of whether CCBill and/or CWIE implemented its repeat infringer policy in an unreasonable manner with respect to any copyright holder other than Perfect 10.

c. Apparent Infringing Activity

In importing the knowledge standards of § 512(c) to the analysis of whether a service provider reasonably implemented its § 512(i) repeat infringer policy, Congress also imported the "red flag" test of § 512(c)(1)(A)(ii). Under this section, a service provider may lose immunity if it fails to take action with regard to infringing material when it is "aware of facts or circumstances from which infringing activity is apparent." § 512(c)(1)(A)(ii). Notice that fails to substantially comply with § 512(c)(3), however, cannot be deemed to impart such awareness. §§ 512(c)(3)(B)(i) & (ii).

Perfect 10 alleges that CCBill and CWIE were aware of a number of "red flags" that signaled apparent infringement. Because CWIE and CCBill provided services to "illegal.net" and "stolencelebritypics.com," Perfect 10 argues that they must have been aware of apparent infringing activity. We disagree. When a website traffics in pictures that are titillating by nature, describing photographs as "illegal" or "stolen" may be an attempt to increase their salacious appeal, rather than an admission that the photographs are actually illegal or stolen. We do not place the burden of determining whether photographs are actually illegal on a service provider.

Perfect 10 also argues that a disclaimer posted on illegal.net made it apparent that infringing activity had taken place. Perfect 10 alleges no facts showing that CWIE and CCBill were aware of that disclaimer, and, in any event, we disagree that the disclaimer made infringement apparent. The disclaimer in question stated: "The copyrights of these files remain the creator's. I do not claim any rights to these files, other than the right to post them." Contrary to Perfect 10's assertion, this disclaimer is not a "red flag" of infringement. The disclaimer specifically states that the webmaster has the right to post the files.

In addition, Perfect 10 argues that password-hacking websites, hosted by CWIE, also obviously infringe. While such sites may not directly infringe on anyone's copyright, they may well contribute to such infringement. The software provided by Grokster in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 125 S. Ct. 2764, 162 L. Ed. 2d 781 (2005), also did not itself infringe, but did enable users to swap infringing files. *Grokster* held that "instructing [users] how to engage in an infringing use" could constitute contributory infringement. *Id.* at 936. Similarly, providing passwords that enable users to illegally access websites with copyrighted content may well amount to contributory infringement.

However, in order for a website to qualify as a "red flag" of infringement, it would need to be apparent that the website instructed or enabled users to infringe another's copyright. *See A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1013 n.2 (9th Cir. 2001). We find that the burden of determining whether passwords on a website enabled infringement is not on the service provider. The website could be a hoax, or out of date. The owner of the protected content may have supplied the passwords as a short-term promotion, or as an attempt to collect information from

unsuspecting users. The passwords might be provided to help users maintain anonymity without infringing on copyright. There is simply no way for a service provider to conclude that the passwords enabled infringement without trying the passwords, and verifying that they enabled illegal access to copyrighted material. We impose no such investigative duties on service providers. Password-hacking websites are thus not *per se* "red flags" of infringement.

Perfect 10 also alleges that "red flags" raised by third parties identified repeat infringers who were not terminated. Because the district court did not consider potential red flags raised by third parties, we remand to the district court to determine whether third-party notices made CCBill and CWIE aware that it provided services to repeat infringers, and if so, whether they responded appropriately.

C. Transitory Digital Network Communications: § 512(a)

Section 512(a) provides safe harbor for service providers who act as conduits for infringing content. In order to qualify for the safe harbor of § 512(a), a party must be a service provider under a more restrictive definition than applicable to the other safe harbors provided under § 512:

> As used in subsection (a), the term "service provider" means 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.

Section 512 (k)(1)(A). The district court held that CCBill met the requirements of § 512(k)(1)(A) by "provid[ing] a connection to the material on its clients' websites through a system which it operates in order to provide its clients with billing services." We reject Perfect 10's argument that CCBill is not eligible for immunity under § 512(a) because it does not itself transmit the infringing material. A service provider is "an entity offering the transmission, routing, or providing of connections for digital online communications." § 512(k)(1)(A). There is no requirement in the statute that the communications must themselves be infringing, and we see no reason to import such a requirement. It would be perverse to hold a service provider immune for transmitting information that was infringing on its face, but find it contributorily liable for transmitting information that did not infringe.

Section 512(a) provides a broad grant of immunity to service providers whose connection with the material is transient. When an individual clicks on an Internet link, his computer sends a request for the information. The company receiving that request sends that request on to another computer, which sends it on to another. After a series of such transmissions, the request arrives at the computer that stores the information. The requested information is then returned in milliseconds, not necessarily along the same path. In passing the information along, each intervening computer makes a short-lived copy of the data. A short time later, the information is displayed on the user's computer.

Those intervening computers provide transient connections among users. The Internet as we know it simply cannot exist if those intervening computers must block indirectly infringing content. We read § 512(a)'s grant of immunity exactly as it is written: Service providers are immune for transmitting all digital online communications, not just those that directly infringe.

CCBill transmits credit card information and proof of payment, both of which are "digital online communications." However, we have little information as to how CCBill sends the payment it receives to its account holders. It is unclear whether such payment is a digital communication, transmitted without modification to the content of the material, or transmitted often enough that CCBill is only a transient holder. On the record before us, we cannot conclude that CCBill is a service provider under § 512(a). Accordingly, we remand to the district court for further consideration the issue of whether CCBill meets the requirements of § 512(a).

D. Information Location Tools: § 512(d)

After CCBill processes a consumer's credit card and issues a password granting access to a client website, CCBill displays a hyperlink so that the user may access the client website. CCBill argues that it falls under the safe harbor of § 512(d) by displaying this hyperlink at the conclusion of the consumer transaction. We disagree. Section 512(d) reads:

> 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 provider 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.

Even if the hyperlink provided by CCBill could be viewed as an "information location tool," the majority of CCBill's functions would remain outside of the safe harbor of § 512(d). Section 512(d) provides safe harbor only for "infringement of copyright *by reason of* the provider referring or linking users to an online location containing infringing material or infringing activity." (Emphasis added). Perfect 10 does not claim that CCBill infringed its copyrights by providing a hyperlink; rather, Perfect 10 alleges infringement through CCBill's performance of other business services for these websites. Even if CCBill's provision of a hyperlink is immune under § 512(n), CCBill does not receive blanket immunity for its other services.

E. Information Residing on Systems or Networks at the Direction of Users: § 512(c)

Section 512(c) "limits the liability of qualifying service providers for claims of direct, vicarious, and contributory infringement for 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." H.R. Rep., at 53. A service provider qualifies for safe harbor under § 512(c) if it meets the requirements of § 512(i) and:

> (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.

Section 512(c)(1). As discussed above, Perfect 10 did not provide CWIE with knowledge or awareness within the standard of § 512(c)(1)(A), and Perfect 10 did not provide notice that complies with the requirements of § 512(c)(3).

The remaining question is whether Perfect 10 raises a genuine issue of material fact that CWIE does not qualify for safe harbor under § 512(c) because it fails to meet the requirements of § 512(c)(1)(B), namely, that a service provider not receive a direct financial benefit from the infringing activity if the service provider also has the right and ability to control the infringing activity.

Based on the "well-established rule of construction that where Congress uses terms that have accumulated settled meaning under common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of these terms,"*Rossi*, 391 F.3d at 1004 n.4 (9th Cir. 2004) (quoting *Neder v. United States*, 527 U.S. 1, 21, 119 S. Ct. 1827, 144 L. Ed. 2d 35 (1999)), we hold that "direct financial benefit" should be interpreted consistent with the similarly-worded common law standard for vicarious copyright liability. *See*, *e.g.*, *Ellison*, 357 F.3d at 1078 (a vicariously liable copyright infringer "derive[s] a direct financial benefit from the infringement and ha[s] the right and ability to supervise the infringing activity"). Thus, the relevant inquiry is "whether the infringing activity constitutes a draw for subscribers, not just an added benefit." *Id.*. In *Ellison*, the court held that "no jury could reasonably conclude that AOL received a direct financial benefit from providing access to the infringing material" because "[t]he record lacks evidence that AOL attracted or retained subscriptions because of the infringement or lost subscriptions because of AOL's eventual obstruction of the infringement." *Id.*

In this case, Perfect 10 provides almost no evidence about the alleged direct financial benefit to CWIE. Perfect 10 only alleges that "CWIE 'hosts' websites for a fee." This allegation is insufficient to show that the infringing activity was "a draw" as required by *Ellison.* 357 F.3d at 1079. Furthermore, the legislative history expressly states that "receiving a one-time set-up fee and flat, periodic payments for service from a person engaging in infringing activities would not constitute receiving a 'financial benefit directly attributable to the infringing activity.'" H.R. Rep., at 54. Perfect 10 has not raised a genuine issue of material fact that CWIE receives a direct financial benefit from infringing activity. Because CWIE does not receive a direct financial benefit, CWIE meets the requirements of § 512(c).

If the district court finds that CWIE meets the threshold requirements of § 512(i), CWIE is entitled to safe harbor under § 512(c).

II. COMMUNICATIONS DECENCY ACT

The Communications Decency Act states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by

another information content provider," and expressly preempts any state law to the contrary. 47 U.S.C. §§ 230(c)(1), (e)(3). "The majority of federal circuits have interpreted the CDA to establish broad 'federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.'" *Almeida v. Amazon.com, Inc.*, 456 F. 3d 1316, 1321 (11th Cir. 2006) (quoting *Zeran v. America Online, Inc.*, 129 F.3d 327, 331 (4th Cir. 1997)); *see also Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003) (citing *Batzel v. Smith*, 333 F.3d 1018, 1026-27 (9th Cir. 2003)).

The immunity created by § 230(c)(1) is limited by § 230(e)(2), which requires the court to "construe Section 230(c)(1) in a manner that would neither 'limit or expand any law pertaining to intellectual property.'" *Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001) (quoting § 230(e)(2)). As a result, the CDA does not clothe service providers in immunity from "law[s] pertaining to intellectual property." *See Almeida*, 456 F.3d at 1322.

The CDA does not contain an express definition of "intellectual property," and there are many types of claims in both state and federal law which may -- or may not -- be characterized as "intellectual property" claims. While the scope of federal intellectual property law is relatively well-established, state laws protecting "intellectual property," however defined, are by no means uniform. Such laws may bear various names, provide for varying causes of action and remedies, and have varying purposes and policy goals. Because material on a website may be viewed across the Internet, and thus in more than one state at a time, permitting the reach of any particular state's definition of intellectual property to dictate the contours of this federal immunity would be contrary to Congress's expressed goal of insulating the development of the Internet from the various state-law regimes. *See* 47 U.S.C. §§ 230(a) and (b); *see also Batzel*, 333 F.3d at 1027 (noting that "courts construing § 230 have recognized as critical in applying the statute the concern that lawsuits could threaten the 'freedom of speech in the new and burgeoning Internet medium'" (quoting *Zeran*, 129 F.3d at 330)). In the absence of a definition from Congress, we construe the term "intellectual property" to mean "federal intellectual property." Accordingly, CCBill and CWIE are eligible for CDA immunity for all of the state claims raised by Perfect 10.

III. DIRECT COPYRIGHT INFRINGEMENT

"Plaintiffs must satisfy two requirements to present a prima facie case of direct infringement: (1) they must show ownership of the allegedly infringed material and (2) they must demonstrate that the alleged infringers violate at least one exclusive right granted to copyright holders under 17 U.S.C. § 106." *Napster*, 239 F.3d at 1013. Perfect 10 alleges that CCBill and CWIE directly infringed its copyrights through its website, hornybees.com.

There is a genuine issue of material fact as to the relationship between CCBill/CWIE and hornybees.com. CCBill and CWIE state that hornybees.com is operated by an entity called "CCBucks," and that CCBill and CWIE have no interest in hornybees.com. However, the hornybees.com website reads: "Brought to you by CCBill LLC and Cavecreek Web Hosting." The record indicates that Cavecreek Web Hosting may be CWIE, and that CWIE may be the registrant of hornybees.com. Furthermore, the vice president of operations of both CCBill and CWIE lists CCBucks as being related to CWIE and CCBill.

Perfect 10 has also raised a genuine issue of material fact that hornybees.com has infringed Perfect 10's copyrights by posting pictures of a Perfect 10 model's body with the head of a

celebrity. The declaration provided by Perfect 10's founder and president asserting that the photo is that of a Perfect 10 model is sufficient evidence to raise a genuine issue of material fact.

Because Perfect 10 has raised a triable issue whether CCBill and CWIE directly infringed Perfect 10 copyrights by operating hornybees.com, and because the district court did not address this issue in its order granting summary judgment in favor of Perfect 10, we remand this issue for a determination by the district court.

Section 512 problems

(1) Michael Crook posted a fake ad on Craigslist pretending to be a 19-year-old female college student seeking a casual sexual encounter, and asking men to send pictures. When men responded, he published their names and pictures to his web site. Blogger Jeffery Diehl wrote a post about Crook, which he illustrated with a photograph of Crook appearing on FOX News. Crook sent a DMCA takedown notice to BlueFX hosting, Diehl's web host, which insisted that Diehl remove the photograph. Diehl has sued Crook under § 512(f). Does Diehl have a case?

(2) Veoh is a video-sharing web site that allows users to upload videos in a variety of file formats. It then automatically converts (or "transcodes") the videos into the standard file format used by the Adobe Flash Player. Other users of the site can then either stream the videos to their computer, or download them as playable video files. UMG Recordings has sued Veoh for copyright infringement of hundreds of music videos. UMG argues that Veoh is ineligible for any of the 512 safe harbors because it modifies the video files. Is Veoh ineligible?

(3) The remaining three questions consider questions raised by the pending *Viacom v. YouTube* litigation. YouTube has developed "fingerprinting" technology that allows it to detect whether an uploaded video is substantially identical to a previously-uploaded one. By keeping a list of fingerprints of video files supplied by copyright owners, YouTube can prevent videos that have been taken down from being uploaded again. Viacom, which is suing YouTube for copyright infringement, alleges that YouTube offered in 2007 to apply the fingerprinting technology to block Viacom videos from being uploaded, but only if Viacom entered into a licensing arrangement with YouTube that would otherwise release YouTube from liability. Only in 2008 did YouTube begin applying the fingerprinting technology routinely, without also requiring a licensing agreement. If proven, how do these facts affect the question of whether YouTube is eligible for the 512 safe harbors?

(4) Also as part of the suit, Viacom alleges that one of YouTube's founders personally uploaded infringing videos to the site (although it cannot prove that any of these videos were copyrighted by Viacom), that YouTube's internal surveys revealed that 70% or more of the videos on the site were self-evidently infringing, that YouTube had contemplated being more rigorous in weeding out infringing videos but feared that doing so would reduce the site's appeal, and that Google was aware of these facts when it purchased YouTube. If proven, how do these facts affect the question of whether YouTube is eligible for the 512 safe harbors?

(5) Also as part of the suit, YouTube alleges that Viacom employees have personally uploaded videos that were later the subject of DMCA takedown notices by Viacom. Viacom has twice amended its complaint in the suit to remove videos that further investigation determined had been uploaded by Viacom or one of its agents. YouTube further alleges that Viacom employed independent marketing companies to upload videos without making it appear they were coming from Viacom (e.g. by using usernames like "MysticalGirl8" and non-Viacom email addresses, and by "alter[ing] its own videos to make them appear stolen.") If proven, how do these facts affect the question of whether YouTube is eligible for the 512 safe harbors?

CLASS 27: NETWORK NEUTRALITY

Network Neutrality, as of this writing, is not a viable legal doctrine. But discussing it provides a good bookend to the policy issues that have haunted us all class.

Preparation questions

(1) The FCC opinion (either the *Free Press* or the *Comcast* opinion, depending on how you abbreviate it) is not good law. The D.C. Circuit has vacated it, holding that the FCC lacks statutory authority to regulate the Internet in this fashion. The administrative law issues would take us much further into telecom law than we could possibly get in this course. The FCC has some possible countermoves if it wants to try again, and Congress could always amend the Telecommunications Act. But for the time being, treat the opinion as purely a policy question. Why did Comcast start effectively blocking BitTorrent? According to the FCC, what's wrong with it? What are the limits of the FCC's proposed nondiscrimination principle?

(2) The DoubleNet problem tries to situate the *Free Press* adjudication in the context of other proposed forms of network management. Which of them do you find worrisome on free speech or innovation grounds? Which of them do you find sensible from a bandwidth-conservation perspective? Both? Neither?

(3) A central argument in the network neutrality debates—which you can see in the faceoff between the FCC *Free Press* opinion and Commissioner McDowell's dissent—has to do with the economic incentives. What do you think of the market-discipline argument: that if Comcast customers don't like this policy, they can buy Internet service elsewhere? Would Comcast have an economic incentive to disregard customers' wishes even if they *don't* have other good alternatives for Internet service? How important is it to give Comcast incentives to upgrade its facilities and invest in next-generation network technologies? Would the FCC's network neutrality rules inhibit those incentives?

(4) The iPhone problem is designed to take the issues raised in the network neutrality debate and ask how broadly they apply. Do the justifications advanced for network neutrality regulations in the *Free Press* adjudication also apply to cellular networks? Do they also apply to the cell phones that operate on those networks? To the applications that run on those cell phones? Does Google need our protection from Apple? Does Apple need our protection from AT&T? What would "neutrality" mean in the context of an app store? Would it be a good idea? Do any of Apple's other practices raise concerns? And if so, should the FCC intervene, or is this a market it should leave alone?

In re *Formal Complaint of Free Press and Public Knowledge Against Comcast Corp. for Secretly Degrading Peer-to-Peer Applications*
23 F.C.C. Rptr. 13028 (2008)

I. INTRODUCTION

1. We consider whether Comcast, a provider of broadband Internet access over cable lines, may selectively target and interfere with connections of peer-to-peer (P2P)

applications under the facts of this case. Although Comcast asserts that its conduct is necessary to ease network congestion, we conclude that the company's discriminatory and arbitrary practice unduly squelches the dynamic benefits of an open and accessible Internet and does not constitute reasonable network management. Moreover, Comcast's failure to disclose the company's practice to its customers has compounded the harm. ...

II. BACKGROUND

3. When an Internet user opens a webpage, sends an email, or shares a document with a colleague, the user's computer usually establishes a connection with another computer (such as a server or another end user's computer) using, for example, the Transmission Control Protocol (TCP). For certain applications to work properly, that connection must be continuous and reliable. Computers linked via a TCP connection monitor that connection to ensure that packets of data sent from one user to the other over the connection "arrive in sequence and without error," at least from the perspective of the receiving computer. If either computer detects that "something seriously wrong has happened within the network," it sends a "reset packet" or "RST packet" to the other, signaling that the current connection should be terminated and a new connection established "if reliable communication is to continue."

4. BitTorrent is an open-source, peer-to-peer networking protocol that has become increasingly popular among Internet users in recent years. Unlike traditional methods of file sharing, which typically require establishing a single TCP connection between a user's computer and a single server, BitTorrent employs a decentralized distribution model: Each computer in a BitTorrent "swarm" is able to download content from the other computers in the swarm, and in turn each computer also makes available content for those same peers to download, all via TCP connections. Furthermore, a computer can download different portions of the same content from multiple computers simultaneously, with each computer providing a different portion of the same content. (For example, a computer could obtain different portions of a video file from several different other computers in the swarm.) BitTorrent thus harnesses the numerous individual Internet connections maintained by its users, rather than relying on a single, central pipeline, to distribute large files "cheaply and quickly," and the efficiency of that peer-to-peer network is dependent directly on Internet users' ability to establish TCP connections for both downloading and uploading content. Although once relegated to serving, in most cases, the savviest Internet users with unsavory or even unlawful purposes,[3] BitTorrent and other peer-to-peer technologies, such as Gnutella, have entered the mainstream. New online content distributors, such as Vuze, Inc., rely on BitTorrent to distribute video programming to millions of online viewers legally,as do several established distributors such as CBS, Twentieth Century Fox, and Sports Illustrated.

5. Peer-to-peer applications, including those relying on BitTorrent, have become a competitive threat to cable operators such as Comcast because Internet users have the opportunity to view high-quality video with BitTorrent that they might otherwise watch (and pay for) on cable television. Such video distribution poses a particular competitive threat to Comcast's video-on-demand ("VOD") service. "VOD . . . operates much like online video, where Internet users can select and download or stream any available program without a schedule and watch it any time, generally with the ability to fast-forward, rewind, or pause the programming." Comcast

[3] The infamy of the Pirate Bay — "the most notorious, most hunted digital-piracy outfit in the world" — largely stems from its assisting BitTorrent users in downloading a vast array of videos in violation of copyright laws.

has recently placed a significant emphasis on expanding its VOD business, and its VOD revenues have experienced robust growth. Moreover, Comcast has "begun incorporating its VOD content online through sites competing directly with BitTorrent protocol sites."

6. Comcast subscribers began to notice that they had problems using BitTorrent and similar technologies over their Comcast broadband connections. ...

7. The Associated Press (AP) subsequently conducted several nationwide tests to investigate the allegations that Comcast was interfering with its customers' use of peer-to-peer applications, including BitTorrent. On October 17, 2007, the AP reported the results of these tests: It concluded that Comcast "actively interferes with attempts by some of its high-speed Internet subscribers to share files online."...

8. AP also concluded that "the method used" by Comcast was "difficult to circumvent and involves [Comcast] falsifying network traffic." Specifically, "when one BitTorrent user attempts to share a complete file with another user" via a TCP connection, Comcast's servers (through which its users' packets of data must pass) send to each user's computer an RST packet "that looks like it comes from the other [user's] computer" and terminates the connection. One month after the AP's report, the Electronic Frontier Foundation (EFF) published the results of its own testing and similarly concluded that Comcast was selectively targeting customers who uploaded files using BitTorrent and other peer-to-peer protocols. Like AP, EFF also found examples where the Comcast's "packet forgery prevent[ed] the transfer of data."

9. Following these tests, Comcast changed its account and admitted that it targets peer-to-peer traffic for interference. Specifically, Comcast asserted that "when P2P unidirectional upload sessions . . . reach a predetermined congestion threshold in a particular neighborhood," Comcast's network "issues instructions called 'reset packets.'" Comcast further claimed that it sent RST packets to peer-to-peer TCP connections being used to upload content until the traffic "in the neighborhood drops below the predetermined level." In all, Comcast claimed that it sent RST packet "only during periods of peak network congestion" and "only . . . during periods of heavy network traffic." Evidence in the record, however, contradicts this claim. One Comcast customer, for example, conducted numerous tests and reported that the level of interference with his use of peer-to-peer applications was approximately equal, "regardless of the time of day or night, regardless of the day of the week, and [despite] the presumable differences in network congestion during prime time and non-prime time hours of use." No matter the time of the test, all of the customer's Gnutella upload requests were thwarted and approximately 40% of all his BitTorrent established upload connections were reset. In short, the customer concluded that for Comcast's claim of neighborhood-specific, congestion-targeted interference to be accurate, "my neighborhood would have to be under the same amount of congestion for 24 hours a day, 7 days a week, 365 days a year." Confronted with this and other evidence, Comcast changed its story yet again, and admitted that its "current P2P management is triggered . . . regardless of the level of overall network congestion at th[e] time, and regardless of the time of day."

10. On November 1, 2007, Free Press filed with the Commission a complaint against Comcast and asked the Commission to declare "that an Internet service provider violates the [Commission's] Internet Policy Statement when it intentionally degrades a targeted Internet application." ...

III. DISCUSSION

A. Our Authority to Enforce Federal Policy

[The Commission held that it had statutory authority to act.]

B. Our Approach to the Present Controversy

[The Commission decided to act via case-by-case adjudication rather than rulemaking.]

C. Resolving the Dispute

41. We now turn to whether Comcast's conduct runs afoul of federal Internet policy, and to whether we should therefore exercise our authority reviewed above to address it. The record leaves no doubt that Comcast's network management practices discriminate among applications and protocols rather than treating all equally. To reiterate: Comcast has deployed equipment across its networks that monitors its customers' TCP connections using deep packet inspection to determine how many connections are peer-to-peer uploads. When Comcast judges that there are too many peer-to-peer uploads in a given area, Comcast's equipment terminates some of those connections by sending RST packets. In other words, Comcast determines how it will route some connections based not on their destinations but on their contents; in laymen's terms, Comcast opens its customers' mail because it wants to deliver mail not based on the address or type of stamp on the envelope but on the type of letter contained therein. Furthermore, Comcast's interruption of customers' uploads by definition interferes with Internet users' downloads since "any end-point that is uploading has a corresponding end-point that is downloading." Also, because Comcast's method, sending RST packets to both sides of a TCP connection, is the same method computers connected via TCP use to communicate with each other, a customer has no way of knowing when Comcast (rather than its peer) terminates a connection.

42. This practice is not "minimally intrusive" but invasive and outright discriminatory. Comcast admits that it interferes with about ten percent of uploading peer-to-peer TCP connections, and independent evidence shows that Comcast's interference may be even more prevalent. In a test of over a thousand networks over the course of more than a million machine-hours, Vuze found that the peer-to-peer TCP connections of Comcast customers were interrupted more consistently and more persistently than those of any other provider's customers. Similarly, independent evidence suggests that Comcast may have interfered with forty if not seventy-five percent of all such connections in certain communities. Comcast also admits that even in its own tests, twenty percent of such terminated connections cannot successfully restart an uploading peer-to-peer connection within a minute. These statistics have real world consequences: We know, for example, that Comcast's conduct disconnected Adam Lynn, who uses peer-to-peer applications to watch movie trailers. We know that Comcast's conduct slowed Jeffrey Pearlman's connection "to a crawl" when he was using peer-to-peer protocols to update his copy of the World of Warcraft game. We know that David Gerisch and Dean Fox had to wait hours if not days to download open-source software over their peer-to-peer clients. And we know that Comcast's conduct entirely prevented Robert Topolski from distributing a "rare cache of Tin-Pan-Alley-era 'Wax Cylinder' recordings and other related musical memorabilia" over the Gnutella peer-to- peer network. These actual examples of interference confirm the observation that "[i]t is easy to imagine scenarios where content is unavailable for periods much longer than minutes."

43. On its face, Comcast's interference with peer-to-peer protocols appears to contravene the federal policy of "promot[ing] the continued development of the Internet" because that interference impedes consumers from "run[ning] applications . . . of their choice," rather than those favored by Comcast, and that interference limits consumers' ability "to access the lawful Internet content of their choice," including the video programming made available by vendors like Vuze. Comcast's selective interference also appears to discourage the "development of technologies" — such as peer-to- peer technologies — that "maximize user control over what information is received by individuals . . . who use the Internet" because that interference (again) impedes consumers from "run[ning] applications . . . of their choice," rather than those favored by Comcast.[4] Thus, Free Press has made a prima facie case that Comcast's practices do impede Internet content and applications, and Comcast must show that its network management practices are reasonable. ...

45. Next, Comcast asserts that even if its practice is discriminatory, it qualifies as reasonable network management.[5] However, experts in the field generally disagree strongly with Comcast's assertion that its network management practices are reasonable. The Internet Engineering Task Force, a repository for the standards and protocols that underlie the functioning of the Internet, has promulgated universal definitions for how the TCP protocol is intended to work. So far in the Internet's history, these standards have created "the equivalent of perfect competition . . . among applications and content . . . with a minimum interference by the network or platform owner." Significantly, Comcast's practices contravene those standards. Comcast's method of sending RST packets to interrupt and terminate TCP connections thus contravenes the established expectations of users and software developers for seamless and transparent communications across the Internet — this practice, known as RST Injection, "violate[s] the expectation that the contents of the envelopes are untouched inside and between Autonomous Systems" and "potentially disrupt[s] systems and applications that are designed assuming the expected behavior of the Internet." ...

47. Moreover, Comcast's practice selectively blocks and impedes the use of particular applications, and we believe that such disparate treatment poses significant risks of anticompetitive abuse. To the extent that a provider argues that such highly questionable conduct constitutes "reasonable network management," there must be a tight fit between its chosen practices and a significant goal. Accordingly, for Comcast's practice to qualify as reasonable network management, the company's justification for its practice must clear a high threshold. Its practice should further a critically important interest and be narrowly or carefully tailored to serve that interest. Comcast justifies its practice as a means of easing network congestion, and we will assume without deciding that this is a critically important interest.

48. We next must ask whether Comcast's means are carefully tailored to its interest in easing network congestion, and it is apparent that no such fit exists. As an initial matter, Comcast's practice is overinclusive for at least three independent reasons. First, it can affect customers who are using little bandwidth simply because they are using a disfavored application.

---

[4] As described in more detail above, Comcast's discriminatory network management practices also run afoul of federal policy because they reduce the rapidity and efficiency of the public Internet . . . .

[5] Free Press requests that we declare that a broadband Internet service access provider's selective interference with a particular protocol or application be a per se unreasonable network management practice. . . . Because we prefer a more nuanced approach to the issue at this time, we decline Free Press's request.

Second, it is not employed only during times of the day when congestion is prevalent: "Comcast's current P2P management is triggered . . . regardless of the level of overall network congestion at that time, and regardless of the time of day." And third, its equipment does not appear to target only those neighborhoods that have congested nodes — evidence suggests that Comcast has deployed some of its network management equipment several routers (or hops) upstream from its customers, encompassing a broader geographic and system area. With some equipment deployed over a wider geographic or system area, Comcast's technique may impact numerous nodes within its network simultaneously, regardless of whether any particular node is experiencing congestion. Furthermore, Comcast's practice suffers from the flaw of being underinclusive. A customer may use an extraordinary amount of bandwidth during periods of network congestion and will be totally unaffected so long as he does not utilize a disfavored application.

49. Moreover, Comcast has several available options it could use to manage network traffic without discriminating as it does. Comcast could cap the average users' capacity and then charge the most aggressive users overage fees.[6] Or Comcast could throttle back the connection speeds of high- capacity users (rather than any user who relies on peer-to-peer technology, no matter how infrequently). Or Comcast can work with the application vendors themselves. As Comcast has touted in this very dispute, negotiations with Pando and BitTorrent, Inc. and other peer-to-peer application companies have advanced the creation of the P4P protocol, which promises "backbone bandwidth optimization" and "improve[d] P2P download performance." Although we do not endorse any of these particular solutions today, they all appear far better tailored to Comcast's basic complaint that a "disproportionately large amount of the traffic currently on broadband networks originates from a relatively small number of users."

50. Comcast and several other commenters maintain a continual refrain that "all network providers must manage bandwidth in some manner" and that providers need "flexibility to engage in the reasonable network management practices." We do not disagree, which is precisely why we do not adopt here an inflexible framework micromanaging providers' network management practices.[7]We also note that because "consumers are entitled to access the lawful Internet content of their choice," providers, consistent with federal policy, may block transmissions of illegal content (e.g., child pornography) or transmissions that violate copyright law. To the extent, however, that providers choose to utilize practices that are not application or content neutral, the risk to the open nature of the Internet is particularly acute and the danger of network management practices being used to further anticompetitive ends is strong. As a result, it is incumbent on the Commission to be vigilant and subject such practices to a searching inquiry, and here Comcast's practice falls well short of being carefully tailored to further the interest offered by the company. ...

54. Remedy. — We finally turn to the issue of what action the Commission should take in this adjudicatory proceeding. ... Specifically, in order to allow the Commission to monitor Comcast's compliance with its pledge, the company must within 30 days of the release of this Order: (1) disclose to the Commission the precise contours of the network management practices

---

[6] We have noted that discriminatory network management is generally an unreasonable response to increased congestion . . . .

[7] Some commenters cite supposedly similar, or more restrictive, policies regarding peer-to-peer traffic of other entities, such as colleges and universities. . . . Given the case-by-case approach that we set forth in this item, we do not (and need not) opine here on other policies and practices.

at issue here, including what equipment has been utilized, when it began to be employed, when and under what circumstances it has been used, how it has been configured, what protocols have been affected, and where it has been deployed; (2) submit a compliance plan to the Commission with interim benchmarks that describes how it intends to transition from discriminatory to nondiscriminatory network management practices by the end of the year; and (3) disclose to the Commission and the public the details of the network management practices that it intends to deploy following the termination of its current practices, including the thresholds that will trigger any limits on customers' access to bandwidth. These disclosures will provide the Commission with the information necessary to ensure that Comcast lives up to the commitment it has made in this proceeding.

55. To the extent that Comcast fails to file the information required above within 30 days of the release of this Order [or fails to "follow through on its commitment to end its discriminatory network management practices by the end of the year"] three steps will occur: (1) interim injunctive relief automatically will take effect requiring Comcast to suspend the network management practices described above within 35 days of the release of this Order; (2) the Enforcement Bureau will immediately issue an order directing Comcast to show cause why a permanent cease-and-desist order should not be issued against it; and (3) a hearing will be set for thirty days after Comcast's receipt of that order. ...

Dissenting Statement of Commissioner Robert M. McDowell

...

Additionally, the majority does not address the issue of motive. The allegations before us boil down to a suspicion that Comcast was motivated not by a need to manage its network, but by a desire to discriminate against BitTorrent and similar technologies for anticompetitive reasons. If Comcast intended to harm its competitors, would it not have targeted other online video providers? Americans download more than eleven billion Internet videos per month, yet the record contains no evidence that Comcast is interfering with sites like YouTube which do not use pipe-clogging P2P software. The record also does not speak to the fact that other prominent video sites, such as Joost, use more efficient P2P software that does not cause the same congestion problems as BitTorrent. As a result of their use of software that works better on existing networks, virtually no network management is needed. The majority's silence on this key exculpatory point is deafening.

Finally, even if this case were not procedurally and legally deficient in so many regards, we must address whether the policies the majority is adopting today are in the public interest. And the answer is no. Ironically, today's action by the FCC may actually result in slower online speeds for 95 percent of America's Internet consumers. That is because, up until this point, engineers made engineering decisions, not unelected bureaucrats. Although I have a tremendous amount of respect for each of my colleagues, none of us has an engineering degree.

As a result, the practical effect of today's order requires all network operators – cable, telcos and wireless providers – to treat all Internet traffic equally. That sounds good if you say it fast. But the reality is that the Internet can function only if engineers are allowed to discriminate among different types of traffic. Now, the word "discriminate" carries with it extremely negative connotations, but to network engineers it means "network management." Discriminatory conduct, in the network management context, does not necessarily mean anticompetitive

conduct. And this is where a lot of the misunderstandings come into play. As human beings, we do not tolerate delay or interference when it comes to certain kinds of applications. For instance, we expect our online movies to be clear and not distorted by competing data coming over the same Internet connection. For us to enjoy online video without interruption or distortion, video bits have to be given priority over, say, email bits. But now that all traffic must be treated equally, that is going to change. The new regime is tantamount to a congested downtown area without stoplights. Gridlock is likely to result.

The majority is creating regulatory uncertainty for engineers. Under the new regulatory rubric of the undefined term "reasonable network management," engineers do not know if they are allowed to manage your Internet experience so you can watch online video without distortion, pops, and hisses. Similarly, they now do not know what the government will allow them to do, or not do, to manage the growing flood of peer-to-peer applications. Here's the problem: If you use cable modem or wireless broadband services, you may not know it, but you share bandwidth with your neighbor. That's just the nature of these networks, many of which were built long before P2P became popular. If your neighbor uses more bandwidth, that leaves less for you to use. This is especially true when your neighbor uses peer-to-peer applications. Many P2P applications consume as much bandwidth as they can find. In fact, only five percent of all Internet consumers are using 90 percent of the bandwidth due to P2P. Some estimate that seventy-five percent of the world's Internet traffic is P2P. As a result of increased P2P usage, many consumers' "last mile" Internet connections are getting clogged. These electronic traffic jams slow down the Internet for the vast majority of consumers who do not use P2P software to watch videos on YouTube or surf the Web. In short, this flood of data has created a tyranny by a minority. By depriving engineers of the freedom to manage these surges of information flow by having to treat all traffic equally as the result of today's order, the Information Superhighway could quickly become the Information Parking Lot. The regulatory law of unintended consequences is sure to prevail.

Network Management problem

You are Senior Counsel at DoubleNet, a major residential and commercial ISP that serves customers in twelve states. You report directly to the Vice President for Legal Affairs. You are the chief legal officer responsible for overseeing DoubleNet's operations, including intellectual property and regulatory compliance. (Your three peers are responsible, respectively, for the company's securities and corporate legal issues, for its labor and employment matters, and for its marketing and consumer relations.)

DoubleNet offers its residential customers their choice of telephone, television, and Internet service. In most of the metropolitan areas that it serves, DoubleNet reaches its customers along fiber-optic links installed in the early and mid-2000s. Unfortunately, many of its routers are a full generation behind the current state of the art, limiting the bandwidth available to DoubleNet's customers. The company about to embark on an expensive (tens of billions of dollars in capital investment) upgrade of the routers, but most of that roll-out won't be complete for 18–24 months. In the meantime, the company's engineers have become concerned by the rising intensity of bandwidth usage among its residential customers. In essence, the problem is that DoubleNet's current network can only supply the full promised bandwidth to a small number of

users at a time. As long as only a few users connected to a given router are downloading large files continually, each user experiences a fast, zippy Internet. But as more users download large files, watch videos online from sites like Hulu, engage in voice- and video-chats, and make other bandwidth-intensive uses, the overall effective bandwidth available to most users has been dropping. Meanwhile, the business side has become concerned that DoubleNet's revenue projections don't appear to be sufficient to convince shareholders of the value of spending tens of billions on greater bandwidth.

You have been summoned to a daylong strategic retreat at which various DoubleNet technical and business teams will pitch ideas for increasing value in the next few years. The following ideas are up for consideration:

- DoubleNet could switch from its current billing system ($35 to $120 a month for all-you-can-eat Internet access at various speeds) to a "metered" system in which the user pays $1 per gigabyte downloaded.

- DoubleNet could partner with a major sports cable network to offer a premium service for watching high-definition sports videos, live, at $25/month. A substantial portion of the revenues from this service would be used to deploy out special-purpose devices that provide the necessary bandwidth *solely* for the sports network's videos. The goal would be to shift many of your video-hungry customers to the sports network's programming, freeing up bandwidth for other uses.

- DoubleNet could start blocking all voice-over-IP traffic, such as Vonage, Skype, and iChat video chats.

- DoubleNet could install software on its routers to scan user communications, and automatically suspend the accounts of users who appear to be uploading copyrighted content.

- DoubleNet could institute a policy that when its routers have more traffic than they can handle, they will attempt to deliver web pages and emails first. Streaming video and peer-to-peer programs, however, will be given lower priority, which may lead them to slow down or, in times of high congestion, fail entirely.

- DoubleNet could attempt charge bandwidth-intensive web sites (such as YouTube, Hulu, and ChatRoulette) for preferential access to DoubleNet's customers. Those who paid would be given priority; those who didn't would be pushed to the end of the queue. The result is that DoubleNet's customers would see the paid-up sites as being speedier than the ones that refuse to pay.

- DoubleNet could raise its rates for Internet service by 50%.

As the head of legal affairs for operations, you will be asked for your views on the various proposals. The executives, of course, are interested in the tradeoff between reward and legal risk; they will want to know what you think of the business prospects of the proposals, as well as their likely legal implications. Prepare an opinion on the advisability of the above schemes. [You should assume, counterfactually, that the FCC *Free Press* ruling is good, binding law.]

iPhone problem

The Apple iPhone is an integrated mobile phone, portable music player, and Internet browser. It has built-in features for placing phone calls, sending and receiving SMS messages, sending and receiving email, listening to music and watching videos, and browsing the Web. One of the principal selling points of the Apple iPhone is the ability of users to download programs (called "apps") from an online App Store that add additional functionality (such as games, restaurant reviews, and thousands of other things). Developers of apps are required to submit them to Apple for approval and to agree to a confidential set of terms and conditions. If Apple approves an application for sale, it becomes available in the App Store for iPhone owners to download it and install it on their iPhones. Applications can only be installed on the iPhone by downloading them from the App Store or by a "jailbreaking" process that likely violates Section 1201 of the DMCA.

At present, in the United States, the iPhone is only available on the AT&T cellular network, owing to an exclusive contract between Apple and AT&T. An iPhone can connect to AT&T's cellular network to place calls, to AT&T's data network to access the Internet, or to a Wi-Fi hot spot to access the Internet at higher speed.

Google Voice is an online service that lets users integrate all of their phones and phone numbers. It offers its users features such as the ability to have one number ring all of their phones, automatic text transcription of voicemails, and integration of your voicemail box with your email inbox and text messages. In July 2009, the New York Times reported that Apple had rejected Google's application for a Google Voice iPhone app. The app would have offered integration with the user's iPhone contacts, outbound dialing that comes from their Google Voice phone number (rather than the iPhone's cellular number). It would have used the underlying voice and SMS connectivity of the iPhone to make all calls and send all messages.

The FCC sent letters to Apple, AT&T, and Google, asking questions about the matter. The following are taken from the companies' responses to those letters.

From Google's response:

> Apple's representatives informed Google that the Google Voice application was rejected because Apple believed the application duplicated the core dialer functionality of the iPhone. The Apple representatives indicated that the company did not want applications that could potentially replace such functionality.

From Apple's response:

> We created an approval process that reviews every application submitted to Apple for the App Store in order to protect consumer privacy, safeguard children from inappropriate content, and avoid applications that degrade the core experience of the iPhone. Some types of content such as pornography are rejected outright from the App Store, while others such as graphic combat scenes in action games may be approved but with an appropriate age rating. Most rejections are based on bugs found in the applications. When there is an issue, we try to provide the developer with helpful feedback so they can modify the application in order for us to approve it. 95% of applications are approved within 14 days of their submission. ...
>
> Contrary to published reports, Apple has not rejected the Google Voice application, and continues to study it. The application has not been approved because,

as submitted for review, it appears to alter the iPhone's distinctive user experience by replacing the iPhone's core mobile telephone functionality and Apple user interface with its own user interface for telephone calls, text messaging and voicemail. Apple spent a lot of time and effort developing this distinct and innovative way to seamlessly deliver core functionality of the iPhone. For example, on an iPhone, the "Phone" icon that is always shown at the bottom of the Home Screen launches Apple's mobile telephone application, providing access to Favorites, Recents, Contacts, a Keypad, and Visual Voicemail. The Google Voice application replaces Apple's Visual Voicemail by routing calls through a separate Google Voice telephone number that stores any voicemail, preventing voicemail from being stored on the iPhone, i.e., disabling Apple's Visual Voicemail. Similarly, SMS text messages are managed through the Google hub —replacing the iPhone's text messaging feature. In addition, the iPhone user's entire Contacts database is transferred to Google's servers, and we have yet to obtain any assurances from Google that this data will only be used in appropriate ways. These factors present several new issues and questions to us that we are still pondering at this time. ...

Apple is acting alone and has not consulted with AT&T about whether or not to approve the Google Voice application. No contractual conditions or non-contractual understandings with AT&T have been a factor in Apple's decision-making process in this matter. ...

Apple alone makes the final decisions to approve or not approve iPhone applications.

There is a provision in Apple's agreement with AT&T that obligates Apple not to include functionality in any Apple phone that enables a customer to use AT&T's cellular network service to originate or terminate a VoIP session without obtaining AT&T's permission. Apple honors this obligation, in addition to respecting AT&T's customer Terms of Service, which, for example, prohibit an AT&T customer from using AT&T's cellular service to redirect a TV signal to an iPhone. From time to time, AT&T has expressed concerns regarding network efficiency and potential network congestion associated with certain applications, and Apple takes such concerns into consideration. ...

Apple does not know if there is a VoIP element in the way the Google Voice application routes calls and messages, and whether VoIP technology is used over the 3G network by the application. Apple has approved numerous standard VoIP applications (such as Skype, Nimbuzz and iCall) for use over WiFi, but not over AT&T's 3G network. ...

The following is a list of representative applications that have been rejected as originally submitted and their current status:

- Twittelator, by Stone Design Corp., was initially rejected because it crashed during loading, but the developer subsequently fixed the application and it has been approved;

- iLoveWiFi!, by iCloseBy LLC, was rejected because it used undocumented application protocols (it has not been resubmitted as of the date of this letter);

- SlingPlayer Mobile, by Sling Media, was initially rejected because redirecting a TV signal to an iPhone using AT&T's cellular network is prohibited by AT&T's customer Terms of Service, but the developer subsequently fixed the application to use WiFi only and it has been approved; and

- Lingerie Fantasy Video (Lite), by On The Go Girls, LLC, was initially rejected because it displayed nudity and explicit sexual content, but the developer subsequently fixed the application and it has been approved with the use of a 17+ age rating.

You are on the staff of FCC Commissioner Joseph Quimby, who has asked for your opinion as to whether the FCC should restrict any of Apple's application-approval policies. [You can leave aside the question of whether the FCC has the legal authority to do so.]