CHAPTER FOURTEEN

Secondary Liability for Copyright Infringement & Safe Harbors in the Digital Age

Introduction

Generally, in the common law, "secondary liability" is imposed on someone who does not commit the legal wrong directly, but is found responsible for encouraging, facilitating or profiting from it. As you will see, the Copyright Act has no provisions imposing secondary liability. (Compare to e.g. § 271 of the Patent Act.) As a result, the secondary liability provisions of copyright law are entirely judge-developed, without even an open-ended statutory basis like that given to fair use jurisprudence under § 107.

Until recently, there were two principal forms of secondary liability: contributory infringement and vicarious liability. (It should be noted here that the *Sony v. Universal* case does not clearly delineate whether and when it is talking about contributory infringement, vicarious liability or both.)

- Contributory infringement may be found if someone, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another.
- Vicarious liability—an outgrowth of *respondeat superior*—may be imposed on someone who has the right and ability to supervise the infringing activity and also has a direct financial interest in the activity.

In both cases, there needs to be underlying *direct* infringement. In other words, someone needs directly to violate the exclusive rights provided by § 106, before contributory or vicarious liability can be imposed on any third party.

Sony Corp. of America v. Universal City Studios, Inc.

464 U.S. 417 (1984)

Re-read sections I, II and III of the *Sony* opinion from Chapter 13, page 425.

PROBLEM 14-1
THE *NAPSTER* CASE.

This problem is designed to be used as either a free-standing hypothetical or as part of a video argument exercise. In the latter incarnation, a video we have edited, showing the *Napster* oral argument in the Ninth Circuit, is played in class. The video is available at http://youtu.be/5ftJ1pFLGQk. Students are placed in role as the lawyers in the case. The video is repeatedly paused throughout its length and the class as a whole is required to brainstorm about how to open their arguments, respond to

particular judges' questions and so on. Then the video is allowed to run and the class can compare its answers to those of the lawyers and the court—for good or ill.

Using the material we have read so far, particularly focusing on the *Sony* case, and the explanation of contributory and vicarious infringement above, please read the facts below and explain how you would argue that Napster is, or is not, infringing copyright law. For the purposes of this exercise, students do not need to read the *Napster* opinion. Indeed the exercise works much better (and is more enjoyable for all concerned) when they do not do so.

> [Excerpted statement of the facts] 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. Napster provides technical support for the indexing and searching of MP3 files, as well as for its other functions, including a "chat room," where users can meet to discuss music, and a directory where participating artists can provide information about their music.
>
> **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. . . .

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). See generally *Brookfield Communications, Inc. v. West Coast Entm't Corp.* (9th Cir. 1999) (describing, in detail, the structure of the Internet). 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."

[T]he 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. . . ."†

What would you need to prove in order to find liability? What would be the defenses? How would you frame your argument? What would be your opening 60 seconds if you were the lawyer arguing either for the plaintiff or the defendant? [These are the crucial moments when you have a chance to frame the issue before the judges interrupt. If you are lucky.] Which, if any, of the frames discussed in Chapter 1 could each side use? On what precedents would you rely? What policy arguments would you stress? What "escape hatches" would you offer to a court contemplating the possibility that Napster might not be liable? What vision of doom would you conjure up were the court not to find Napster liable?

1.) The Stakes of Contributory Infringement

As *Tiffany v. eBay* showed in the trademark context, contributory infringement assumes particular importance in the world of the internet. Or perhaps, more broadly, in the world of devices and networks which give powers to individuals that were formerly held—to any significant extent—exclusively by large commercial intermediaries. The internet allows any individual to set up a global storefront. Your laptop or tablet or phone can implicate many of the rights in § 106 of the Copyright Act—a dramatic technologically enabled change to the legal significance of your actions. You can copy, distribute, and modify existing works—indeed on a daily basis, you would be hard put not to. At the same time, these devices and networks also allow an unprecedented flowering of creativity, innovation and disruptive business models. From Amazon and eBay to blogs, Wikipedia,

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

open source software and the world of social media, the devices and networks of the digital era demonstrate a broad decentralization of creative tools and a "disintermediation" of previous business models and forms of social organization. ("Disintermediation" is an ugly, but useful, word meaning that it is possible to cut out the middle man—to go directly from musician or artist or technologist to the public or to the market.)

In this world, secondary liability will be crucial. For rights-holders, secondary liability will hold out the promise of being able to restrain the actions of swarms of anonymous infringers. If you can shut down the platform, the network or the technology—or bring it under your control financially or technologically—then you can strike at the root of infringement, rather than having to deal with a million individual instances. (Compare the arguments made by the trademark owner in a case such as *Tiffany* to the arguments made by copyright holders in the situation of a peer-to-peer network such as Napster.)

For technologists, many of whom will also be rights holders, the stakes are equally high. It is easy convincingly to portray *any* digital product or service in such a way as a.) to highlight its potential for massive infringement, b.) to point out that the developers of the technology or service "must have known of" this potential for infringement and c.) to show that the developers of the technology are profiting from demand that is *in part* fuelled by the potential for infringing uses. What would the demand be for an iPod that could only be filled with legally purchased music (for example by requiring DRM authentication that the music had been licitly purchased)? Do you think that Dropbox (or any cyberlocker) is popular among some users because it can be used to illicitly share copyrighted material? YouTube?

As you read the cases that follow try to be attentive both to the concerns of copyright holders and those of the technology developers. From the point of view of the copyright holder, consider the sheer scale and magnitude of the infringement. Surely this demands immediate and extensive intervention—particularly given the fact that the technology developers know that their products will be used to infringe and actually profit from it? From the perspective of the technology developer, do not assess the effect of the rules on technologies *ex post*—whether you think you could persuade a Federal District Court judge *today* that her existing iPod is illegal. Rather, consider the rule *ex ante*. Imagine yourself the lawyer in charge of vetting product development at a technology company *before* these products have been brought to market, widely used and accepted. The engineer comes and lays out the product or the service. "This will put 20,000 songs in your pocket!" "This search engine will allow users to search for and go directly to any content anywhere on the internet!" "This cyberlocker will allow anyone to exchange files of any size with anyone else in the world!"

Can you come up with a rule that protects the copyright holders without causing you—as a properly cautious lawyer vetting product development—to forbid *ex ante* the development of the iPod, Google, Dropbox and YouTube in the forms that we currently know? Or do you think that the correct answer would have been to impose secondary liability and veto all the technologies that could not internalize the costs of infringement? This chapter is about the attempt to answer these questions.

2.) Contributory and Vicarious Infringement

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

BEEZER, Circuit Judge.
[In order to hold Napster liable for contributory or vicarious infringement, it is necessary for a court to find that there has been underlying direct infringement by Napster *users*.]
. . .

Plaintiffs claim Napster users are engaged in the wholesale reproduction and distribution of copyrighted works, all constituting direct infringement. The district court agreed. . . .

A. Infringement

. . . [P]laintiffs have shown that Napster users infringe at least two of the copyright holders' exclusive rights: the rights of reproduction, § 106(1); and distribution, § 106(3). Napster users who upload file names to the search index for others to copy violate plaintiffs' distribution rights. Napster users who download files containing copyrighted music violate plaintiffs' reproduction rights.

Napster asserts an affirmative defense to the charge that its users directly infringe plaintiffs' copyrighted musical compositions and sound recordings.

B. Fair Use

Napster contends that its users do not directly infringe plaintiffs' copyrights because the users are engaged in fair use of the material. 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 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.* (1994).

The district court first concluded that downloading MP3 files does not transform the copyrighted work. This conclusion is supportable. Courts have been reluctant to find fair use when an original work is merely retransmitted in a different medium.

This "purpose and character" element also requires the district court to determine whether the allegedly infringing use is commercial or noncommercial. A commercial use weighs against a finding of fair use but is not conclusive on the issue. 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." The district court's findings are not clearly erroneous.

Direct economic benefit is not required to demonstrate a commercial use. Rather, repeated and exploitative copying of copyrighted works, even if the copies are not

offered for sale, may constitute a commercial use. In the record before us, commercial use is demonstrated by a showing that repeated and exploitative unauthorized copies of copyrighted works were made to save the expense of purchasing authorized copies. . . .

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." 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." We agree. We note, however, that under certain circumstances, a court will conclude that a use is fair even when the protected work is copied in its entirety. *See, e.g., Sony Corp. v. Universal City Studios, Inc.*

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." *Harper & Row Publishers, Inc. v. Nation Enters.* (1985). "[T]he 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." *Campbell*. The proof required to demonstrate present or future market harm varies with the purpose and character of the use:

> A challenge to a noncommercial use of a copyrighted work requires proof either that the particular use is harmful, or that if it should become widespread, it would adversely affect the potential market for the copyrighted work. . . . *If the intended use is for commercial gain, that likelihood [of market harm] may be presumed. But if it is for a noncommercial purpose, the likelihood must be demonstrated. Sony*.

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." . . . Defendant has failed to show any basis for disturbing the district court's findings. . . .

Judge Patel did not abuse her discretion in reaching the above fair use conclusions, nor were the findings of fact with respect to fair use considerations clearly erroneous. We next address Napster's identified uses of sampling and space-shifting.

5. Identified Uses

Napster maintains that its identified uses of sampling and space-shifting were wrongly excluded as fair uses by the district court. . . . 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.* (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* (holding that "time-shifting," where a video tape recorder owner records a television show for later viewing, is a fair use).

We conclude that the district court did not err when it refused to apply the "shifting" analyses of *Sony* and *Diamond*. 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." 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.

c. Other Uses

Permissive reproduction by either independent or established artists is the final fair use claim made by Napster. The district court noted that plaintiffs did not seek to enjoin this and any other noninfringing use of the Napster system, including: chat rooms, message boards and Napster's New Artist Program. Plaintiffs do not challenge these uses on appeal.

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. Accordingly, we next address whether Napster is secondarily liable for the direct infringement under two doctrines of copyright law: contributory copyright infringement and vicarious copyright infringement.

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.* (2d Cir. 1971).

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.* (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." 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."

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. *See* [*Sony*] (rejecting argument that merely supplying the "'means' to accomplish an infringing activity" leads to imposition of liability). We depart from the reasoning of the district court that Napster failed to demonstrate that its system is capable of commercially significant noninfringing uses. The district court improperly confined the use analysis to current uses, ignoring the system's capabilities. *See generally Sony* (framing inquiry as whether the video tape recorder is "*capable* of commercially significant noninfringing uses"). Consequently, the district court placed undue weight on the proportion of current infringing use as compared to current and future noninfringing use. Nonetheless, whether we might arrive at a different result is not the issue here. The instant appeal occurs at an early point in the proceedings and "the fully developed factual record may be materially different from that initially before the district court. . . ." 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. . . .

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. 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. 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, Inc. v. Cherry Auction, Inc.* (9th Cir. 1996), 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." We agree that Napster provides "the site and facilities" for direct infringement. The district court correctly applied the reasoning in *Fonovisa*, and properly found that Napster materially contributes to direct infringement.

We affirm the district court's conclusion that plaintiffs have demonstrated a likelihood of success on the merits of the contributory copyright infringement claim. We will address the scope of the injunction in part VIII of this opinion.

V

We turn to the question whether Napster engages in vicarious copyright infringement. Vicarious copyright liability is an "outgrowth" of respondeat superior. *Fonovisa*. 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."

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. *See generally* 3 NIMMER ON COPYRIGHT §§ 12.04[A][2] & [A][2][b] (2000) (confining *Sony* to contributory infringement analysis: "Contributory infringement itself is of two types — personal conduct that forms part of or furthers the infringement and contribution of machinery or goods that provide the means to infringe.") The issues of *Sony*'s liability under the "doctrines of 'direct infringement' and 'vicarious liability'" were not before the Supreme Court, although the Court recognized that the "lines between direct infringement, contributory infringement, and vicarious liability are not clearly drawn." Consequently, when the *Sony* Court used the term "vicarious liability," it did so broadly and outside of a technical analysis of the doctrine of vicarious copyright infringement. ("[V]icarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another.")

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. We agree. Financial benefit exists where the availability of infringing material "acts as a 'draw' for customers." *Fonovisa*. 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." 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. 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. 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.

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. 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. We address the scope of the injunction in part VIII of this opinion. . . .

VIII

The district court correctly recognized that a preliminary injunction against Napster's participation in copyright infringement is not only warranted but required. We believe, however, that the scope of the injunction needs modification in light of our opinion. Specifically, we reiterate that contributory liability may potentially be imposed only to the extent that Napster: (1) receives reasonable knowledge of specific infringing files with copyrighted musical compositions and sound recordings; (2) knows or should know that such files are available on the Napster system; and (3) fails to act to prevent viral distribution of the works. The mere existence of the Napster system, absent actual notice and Napster's demonstrated failure to remove the offending material, is insufficient to impose contributory liability.

Conversely, Napster may be vicariously liable when it fails to affirmatively use its ability to patrol its system and preclude access to potentially infringing files listed in its search index. Napster has both the ability to use its search function to identify infringing musical recordings and the right to bar participation of users who engage in the transmission of infringing files.

The preliminary injunction which we stayed is overbroad because it places on Napster the entire burden of ensuring that no "copying, downloading, uploading, transmitting, or distributing" of plaintiffs' works occur on the system. As stated, we place the burden on plaintiffs to provide notice to Napster of copyrighted works and files containing such works available on the Napster system before Napster has the duty to disable access to the offending content. Napster, however, also bears the burden of policing the system within the limits of the system. Here, we recognize that this is not an exact science in that the files are user named. In crafting the injunction on remand, the district court should recognize that Napster's system does not currently appear to allow Napster access to users' MP3 files.

Based on our decision to remand, Napster's additional arguments on appeal going to the scope of the injunction need not be addressed. We, however, briefly address Napster's First Amendment argument so that it is not reasserted on remand. Napster contends that the present injunction violates the First Amendment because it is broader

than necessary. The company asserts two distinct free speech rights: (1) its right to publish a "directory" (here, the search index) and (2) its users' right to exchange information. We note that First Amendment concerns in copyright are allayed by the presence of the fair use doctrine. There was a preliminary determination here that Napster users are not fair users. Uses of copyrighted material that are not fair uses are rightfully enjoined. . . .

Questions:

1.) You had a chance to do Problem 14-1 and perhaps to see the video of the argument. How closely did the court decision mirror either your proposed framing of the issues or the way you thought the decision was going to come out? To what extent did the court attempt to *respond* to some of those proposed framings?

2.) "Get[ting] for free something they would ordinarily have to buy. . . ." The court finds that "commercial use is demonstrated by a showing that repeated and exploitative unauthorized copies of copyrighted works were made to save the expense of purchasing authorized copies." Do you agree with this definition of "commercial use"? *Harper & Row* offered a similar definition. Why does the court adopt it here? In *Harper*, after all, one commercial publisher was portrayed as scooping another commercial publisher. Here we have legions of private individuals "sharing" files for free. What is it about the disaggregated mass of millions of individuals that causes the court to label their collective, albeit uncompensated, efforts "commercial"?

3.) What would happen if the court held that this was *not* commercial? What would the record companies have to prove?

4.) Is the court correct in its characterization of the *Sony* opinion? Was *Sony* only a case about what knowledge could be attributed to the defendants, merely because of the capabilities of their technology, in the absence of more concrete information?

5.) *Napster* suggests that "*Sony*'s 'staple article of commerce' analysis has no application to Napster's potential liability for *vicarious* copyright infringement." Do you agree? Did the *Sony* court confine itself to contributory infringement, when it said that liability could not be imposed if the product was capable of substantial non-infringing uses? Which answer makes sense from the point of view of copyright policy?

6.) What burdens does the court impose on Napster to filter, block and monitor content on its system?

7.) Section 2, above, discusses the "stakes" of secondary liability. Does the line the court draws here manage to thread the needle between the concerns of the copyright holders and the technologists? Why? Why not?

3.) Inducement Liability

We said at the beginning of this chapter that contributory infringement and vicarious liability were, until recently, the only two forms of secondary liability for copyright infringement. But then came *MGM v. Grokster*.

MGM 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 by third parties.

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.

Grokster's eponymous software employs what is known as FastTrack technology, a protocol developed by others and licensed to Grokster. StreamCast distributes a very similar product except that its software, called Morpheus, relies on what is known as Gnutella technology. A user who downloads and installs either software possesses the protocol to send requests for files directly to the computers of others using software compatible with FastTrack or Gnutella. On the FastTrack network opened by the Grokster software, the user's request goes to a computer given an indexing capacity by the software and designated a supernode, or to some other computer with comparable power and capacity to collect temporary indexes of the files available on the computers of users connected to it. The supernode (or indexing computer) searches its own index and may communicate the search request to other supernodes. If the file is found, the supernode discloses its location to the computer requesting it, and the requesting user can download the file directly from the computer located. The copied file is placed in a designated sharing folder on the requesting user's computer, where it is available for other users to download in turn, along with any other file in that folder.

In the Gnutella network made available by Morpheus, the process is mostly the same, except that in some versions of the Gnutella protocol there are no supernodes. In these versions, 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.

Grokster and StreamCast concede the infringement in most downloads, and it is uncontested that they are aware that users employ their software primarily to download copyrighted files, even if the decentralized FastTrack and Gnutella networks fail to reveal which files are being copied, and when. From time to time, moreover, the companies have learned about their users' infringement directly, as from users who have sent e-mail to each company with questions about playing copyrighted movies they had downloaded, to whom the companies have responded with guidance. And MGM notified the companies of 8 million copyrighted files that could be obtained using their software.

Grokster and StreamCast are not, however, merely passive recipients of information about infringing use. The record is replete with evidence that from the moment Grokster and StreamCast began to distribute their free software, each one clearly voiced the objective that recipients use it to download copyrighted works, and each took active steps to encourage infringement.

After the notorious file-sharing service, Napster, was sued by copyright holders for facilitation of copyright infringement, StreamCast gave away a software program of a kind known as OpenNap, designed as compatible with the Napster program and open to Napster users for downloading files from other Napster and OpenNap users' computers. Evidence indicates that "[i]t was always [StreamCast's] intent to use [its

OpenNap network] to be able to capture email addresses of [its] initial target market so that [it] could promote [its] StreamCast Morpheus interface to them," indeed, the OpenNap program was engineered "'to leverage Napster's 50 million user base.'"

. . . Internal company documents indicate that StreamCast hoped to attract large numbers of former Napster users if that company was shut down by court order or otherwise, and that StreamCast planned to be the next Napster. A kit developed by StreamCast to be delivered to advertisers, for example, contained press articles about StreamCast's potential to capture former Napster users, and it introduced itself to some potential advertisers as a company "which is similar to what Napster was." It broadcast banner advertisements to users of other Napster-compatible software, urging them to adopt its OpenNap. An internal e-mail from a company executive stated: "'We have put this network in place so that when Napster pulls the plug on their free service . . . or if the Court orders them shut down prior to that . . . we will be positioned to capture the flood of their 32 million users that will be actively looking for an alternative.'"

Thus, StreamCast developed promotional materials to market its service as the best Napster alternative. One proposed advertisement read: "Napster Inc. has announced that it will soon begin charging you a fee. That's if the courts don't order it shut down first. What will you do to get around it?" Another proposed ad touted StreamCast's software as the "# 1 alternative to Napster" and asked "[w]hen the lights went off at Napster . . . where did the users go?" StreamCast even planned to flaunt the illegal uses of its software; when it launched the OpenNap network, the chief technology officer of the company averred that "[t]he goal is to get in trouble with the law and get sued. It's the best way to get in the new[s]."

The evidence that Grokster sought to capture the market of former Napster users is sparser but revealing, for Grokster launched its own OpenNap system called Swaptor and inserted digital codes into its Web site so that computer users using Web search engines to look for "Napster" or "[f]ree filesharing" would be directed to the Grokster Web site, where they could download the Grokster software. And Grokster's name is an apparent derivative of Napster.

StreamCast's executives monitored the number of songs by certain commercial artists available on their networks, and an internal communication indicates they aimed to have a larger number of copyrighted songs available on their networks than other file-sharing networks. The point, of course, would be to attract users of a mind to infringe, just as it would be with their promotional materials developed showing copyrighted songs as examples of the kinds of files available through Morpheus. Morpheus in fact allowed users to search specifically for "Top 40" songs, which were inevitably copyrighted.

In addition to this evidence of express promotion, marketing, and intent to promote further, the business models employed by Grokster and StreamCast confirm that their principal object was use of their software to download copyrighted works. Grokster and StreamCast receive no revenue from users, who obtain the software itself for nothing. Instead, both companies generate income by selling advertising space, and they stream the advertising to Grokster and Morpheus users while they are employing the programs. As the number of users of each program increases, advertising opportunities become worth more. While there is doubtless some demand for free Shakespeare, the evidence shows that substantive volume is a function of free access to copyrighted work. Users seeking Top 40 songs, for example, or the latest release by Modest Mouse, are certain to be far more numerous than those seeking a free Decameron, and Grokster and StreamCast translated that demand into dollars.

Finally, there is no evidence that either company made an effort to filter copyrighted

material from users' downloads or otherwise impede the sharing of copyrighted files. Although Grokster appears to have sent e-mails warning users about infringing content when it received threatening notice from the copyright holders, it never blocked anyone from continuing to use its software to share copyrighted files. StreamCast not only rejected another company's offer of help to monitor infringement, but blocked the Internet Protocol addresses of entities it believed were trying to engage in such monitoring on its networks.

B

. . . The District Court limited its consideration to the asserted liability of Grokster and StreamCast for distributing the current versions of their software, leaving aside whether either was liable "for damages arising from past versions of their software, or from other past activities." The District Court held that those who used the Grokster and Morpheus software to download copyrighted media files directly infringed MGM's copyrights, a conclusion not contested on appeal, but the court nonetheless granted summary judgment in favor of Grokster and StreamCast as to any liability arising from distribution of the then current versions of their software. Distributing that software gave rise to no liability in the court's view, because its use did not provide the distributors with actual knowledge of specific acts of infringement.

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.* (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 court also held that Grokster and StreamCast did not materially contribute to their users' infringement because it was the users themselves who searched for, retrieved, and stored the infringing files, with no involvement by the defendants beyond providing the software in the first place.

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

A

MGM and many of the amici fault the Court of Appeals's holding for upsetting a sound balance between the respective values of supporting creative pursuits through copyright protection and promoting innovation in new communication technologies by limiting the incidence of liability for copyright infringement. The more artistic protection is favored, the more technological innovation may be discouraged; the administration of copyright law is an exercise in managing the trade-off.

The tension between the two values is the subject of this case, with its claim that digital distribution of copyrighted material threatens copyright holders as never before, because every copy is identical to the original, copying is easy, and many people (especially the young) use file-sharing software to download copyrighted works. This

very breadth of the software's use may well draw the public directly into the debate over copyright policy, and the indications are that the ease of copying songs or movies using software like Grokster's and Napster's is fostering disdain for copyright protection. As the case has been presented to us, these fears are said to be offset by the different concern that imposing liability, not only on infringers but on distributors of software based on its potential for unlawful use, could limit further development of beneficial technologies.[8]

The argument for imposing indirect liability in this case is, however, a powerful one, given the number of infringing downloads that occur every day using StreamCast's and Grokster's software. When a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement.

One infringes contributorily by intentionally inducing or encouraging direct infringement, and infringes vicariously by profiting from direct infringement while declining to exercise a right to stop or limit it.[9] Although "[t]he Copyright Act does not expressly render anyone liable for infringement committed by another," *Sony Corp. v. Universal City Studios*, these doctrines of secondary liability emerged from common law principles and are well established in the law.

B

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*, 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. Copyright holders sued *Sony* as the manufacturer, claiming it was contributorily liable for infringement that occurred when VCR owners taped copyrighted programs because it supplied the means used to infringe, and it had constructive knowledge that infringement would occur. At the trial on the merits, the evidence showed that the principal use of the VCR was for "'time-shifting,'" or taping a program for later viewing at a more convenient time, which the Court found to be a fair, not an infringing, use. There was no evidence that *Sony* had expressed an object of bringing about taping in violation of copyright or had taken active steps to increase its profits from unlawful taping. Although *Sony*'s advertisements urged consumers to buy the VCR to "'record favorite shows'" or "'build a library'" of recorded programs, *Sony* (Blackmun, J., dissenting), neither of these uses was necessarily infringing.

---

[8] The mutual exclusivity of these values should not be overstated, however. On the one hand technological innovators, including those writing file-sharing computer programs, may wish for effective copyright protections for their work. On the other hand the widespread distribution of creative works through improved technologies may enable the synthesis of new works or generate audiences for emerging artists.

[9] We stated in *Sony Corp. of America v. Universal City Studios, Inc.* (1984), that "'the lines between direct infringement, contributory infringement and vicarious liability are not clearly drawn'. . . . [R]easoned analysis of [the *Sony* plaintiffs' contributory infringement claim] necessarily entails consideration of arguments and case law which may also be forwarded under the other labels, and indeed the parties . . . rely upon such arguments and authority in support of their respective positions on the issue of contributory infringement." In the present case MGM has argued a vicarious liability theory, which allows imposition of liability when the defendant profits directly from the infringement and has a right and ability to supervise the direct infringer, even if the defendant initially lacks knowledge of the infringement. Because we resolve the case based on an inducement theory, there is no need to analyze separately MGM's vicarious liability theory.

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." 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.

We agree with MGM that the Court of Appeals misapplied *Sony*, which it read as limiting secondary liability quite beyond the circumstances to which the case applied. *Sony* barred secondary liability based on presuming or imputing intent to cause infringement solely from the design or distribution of a product capable of substantial lawful use, which the distributor knows is in fact used for infringement. The Ninth Circuit has read *Sony*'s limitation to mean that whenever a product is capable of substantial lawful use, the producer can never be held contributorily liable for third parties' infringing use of it; it read the rule as being this broad, even when an actual purpose to cause infringing use is shown by evidence independent of design and distribution of the product, unless the distributors had "specific knowledge of infringement at a time at which they contributed to the infringement, and failed to act upon that information." Because the Circuit found the StreamCast and Grokster software capable of substantial lawful use, it concluded on the basis of its reading of *Sony* that neither company could be held liable, since there was no showing that their software, being without any central server, afforded them knowledge of specific unlawful uses.

This view of *Sony*, however, was error, converting the case from one about liability resting on imputed intent to one about liability on any theory. 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. ("If vicarious liability is to be imposed on *Sony* in this case, it must rest on the fact that it has sold equipment with constructive knowledge" of the potential for infringement). 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.

The classic case of direct evidence of unlawful purpose occurs when one induces commission of infringement by another, or "entic[es] or persuad[es] another" to infringe, Black's Law Dictionary 790 (8th ed. 2004), as by advertising. Thus at common law a copyright or patent defendant who "not only expected but invoked [infringing use] by advertisement" was liable for infringement "on principles recognized in every part of the law." *Kalem Co. v. Harper Brothers* (copyright infringement).

The rule on inducement of infringement as developed in the early cases is no different today.[11] Evidence of "active steps . . . taken to encourage direct infringement," such as advertising an infringing use or instructing how to engage in an infringing use, show an affirmative intent that the product be used to infringe, and a showing that infringement was encouraged overcomes the law's reluctance to find liability when a defendant merely sells a commercial product suitable for some lawful use, see, e.g., *Water Technologies Corp. v. Calco, Ltd.* (Fed. Cir. 1988) (liability for inducement where one "actively and knowingly aid[s] and abet[s] another's direct infringement" (emphasis omitted)); *Fromberg, Inc. v. Thornhill* (5th Cir. 1963) (demonstrations by sales staff of infringing uses supported liability for inducement); *Haworth Inc. v. Herman Miller Inc.* (W.D.Mich. 1994) (evidence that defendant "demonstrate[d] and recommend[ed] infringing configurations" of its product could support inducement liability); *Sims v. Mack Trucks, Inc.* (E.D.Pa. 1978) (finding inducement where the use "depicted by the defendant in its promotional film and brochures infringes the . . . patent"), overruled on other grounds, 608 F.2d 87 (3d Cir. 1979).

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.

[11] Inducement has been codified in patent law.

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.[12]

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.

It is so ordered.

---

[12] Of course, in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses. Such a holding would tread too close to the *Sony* safe harbor.

Justice GINSBURG, with whom THE CHIEF JUSTICE and Justice KENNEDY join, concurring.

I concur in the Court's decision . . . and write separately to clarify why I conclude that the Court of Appeals misperceived, and hence misapplied, our holding in *Sony Corp. of America v. Universal City Studios, Inc.* (1984). There is here at least a "genuine issue as to [a] material fact," Fed. Rule Civ. Proc. 56(c), on the liability of Grokster or StreamCast, not only for actively inducing copyright infringement, but also or alternatively, based on the distribution of their software products, for contributory copyright infringement. On neither score was summary judgment for Grokster and StreamCast warranted. . . .

This case differs markedly from *Sony*. Here, there has been no finding of any fair use and little beyond anecdotal evidence of noninfringing uses. In finding the Grokster and StreamCast software products capable of substantial noninfringing uses, the District Court and the Court of Appeals appear to have relied largely on declarations submitted by the defendants. These declarations include assertions (some of them hearsay) that a number of copyright owners authorize distribution of their works on the Internet and that some public domain material is available through peer-to-peer networks including those accessed through Grokster's and StreamCast's software. . . .[3]

Even if the absolute number of noninfringing files copied using the Grokster and StreamCast software is large, it does not follow that the products are therefore put to substantial noninfringing uses and are thus immune from liability. The number of noninfringing copies may be reflective of, and dwarfed by, the huge total volume of files shared. In sum, when the record in this case was developed, there was evidence that Grokster's and StreamCast's products were, and had been for some time, overwhelmingly used to infringe, and that this infringement was the overwhelming source of revenue from the products. Fairly appraised, the evidence was insufficient to demonstrate, beyond genuine debate, a reasonable prospect that substantial or commercially significant noninfringing uses were likely to develop over time. On this record, the District Court should not have ruled dispositively on the contributory infringement charge by granting summary judgment to Grokster and StreamCast.

If, on remand, the case is not resolved on summary judgment in favor of MGM based on Grokster and StreamCast actively inducing infringement, the Court of Appeals, I would emphasize, should reconsider, on a fuller record, its interpretation of *Sony*'s product distribution holding.

Justice BREYER, with whom Justice STEVENS and Justice O'CONNOR join, concurring.

---

[3] Justice Breyer finds support for summary judgment in this motley collection of declarations and in a survey conducted by an expert retained by MGM. That survey identified 75% of the files available through Grokster as copyrighted works owned or controlled by the plaintiffs, and 15% of the files as works likely copyrighted. As to the remaining 10% of the files, "there was not enough information to form reasonable conclusions either as to what those files even consisted of, and/or whether they were infringing or non-infringing." Even assuming, as Justice Breyer does, that the *Sony* Court would have absolved *Sony* of contributory liability solely on the basis of the use of the Betamax for authorized time-shifting, summary judgment is not inevitably appropriate here. *Sony* stressed that the plaintiffs there owned "well below 10%" of copyrighted television programming, [*Sony*], and found, based on trial testimony from representatives of the four major sports leagues and other individuals authorized to consent to home recording of their copyrighted broadcasts, that a similar percentage of program copying was authorized. Here, the plaintiffs allegedly control copyrights for 70% or 75% of the material exchanged through the Grokster and StreamCast software, and the District Court does not appear to have relied on comparable testimony about authorized copying from copyright holders.

I agree with the Court that the distributor of a dual-use technology may be liable for the infringing activities of third parties where he or she actively seeks to advance the infringement. I further agree that, in light of our holding today, we need not now "revisit" *Sony*. Other Members of the Court, however, take up the *Sony* question: whether Grokster's product is "capable of 'substantial' or 'commercially significant' noninfringing uses." And they answer that question by stating that the Court of Appeals was wrong when it granted summary judgment on the issue in Grokster's favor. I write to explain why I disagree with them on this matter. . . .

The Court's opinion in *Sony* and the record evidence (as described and analyzed in the many briefs before us) together convince me that the Court of Appeals' conclusion has adequate legal support. . . .

When measured against *Sony*'s underlying evidence and analysis, the evidence now before us shows that Grokster passes *Sony*'s test—that is, whether the company's product is capable of substantial or commercially significant noninfringing uses. For one thing, petitioners' (hereinafter MGM) own expert declared that 75% of current files available on Grokster are infringing and 15% are "likely infringing." That leaves some number of files near 10% that apparently are noninfringing, a figure very similar to the 9% or so of authorized time-shifting uses of the VCR that the Court faced in *Sony*. . . .

Importantly, *Sony* also used the word "capable," asking whether the product is "capable of" substantial noninfringing uses. Its language and analysis suggest that a figure like 10%, if fixed for all time, might well prove insufficient, but that such a figure serves as an adequate foundation where there is a reasonable prospect of expanded legitimate uses over time. [*Sony*] (noting a "significant potential for future authorized copying"). And its language also indicates the appropriateness of looking to potential future uses of the product to determine its "capability."

Here the record reveals a significant future market for noninfringing uses of Grokster-type peer-to-peer software. Such software permits the exchange of any sort of digital file—whether that file does, or does not, contain copyrighted material. As more and more uncopyrighted information is stored in swappable form, it seems a likely inference that lawful peer-to-peer sharing will become increasingly prevalent.

And that is just what is happening. Such legitimate noninfringing uses are coming to include the swapping of: research information (the initial purpose of many peer-to-peer networks); public domain films (e.g., those owned by the Prelinger Archive); historical recordings and digital educational materials (e.g., those stored on the Internet Archive); digital photos (OurPictures, for example, is starting a P2P photo-swapping service); "shareware" and "freeware" (e.g., Linux and certain Windows software); secure licensed music and movie files (Intent MediaWorks, for example, protects licensed content sent across P2P networks); news broadcasts past and present (the BBC Creative Archive lets users "rip, mix and share the BBC"); user-created audio and video files (including "podcasts" that may be distributed through P2P software); *and all manner of free "open content" works collected by Creative Commons* (one can search for Creative Commons material on StreamCast). I can find nothing in the record that suggests that this course of events will not continue to flow naturally as a consequence of the character of the software taken together with the foreseeable development of the Internet and of information technology. . . .

As I have said, *Sony* itself sought to "strike a balance between a copyright holder's legitimate demand for effective—not merely symbolic—protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce." Thus, to determine whether modification, or a strict interpretation, of *Sony*

is needed, I would ask whether MGM has shown that *Sony* incorrectly balanced copyright and new-technology interests. In particular: (1) Has *Sony* (as I interpret it) worked to protect new technology? (2) If so, would modification or strict interpretation significantly weaken that protection? (3) If so, would new or necessary copyright-related benefits outweigh any such weakening?

A

The first question is the easiest to answer. *Sony*'s rule, as I interpret it, has provided entrepreneurs with needed assurance that they will be shielded from copyright liability as they bring valuable new technologies to market.

Sony's rule is clear. That clarity allows those who develop new products that are capable of substantial noninfringing uses to know, ex ante, that distribution of their product will not yield massive monetary liability. At the same time, it helps deter them from distributing products that have no other real function than—or that are specifically intended for—copyright infringement, deterrence that the Court's holding today reinforces (by adding a weapon to the copyright holder's legal arsenal).

Sony's rule is strongly technology protecting. The rule deliberately makes it difficult for courts to find secondary liability where new technology is at issue. It establishes that the law will not impose copyright liability upon the distributors of dual-use technologies (who do not themselves engage in unauthorized copying) unless the product in question will be used almost exclusively to infringe copyrights (or unless they actively induce infringements as we today describe). *Sony* thereby recognizes that the copyright laws are not intended to discourage or to control the emergence of new technologies, including (perhaps especially) those that help disseminate information and ideas more broadly or more efficiently. Thus *Sony*'s rule shelters VCRs, typewriters, tape recorders, photocopiers, computers, cassette players, compact disc burners, digital video recorders, MP3 players, Internet search engines, and peer-to-peer software. But *Sony*'s rule does not shelter descramblers, even if one could theoretically use a descrambler in a noninfringing way.

Sony's rule is forward looking. It does not confine its scope to a static snapshot of a product's current uses (thereby threatening technologies that have undeveloped future markets). Rather, as the VCR example makes clear, a product's market can evolve dramatically over time. And *Sony*—by referring to a capacity for substantial noninfringing uses—recognizes that fact. *Sony*'s word "capable" refers to a plausible, not simply a theoretical, likelihood that such uses will come to pass, and that fact anchors *Sony* in practical reality.

Sony's rule is mindful of the limitations facing judges where matters of technology are concerned. Judges have no specialized technical ability to answer questions about present or future technological feasibility or commercial viability where technology professionals, engineers, and venture capitalists themselves may radically disagree and where answers may differ depending upon whether one focuses upon the time of product development or the time of distribution.

Given the nature of the *Sony* rule, it is not surprising that in the last 20 years, there have been relatively few contributory infringement suits—based on a product distribution theory—brought against technology providers (a small handful of federal appellate court cases and perhaps fewer than two dozen District Court cases in the last 20 years). I have found nothing in the briefs or the record that shows that *Sony* has failed to achieve its innovation-protecting objective. . . .

The second, more difficult, question is whether a modified *Sony* rule (or a strict interpretation) would significantly weaken the law's ability to protect new technology.

Justice Ginsburg's approach would require defendants to produce considerably more concrete evidence—more than was presented here—to earn *Sony*'s shelter. That heavier evidentiary demand, and especially the more dramatic (case-by-case balancing) modifications that MGM and the Government seek, would, I believe, undercut the protection that *Sony* now offers. . . .

The third question—whether a positive copyright impact would outweigh any technology-related loss—I find the most difficult of the three. I do not doubt that a more intrusive *Sony* test would generally provide greater revenue security for copyright holders. But it is harder to conclude that the gains on the copyright swings would exceed the losses on the technology roundabouts.

For one thing, the law disfavors equating the two different kinds of gain and loss; rather, it leans in favor of protecting technology. As *Sony* itself makes clear, the producer of a technology which permits unlawful copying does not himself engage in unlawful copying—a fact that makes the attachment of copyright liability to the creation, production, or distribution of the technology an exceptional thing. Moreover, *Sony* has been the law for some time. And that fact imposes a serious burden upon copyright holders like MGM to show a need for change in the current rules of the game, including a more strict interpretation of the test.

In any event, the evidence now available does not, in my view, make out a sufficiently strong case for change. . . . Will an unmodified *Sony* lead to a significant diminution in the amount or quality of creative work produced? Since copyright's basic objective is creation and its revenue objectives but a means to that end, this is the underlying copyright question. See *Twentieth Century Music Corp. v. Aiken* (1975) ("Creative work is to be encouraged and rewarded, but private motivation must ultimately serve the cause of promoting broad public availability of literature, music, and the other arts"). And its answer is far from clear.

Unauthorized copying likely diminishes industry revenue, though it is not clear by how much. . . . The extent to which related production has actually and resultingly declined remains uncertain, though there is good reason to believe that the decline, if any, is not substantial. See, e. g., M. Madden, Pew Internet & American Life Project, Artists, Musicians, and the Internet (nearly 70% of musicians believe that file sharing is a minor threat or no threat at all to creative industries); Benkler, *Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production*, 114 Yale L. J. 273, 351–352 (2004) ("Much of the actual flow of revenue to artists—from performances and other sources—is stable even assuming a complete displacement of the CD market by peer-to-peer distribution. . . . [I]t would be silly to think that music, a cultural form without which no human society has existed, will cease to be in our world [because of illegal file swapping]"). . . .

. . . As *Sony* recognized, the legislative option remains available. Courts are less well suited than Congress to the task of "accommodat[ing] fully the varied permutations of competing interests that are inevitably implicated by such new technology."

For these reasons, I disagree with Justice Ginsburg, but I agree with the Court and join its opinion.

Questions:

1.) A host of issues present themselves. We think one of the most important questions in intellectual property law (and perhaps law in general) is what role judges should play in elaborating its doctrines in the context of new technologies and new social realities. We

discussed that extensively in the preceding two chapters, focusing in particular on software and on fair use. How should judges interpret the law and apply it, when the statutory text is either vague or absent, or the technological context clearly different from the ones to which the law initially applied? Your question is this: is it appropriate for Federal judges to fashion—with no statutory basis whatsoever—a law of secondary infringement? Whether your answer was affirmative or negative, did you have the *same* answer in the fair use and software cases? If not, why not?

2.) Having fashioned such a law—built around contributory infringement and vicarious liability—why does it make sense to add a new form of liability built around inducement? Describe Justice Souter's motivation for doing so. Justice Ginsburg's? Justice Breyer's?

3.) State the test that *Grokster* lays down for inducement liability.

PROBLEM 14-2

You are an associate product development lawyer for Apple. The *Grokster* decision has been taken back in time and has just landed on your desk. Five minutes later, the first iPod is laid in front of you. At the time, assume the principal competing digital music player (from *Sony*) only plays DRM-protected music and will not play MP3 files. Assume a deliberate engineering decision has been made that the iPod will play unprotected MP3 files. Assume the iPod can also hold dramatically more songs than any available competing player. The iPod will be marketed in conjunction with three advertising campaigns. "Rip, Mix and Burn!" "10,000 songs in your pocket!" and a dystopian, *1984*-like image of shackled slaves, listening to a droning Big Brother, suddenly revolting when exposed to Apple's new technology. "The revolution is here," says the ad, "free your head. Free the music!" The advertisements have been made and circulated internally at Apple, but not yet aired. One of the attractive features of iTunes is that it will automatically retrieve album art for any digital music found on your computer or iPod. To do this, iTunes relies on "digital signatures" of the tracks on your iPod or computer. This service does not restrict itself to the DRM-protected AARC files sold from the iTunes store, it also works for any album "ripped" from a CD into MP3 form (which would be a fair use, were the original CD owned by the person doing the ripping). By the same token, it works for any illicitly downloaded MP3.

You must tell your boss whether the iPod might violate the rules laid down in the new *Grokster* decision, or the more traditional rules of contributory and vicarious infringement. How do you advise? What factors inform your analysis? Would you advise any changes to the product, accompanying service or advertising?

4.) Safe Harbors: Section 512, Direct Infringement and Secondary Liability

Let us leave secondary infringement for a moment and turn back to *direct* infringement. Having read *MAI*, which suggests that even transitory copies count as copies for the purpose of § 106, and learned that copyright is a strict liability system, which does not require bad intent, or even negligence, for liability, you may be wondering why the entire internet is not illegal—or constantly subject to copyright suits for *direct* infringement. After all, Google's "spiders" copy the entire web every day in order to index

it. Much of the material Google copies was itself illicitly copied—though Google does not "know" this when its spiders make copies. And those copies then sit on Google's titanic hard drives far longer than is needed to count as fixed; they are much more stable than a RAM copy. Google does this "on purpose"—there is much more intentionality about the copying than there was in the *Netcom* case. Hundreds of hours of video are uploaded to YouTube every *minute*: even though its digital fingerprinting and detection software is now very good, and even though some unauthorized uploads would be sufficiently transformative to count as fair use, that still leaves an enormous quantity of illicitly reproduced material. Facebook has millions of users posting content, some of which is illicitly copied (even if the users and Facebook sometimes do not know that). Dropbox and every other cyberlocker can be used to store both licit and infringing material. Gmail has billions of emails with infringing attachments passing through its systems, and sitting in its hard drives, every year. Time Warner Cable, Comcast and AT&T provide internet service to millions, and infringing material flows over those connections, and over the law school network you may be on right now. The networks temporarily "cache" material to speed up transmission. Some of the cached material is illicitly copied.

Why does this activity not make all of these intermediaries *directly* liable? (We will come to their potential indirect or secondary liability in a moment.) In each of these cases, the intermediary is *making* copies, on its own system, of infringing material. Is the whole internet somehow protected by *Netcom*, a single District Court decision that took a "creative" interpretation towards the law of its own circuit? (Revisit the *Netcom* decision from Chapter 11 to understand why we say that.)

The answer to this question is that, initially, it was the US government's official position that all these entities *should be*—indeed already were—strictly liable without any change in existing law, simply because of the combination of a broad conception of fixation and the fact that copyright was a strict liability system. As of 1995, the USPTO was saying that strict liability for internet intermediaries was a feature, not a bug. This is the way copyright infringement would be policed, just as products liability imposes strict liability on product sellers and then lets them decide how to keep their level of liability down.

Why did this not come to pass? The Digital Millennium Copyright Act—or more accurately, that part of it with the mellifluous name of the Online Copyright Infringement Liability Limitation Act (OCILLA)—provided a set of safe harbors which immunized many types of intermediaries, under certain conditions, from copyright liability. The key safe harbors are in § 512. It is no exaggeration to say that, without them, the internet as you know it would not exist. There would be a network, of course, but it would be wildly different from the one you know.

Look in the WIPO Copyright Treaty from the statutory supplement. You will see no requirement that there be § 512 limitations. In fact, while the EU E-Commerce Directive contains similar limitations, what is remarkable is that none of these are *required*. Rights are mandatory. Exceptions and limitations are optional. What would Jefferson say?

Section 512's structure is relatively simple. A series of types of online services are laid out. A set of requirements for the safe harbor is outlined for each type of service. But the safe harbor also contains *limitations*—patterns of behavior that will forfeit the safe harbor. The section is too long to reproduce in its entirety—please read it in the statutory supplement before reading the rest of this chapter. For illustration's sake, here is the beginning of section § 512(c). Ask yourself which specific services would benefit from it.

> **(c) Information Residing on Systems or Networks at Direction of Users.—**
> **(1) In general.—A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive**

> **or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if 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.**

The rest of the section goes on to detail the requirements of the "notice and takedown" procedure.

Notice subsection (B), which takes away the safe harbor if the service "receive[s] 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." What does that sound like? It should be extremely reminiscent of the discussion we have just had of vicarious liability. So how are we to think of 512? Is it a limitation only on liability for *direct* copyright infringement? Is it a limitation on both direct and secondary copyright liability, but one that does not apply if the provider is vicariously liable? Or is it something else altogether?

To answer these questions we will start with the Copyright Office's excellent summary of § 512. The summary is from December 1998, shortly after the passage of the DMCA. Several high profile cases have been decided since then, including the 2012 *Viacom v. YouTube* case, which follows the summary. *Viacom* analyzes the applicability of the § 512(c) safe harbor we have just read, and addresses the questions we posed. As the internet has developed, this provision has become increasingly important because it potentially limits the copyright liability of video sharing, social networking, and cloud computing services for material stored on their systems by users. YouTube, Facebook, Instagram, and Dropbox rely on § 512(c). Therefore, the court's interpretation of its requirements has far-reaching consequences.

Title II: Online Copyright Infringement Liability Limitation

U.S. Copyright Office Summary

Title II of the DMCA adds a new section 512 to the Copyright Act to create four new limitations on liability for copyright infringement by online service providers. The limitations are based on the following four categories of conduct by a service provider:

1. Transitory communications;
2. System caching;
3. Storage of information on systems or networks at direction of users; and
4. Information location tools.

New section 512 also includes special rules concerning the application of these limitations to nonprofit educational institutions.

Each limitation entails a complete bar on monetary damages, and restricts the availability of injunctive relief in various respects. (Section 512(j)). Each limitation relates to a separate and distinct function, and a determination of whether a service provider qualifies for one of the limitations does not bear upon a determination of whether the provider qualifies for any of the other three. (Section 512(n)).

The failure of a service provider to qualify for any of the limitations in section 512 does not necessarily make it liable for copyright infringement. The copyright owner must still demonstrate that the provider has infringed, and the provider may still avail itself of any of the defenses, such as fair use, that are available to copyright defendants generally. (Section 512(*l*)).

In addition to limiting the liability of service providers, Title II establishes a procedure by which a copyright owner can obtain a subpoena from a federal court ordering a service provider to disclose the identity of a subscriber who is allegedly engaging in infringing activities. (Section 512(h)).

Section 512 also contains a provision to ensure that service providers are not placed in the position of choosing between limitations on liability on the one hand and preserving the privacy of their subscribers, on the other. Subsection (m) explicitly states that nothing in section 512 requires a service provider to monitor its service or access material in violation of law (such as the Electronic Communications Privacy Act) in order to be eligible for any of the liability limitations.

Eligibility for Limitations Generally

A party seeking the benefit of the limitations on liability in Title II must qualify as a "service provider." For purposes of the first limitation, relating to transitory communications, "service provider" is defined in section 512(k)(1)(A) as "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." For purposes of the other three limitations, "service provider" is more broadly defined in section 512(k)(l)(B) as "a provider of online services or network access, or the operator of facilities therefor."

In addition, to be eligible for any of the limitations, a service provider must meet two overall conditions: (1) it must adopt and reasonably implement a policy of terminating in appropriate circumstances the accounts of subscribers who are repeat infringers; and (2) it must accommodate and not interfere with "standard technical measures." (Section 512(i)). "Standard technical measures" are defined as measures that copyright owners use to identify or protect copyrighted works, that have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair and voluntary multi-industry process, are available to anyone on reasonable nondiscriminatory terms, and do not impose substantial costs or burdens on service providers.

Limitation for Transitory Communications

In general terms, section 512(a) limits the liability of service providers in

circumstances where the provider merely acts as a data conduit, transmitting digital information from one point on a network to another at someone else's request. This limitation covers acts of transmission, routing, or providing connections for the information, as well as the intermediate and transient copies that are made automatically in the operation of a network.

In order to qualify for this limitation, the service provider's activities must meet the following conditions:

- The transmission must be initiated by a person other than the provider.
- The transmission, routing, provision of connections, or copying must be carried out by an automatic technical process without selection of material by the service provider.
- The service provider must not determine the recipients of the material.
- Any intermediate copies must not ordinarily be accessible to anyone other than anticipated recipients, and must not be retained for longer than reasonably necessary.
- The material must be transmitted with no modification to its content.

Limitation for System Caching

Section 512(b) limits the liability of service providers for the practice of retaining copies, for a limited time, of material that has been made available online by a person other than the provider, and then transmitted to a subscriber at his or her direction. The service provider retains the material so that subsequent requests for the same material can be fulfilled by transmitting the retained copy, rather than retrieving the material from the original source on the network.

The benefit of this practice is that it reduces the service provider's bandwidth requirements and reduces the waiting time on subsequent requests for the same information. On the other hand, it can result in the delivery of outdated information to subscribers and can deprive website operators of accurate "hit" information—information about the number of requests for particular material on a website—from which advertising revenue is frequently calculated. For this reason, the person making the material available online may establish rules about updating it, and may utilize technological means to track the number of "hits."

The limitation applies to acts of intermediate and temporary storage, when carried out through an automatic technical process for the purpose of making the material available to subscribers who subsequently request it. It is subject to the following conditions:

- The content of the retained material must not be modified.
- The provider must comply with rules about "refreshing" material—replacing retained copies of material with material from the original location—when specified in accordance with a generally accepted industry standard data communication protocol.
- The provider must not interfere with technology that returns "hit" information to the person who posted the material, where such technology meets certain requirements.
- The provider must limit users' access to the material in accordance with conditions on access (e.g., password protection) imposed by the person who posted the material.
- Any material that was posted without the copyright owner's authorization must be removed or blocked promptly once the service provider has been notified

that it has been removed, blocked, or ordered to be removed or blocked, at the originating site.

Limitation for Information Residing on Systems or Networks at the Direction of Users

Section 512(c) limits the liability of service providers for infringing material on websites (or other information repositories) hosted on their systems. It applies to storage at the direction of a user. In order to be eligible for the limitation, the following conditions must be met:

- The provider must not have the requisite level of knowledge of the infringing activity, as described below.
- If the provider has the right and ability to control the infringing activity, it must not receive a financial benefit directly attributable to the infringing activity.
- Upon receiving proper notification of claimed infringement, the provider must expeditiously take down or block access to the material.

In addition, a service provider must have filed with the Copyright Office a designation of an agent to receive notifications of claimed infringement. The Office provides a suggested form for the purpose of designating an agent (https://www.copyright.gov/dmca-directory/) and maintains a list of agents on the Copyright Office website (https:/dmca.copyright.gov/osp/).

Under the knowledge standard, a service provider is eligible for the limitation on liability only if it does not have actual knowledge of the infringement, is not aware of facts or circumstances from which infringing activity is apparent, or upon gaining such knowledge or awareness, responds expeditiously to take the material down or block access to it.

The statute also establishes procedures for proper notification, and rules as to its effect. (Section 512(c)(3)). Under the notice and takedown procedure, a copyright owner submits a notification under penalty of perjury, including a list of specified elements, to the service provider's designated agent. Failure to comply substantially with the statutory requirements means that the notification will not be considered in determining the requisite level of knowledge by the service provider. If, upon receiving a proper notification, the service provider promptly removes or blocks access to the material identified in the notification, the provider is exempt from monetary liability. In addition, the provider is protected from any liability to any person for claims based on its having taken down the material. (Section 512(g)(1)).

In order to protect against the possibility of erroneous or fraudulent notifications, certain safeguards are built into section 512. Subsection (g)(1) gives the subscriber the opportunity to respond to the notice and takedown by filing a counter notification. In order to qualify for the protection against liability for taking down material, the service provider must promptly notify the subscriber that it has removed or disabled access to the material. If the subscriber serves a counter notification complying with statutory requirements, including a statement under penalty of perjury that the material was removed or disabled through mistake or misidentification, then unless the copyright owner files an action seeking a court order against the subscriber, the service provider must put the material back up within 10–14 business days after receiving the counter notification.

Penalties are provided for knowing material misrepresentations in either a notice or a counter notice. Any person who knowingly materially misrepresents that material is infringing, or that it was removed or blocked through mistake or misidentification, is liable for any resulting damages (including costs and attorneys' fees) incurred by the alleged infringer, the copyright owner or its licensee, or the service provider. (Section 512(f)).

Limitation for Information Location Tools

Section 512(d) relates to hyperlinks, online directories, search engines and the like. It limits liability for the acts of referring or linking users to a site that contains infringing material by using such information location tools, if the following conditions are met:

- The provider must not have the requisite level of knowledge that the material is infringing. The knowledge standard is the same as under the limitation for information residing on systems or networks.
- If the provider has the right and ability to control the infringing activity, the provider must not receive a financial benefit directly attributable to the activity.
- Upon receiving a notification of claimed infringement, the provider must expeditiously take down or block access to the material.

These are essentially the same conditions that apply under the previous limitation, with some differences in the notification requirements. The provisions establishing safeguards against the possibility of erroneous or fraudulent notifications, as discussed above, as well as those protecting the provider against claims based on having taken down the material apply to this limitation. (Sections 512(f)–(g)).

PROBLEM 14-3

a.) **List one service that you use that seems to fit into each of the safe harbors provided by § 512(a), (b), (c), and (d) (i.e., list one service per safe harbor). In each case describe what the service has to do in order to qualify for the safe harbor. Put differently, what specific types of behavior could cause it to *lose* the safe harbor? Finally, explain why the requirements for each type of service are different.**

b.) [As always, facts have been changed—or invented—for the purposes of this assignment.] Each year, James, a Duke law professor, assigns *The Grey Album* by DJ Danger Mouse as part of his Intellectual Property class. *The Grey Album* is a mashup of the Beatles' *The White Album* and an *a capella* version of Jay Z's *The Black Album*. James includes the audio and video of *The Grey Album* in his discussion of fair use under § 107. He uses it as a practice example and asks the students whether it is a fair use. (Responses vary.)

The Grey Album is controversial. The owners of the rights to the original works that Danger Mouse sampled have repeatedly claimed that it is a blatant copyright infringement. Through legal action, they were able to stop *The Grey Album* from being released commercially which, ironically, made it an online sensation. (*See* "Streisand Effect, The".) Finding they were unable to quell demand for the album, they have aimed at restricting supply. They have sent numerous DMCA takedown notices, as described in § 512(c), to sites such as YouTube. Even when counter-notices were sent by Danger Mouse, YouTube and other sites claimed that they were required to take the material down in order to keep their safe harbor. (True?) Thus, there are very few online sources for *The Grey Album*, or for the extremely amusing mashup videos that have been made using its soundtrack. Because of the dearth of online access, James declares that he has to make the music and videos available—"for educational purposes." All Duke professors have their own pages on the Duke network—"a foundational part of academic freedom," the Provost explains. James uploaded the audio and video to the Duke network and featured it prominently on his page, which is available not just to his students but to everyone on the internet. James's page

presents the Danger Mouse audio and video in the middle of a dense commentary by him on fair use. Ego-bruisingly, most of those who come to the page just view or download the video and audio, and seem unmoved by the § 107 analysis. Not content with this, James created a "Grey Album Search Engine" which scans the web for other copies of Danger Mouse's classic work and supplies current and live hyperlinks to any searcher. Duke (and James) have been served with many takedown notices because of this behavior. Duke's beloved OIT department removes the material on James's page each time it receives a notice to the designated DMCA compliance agent, but James simply re-posts the files, and the links, again the next day. He claims that the copyright owners know this is a fair use and that Duke's administration "needs to make the crucial evolutionary leap from invertebrate to vertebrate."

Can James claim the DMCA safe harbor if he is sued personally for copyright infringement? Can Duke if it is sued for copyright infringement? [Hint: remember § 512(e).] Does failing to get the safe harbor mean that either James, or Duke, is liable?

Viacom International, Inc. v. YouTube, Inc.

676 F.3d 19 (2d Cir. 2012)

JOSÉ A. CABRANES, Circuit Judge.

This appeal requires us to clarify the contours of the "safe harbor" provision of the Digital Millennium Copyright Act (DMCA) that limits the liability of online service providers for copyright infringement that occurs "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." 17 U.S.C. § 512(c). . . .

The plaintiffs alleged direct and secondary copyright infringement based on the public performance, display, and reproduction of approximately 79,000 audiovisual "clips" that appeared on the YouTube website between 2005 and 2008. They demanded, inter alia, statutory damages pursuant to 17 U.S.C. § 504(c) or, in the alternative, actual damages from the alleged infringement, as well as declaratory and injunctive relief.

In a June 23, 2010 Opinion and Order (the "June 23 Opinion"), the District Court held that the defendants were entitled to DMCA safe harbor protection primarily because they had insufficient notice of the particular infringements in suit. In construing the statutory safe harbor, the District Court concluded that the "actual knowledge" or "aware[ness] of facts or circumstances" that would disqualify an online service provider from safe harbor protection under § 512(c)(1)(A) refer to "knowledge of specific and identifiable infringements." The District Court further held that item-specific knowledge of infringing activity is required for a service provider to have the "right and ability to control" infringing activity under § 512(c)(1)(B). . . .

These related cases present a series of significant questions of statutory construction. We conclude that the District Court correctly held that the § 512(c) safe harbor requires knowledge or awareness of specific infringing activity, but we vacate the order granting summary judgment because a reasonable jury could find that YouTube had actual knowledge or awareness of specific infringing activity on its website. We further hold that the District Court erred by interpreting the "right and ability to control" provision to require "item-specific" knowledge. . . .

BACKGROUND

A. The DMCA Safe Harbors

"The DMCA was enacted in 1998 to implement the World Intellectual Property Organization Copyright Treaty," *Universal City Studios, Inc. v. Corley* (2d Cir. 2001), and to update domestic copyright law for the digital age. Title II of the DMCA, separately titled the "Online Copyright Infringement Liability Limitation Act" (OCILLA), was designed to "clarif[y] the liability faced by service providers who transmit potentially infringing material over their networks." S.Rep. No. 105-190 at 2 (1998). But "[r]ather than embarking upon a wholesale clarification" of various copyright doctrines, Congress elected "to leave current law in its evolving state and, instead, to create a series of 'safe harbors[]' for certain common activities of service providers." To that end, OCILLA established a series of four "safe harbors" that allow qualifying service providers to limit their liability for claims of copyright infringement based on (a) "transitory digital network communications," (b) "system caching," (c) "information residing on systems or networks at [the] direction of users," and (d) "information location tools." 17 U.S.C. § 512(a)–(d).

To qualify for protection under any of the safe harbors, a party must meet a set of threshold criteria. First, the party must in fact be a "service provider," defined, in pertinent part, as "a provider of online services or network access, or the operator of facilities therefor." 17 U.S.C. § 512(k)(1)(B). A party that qualifies as a service provider must also satisfy certain "conditions of eligibility," including the adoption and reasonable implementation of a "repeat infringer" policy that "provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network." § 512(i)(1)(A). In addition, a qualifying service provider must accommodate "standard technical measures" that are "used by copyright owners to identify or protect copyrighted works." § 512(i)(1)(B), (i)(2).

Beyond the threshold criteria, a service provider must satisfy the requirements of a particular safe harbor. In this case, the safe harbor at issue is § 512(c), which covers infringement claims that arise "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." § 512(c)(1). The § 512(c) safe harbor will apply only 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.

§ 512(c)(1)(A)–(C). Section 512(c) also sets forth a detailed notification scheme that requires service providers to "designate[] an agent to receive notifications of claimed infringement," § 512(c)(2), and specifies the components of a proper notification, commonly known as a "takedown notice," to that agent, see § 512(c)(3). Thus, actual knowledge of infringing material, awareness of facts or circumstances that make infringing activity apparent, or receipt of a takedown notice will each trigger an

obligation to expeditiously remove the infringing material.

With the statutory context in mind, we now turn to the facts of this case.

B. Factual Background

YouTube was founded in February 2005 by Chad Hurley ("Hurley"), Steve Chen ("Chen"), and Jawed Karim ("Karim"), three former employees of the internet company PayPal. When YouTube announced the "official launch" of the website in December 2005, a press release described YouTube as a "consumer media company" that "allows people to watch, upload, and share personal video clips at www.YouTube.com." Under the slogan "Broadcast yourself," YouTube achieved rapid prominence and profitability, eclipsing competitors such as Google Video and Yahoo Video by wide margins. In November 2006, Google acquired YouTube in a stock-for-stock transaction valued at $1.65 billion. By March 2010, at the time of summary judgment briefing in this litigation, site traffic on YouTube had soared to more than 1 billion daily video views, with more than 24 hours of new video uploaded to the site every minute.

The basic function of the YouTube website permits users to "upload" and view video clips free of charge. Before uploading a video to YouTube, a user must register and create an account with the website. The registration process requires the user to accept YouTube's Terms of Use agreement, which provides, inter alia, that the user "will not submit material that is copyrighted . . . unless [he is] the owner of such rights or ha[s] permission from their rightful owner to post the material and to grant YouTube all of the license rights granted herein." When the registration process is complete, the user can sign in to his account, select a video to upload from the user's personal computer, mobile phone, or other device, and instruct the YouTube system to upload the video by clicking on a virtual upload "button."

Uploading a video to the YouTube website triggers a series of automated software functions. During the upload process, YouTube makes one or more exact copies of the video in its original file format. YouTube also makes one or more additional copies of the video in "Flash" format, a process known as "transcoding." The transcoding process ensures that YouTube videos are available for viewing by most users at their request. The YouTube system allows users to gain access to video content by "streaming" the video to the user's computer in response to a playback request. YouTube uses a computer algorithm to identify clips that are "related" to a video the user watches and display links to the "related" clips. . . .

DISCUSSION

A. Actual and "Red Flag" Knowledge: § 512(c)(1)(A)

The first and most important question on appeal is whether the DMCA safe harbor at issue requires "actual knowledge" or "aware[ness]" of facts or circumstances indicating "specific and identifiable infringements." We consider first the scope of the statutory provision and then its application to the record in this case.

1. The Specificity Requirement

"As in all statutory construction cases, we begin with the language of the statute," *Barnhart v. Sigmon Coal Co.* (2002). Under § 512(c)(1)(A), safe harbor protection is available only if the service provider:

> (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. . . .

17 U.S.C. § 512(c)(1)(A). As previously noted, the District Court held that the statutory phrases "actual knowledge that the material . . . is infringing" and "facts or circumstances from which infringing activity is apparent" refer to "knowledge of specific and identifiable infringements." For the reasons that follow, we substantially affirm that holding.

Although the parties marshal a battery of other arguments on appeal, it is the text of the statute that compels our conclusion. In particular, we are persuaded that the basic operation of § 512(c) requires knowledge or awareness of specific infringing activity. Under § 512(c)(1)(A), knowledge or awareness alone does not disqualify the service provider; rather, the provider that gains knowledge or awareness of infringing activity retains safe-harbor protection if it "acts expeditiously to remove, or disable access to, the material." 17 U.S.C. § 512(c)(1)(A)(iii). Thus, the nature of the removal obligation itself contemplates knowledge or awareness of specific infringing material, because expeditious removal is possible only if the service provider knows with particularity which items to remove. Indeed, to require expeditious removal in the absence of specific knowledge or awareness would be to mandate an amorphous obligation to "take commercially reasonable steps" in response to a generalized awareness of infringement. Such a view cannot be reconciled with the language of the statute, which requires "expeditious[]" action to remove or disable "*the material*" at issue. 17 U.S.C. § 512(c)(1)(A)(iii) (emphasis added).

On appeal, the plaintiffs dispute this conclusion by drawing our attention to § 512(c)(1)(A)(ii), the so-called "red flag" knowledge provision. See § 512(c)(1)(A)(ii) (limiting liability where, "in the absence of such actual knowledge, [the service provider] is not aware of facts or circumstances from which infringing activity is apparent"). In their view, the use of the phrase "facts or circumstances" demonstrates that Congress did not intend to limit the red flag provision to a particular type of knowledge. The plaintiffs contend that requiring awareness of specific infringements in order to establish "aware[ness] of facts or circumstances from which infringing activity is apparent," 17 U.S.C. § 512(c)(1)(A)(ii), renders the red flag provision superfluous, because that provision would be satisfied only when the "actual knowledge" provision is also satisfied. For that reason, the plaintiffs urge the Court to hold that the red flag provision "requires less specificity" than the actual knowledge provision.

This argument misconstrues the relationship between "actual" knowledge and "red flag" knowledge. It is true that "we are required to 'disfavor interpretations of statutes that render language superfluous.'" *Conn. ex rel. Blumenthal v. U.S. Dep't of the Interior* (2d Cir. 2000). But contrary to the plaintiffs' assertions, construing § 512(c)(1)(A) to require actual knowledge or awareness of specific instances of infringement does not render the red flag provision superfluous. The phrase "actual knowledge," which appears in § 512(c)(1)(A)(i), is frequently used to denote subjective belief. By contrast, courts often invoke the language of "facts or circumstances," which appears in § 512(c)(1)(A)(ii), in discussing an objective reasonableness standard.

The difference between actual and red flag knowledge is thus not between specific and generalized knowledge, but instead between a subjective and an objective standard. In other words, the actual knowledge provision turns on whether the provider actually or "subjectively" knew of specific infringement, while the red flag provision turns on whether the provider was subjectively aware of facts that would have made the specific infringement "objectively" obvious to a reasonable person. The red flag provision, because it incorporates an objective standard, is not swallowed up by the actual

knowledge provision under our construction of the § 512(c) safe harbor. Both provisions do independent work, and both apply only to specific instances of infringement.

The limited body of case law interpreting the knowledge provisions of the § 512(c) safe harbor comports with our view of the specificity requirement. Most recently, a panel of the Ninth Circuit addressed the scope of § 512(c) in *UMG Recordings, Inc. v. Shelter Capital Partners LLC* (9th Cir. 2011), a copyright infringement case against Veoh Networks, a video-hosting service similar to YouTube. As in this case, various music publishers brought suit against the service provider, claiming direct and secondary copyright infringement based on the presence of unauthorized content on the website, and the website operator sought refuge in the § 512(c) safe harbor. The Court of Appeals affirmed the district court's determination on summary judgment that the website operator was entitled to safe harbor protection. With respect to the actual knowledge provision, the panel declined to "adopt[] a broad conception of the knowledge requirement," holding instead that the safe harbor "[r]equir[es] specific knowledge of particular infringing activity." The Court of Appeals "reach[ed] the same conclusion" with respect to the red flag provision, noting that "[w]e do not place the burden of determining whether [materials] are actually illegal on a service provider."

Although *Shelter Capital* contains the most explicit discussion of the § 512(c) knowledge provisions, other cases are generally in accord. While we decline to adopt the reasoning of those decisions in toto, we note that no court has embraced the contrary proposition—urged by the plaintiffs—that the red flag provision "requires less specificity" than the actual knowledge provision.

Based on the text of § 512(c)(1)(A), as well as the limited case law on point, we affirm the District Court's holding that actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement will disqualify a service provider from the safe harbor.

2. The Grant of Summary Judgment

The corollary question on appeal is whether, under the foregoing construction of § 512(c)(1)(A), the District Court erred in granting summary judgment to YouTube on the record presented. For the reasons that follow, we hold that although the District Court correctly interpreted § 512(c)(1)(A), summary judgment for the defendants was premature.

i. Specific Knowledge or Awareness

The plaintiffs argue that, even under the District Court's construction of the safe harbor, the record raises material issues of fact regarding YouTube's actual knowledge or "red flag" awareness of specific instances of infringement. To that end, the plaintiffs draw our attention to various estimates regarding the percentage of infringing content on the YouTube website. For example, Viacom cites evidence that YouTube employees conducted website surveys and estimated that 75–80% of all YouTube streams contained copyrighted material. The class plaintiffs similarly claim that Credit Suisse, acting as financial advisor to Google, estimated that more than 60% of YouTube's content was "premium" copyrighted content—and that only 10% of the premium content was authorized. These approximations suggest that the defendants were conscious that significant quantities of material on the YouTube website were infringing. But such estimates are insufficient, standing alone, to create a triable issue of fact as to whether YouTube actually knew, or was aware of facts or circumstances that would indicate, the existence of particular instances of infringement.

Beyond the survey results, the plaintiffs rely upon internal YouTube communications that do refer to particular clips or groups of clips. The class plaintiffs

argue that YouTube was aware of specific infringing material because, inter alia, YouTube attempted to search for specific Premier League videos on the site in order to gauge their "value based on video usage." In particular, the class plaintiffs cite a February 7, 2007 e-mail from Patrick Walker, director of video partnerships for Google and YouTube, requesting that his colleagues calculate the number of daily searches for the terms "soccer," "football," and "Premier League" in preparation for a bid on the global rights to Premier League content. On another occasion, Walker requested that any "clearly infringing, official broadcast footage" from a list of top Premier League clubs—including Liverpool Football Club, Chelsea Football Club, Manchester United Football Club, and Arsenal Football Club—be taken down in advance of a meeting with the heads of "several major sports teams and leagues." YouTube ultimately decided not to make a bid for the Premier League rights—but the infringing content allegedly remained on the website.

The record in the Viacom action includes additional examples. For instance, YouTube founder Jawed Karim prepared a report in March 2006 which stated that, "[a]s of today[,] episodes and clips of the following well-known shows can still be found [on YouTube]: Family Guy, South Park, MTV Cribs, Daily Show, Reno 911, [and] Dave Chapelle [sic]." Karim further opined that, "although YouTube is not legally required to monitor content . . . and complies with DMCA takedown requests, we would benefit from preemptively removing content that is blatantly illegal and likely to attract criticism." He also noted that "a more thorough analysis" of the issue would be required. At least some of the TV shows to which Karim referred are owned by Viacom. A reasonable juror could conclude from the March 2006 report that Karim knew of the presence of Viacom-owned material on YouTube, since he presumably located specific clips of the shows in question before he could announce that YouTube hosted the content "[a]s of today." A reasonable juror could also conclude that Karim believed the clips he located to be infringing (since he refers to them as "blatantly illegal"), and that YouTube did not remove the content from the website until conducting "a more thorough analysis," thus exposing the company to liability in the interim.

Furthermore, in a July 4, 2005 e-mail exchange, YouTube founder Chad Hurley sent an e-mail to his co-founders with the subject line "budlight commercials," and stated, "we need to reject these too." Steve Chen responded, "can we please leave these in a bit longer? another week or two can't hurt." Karim also replied, indicating that he "added back in all 28 bud videos." Similarly, in an August 9, 2005 e-mail exchange, Hurley urged his colleagues "to start being diligent about rejecting copyrighted / inappropriate content," noting that "there is a cnn clip of the shuttle clip on the site today, if the boys from Turner would come to the site, they might be pissed?" Again, Chen resisted:

> but we should just keep that stuff on the site. i really don't see what will happen. what? someone from cnn sees it? he happens to be someone with power? he happens to want to take it down right away. he gets in touch with cnn legal. 2 weeks later, we get a cease & desist letter. we take the video down.

And again, Karim agreed, indicating that "the CNN space shuttle clip, I like. we can remove it once we're bigger and better known, but for now that clip is fine."

Upon a review of the record, we are persuaded that the plaintiffs may have raised a material issue of fact regarding YouTube's knowledge or awareness of specific instances of infringement. The foregoing Premier League e-mails request the identification and removal of "clearly infringing, official broadcast footage." The March 2006 report indicates Karim's awareness of specific clips that he perceived to be "blatantly illegal." Similarly, the Bud Light and space shuttle e-mails refer to particular clips in the context

of correspondence about whether to remove infringing material from the website. On these facts, a reasonable juror could conclude that YouTube had actual knowledge of specific infringing activity, or was at least aware of facts or circumstances from which specific infringing activity was apparent. See § 512(c)(1)(A)(i)–(ii). Accordingly, we hold that summary judgment to YouTube on all clips-in-suit, especially in the absence of any detailed examination of the extensive record on summary judgment, was premature. . . .

ii. "Willful Blindness"

The plaintiffs further argue that the District Court erred in granting summary judgment to the defendants despite evidence that YouTube was "willfully blind" to specific infringing activity. On this issue of first impression, we consider the application of the common law willful blindness doctrine in the DMCA context.

"The principle that willful blindness is tantamount to knowledge is hardly novel." *Tiffany (NJ) Inc. v. eBay, Inc.* (2d Cir. 2010). A person is "willfully blind" or engages in "conscious avoidance" amounting to knowledge where the person "'was aware of a high probability of the fact in dispute and consciously avoided confirming that fact.'" *United States v. Aina-Marshall* (2d Cir. 2003). Writing in the trademark infringement context, we have held that "[a] service provider is not . . . permitted willful blindness. When it has reason to suspect that users of its service are infringing a protected mark, it may not shield itself from learning of the particular infringing transactions by looking the other way." *Tiffany*.

The DMCA does not mention willful blindness. As a general matter, we interpret a statute to abrogate a common law principle only if the statute "speak[s] directly to the question addressed by the common law." *Matar v. Dichter* (2d Cir. 2009). The relevant question, therefore, is whether the DMCA "speak[s] directly" to the principle of willful blindness. The DMCA provision most relevant to the abrogation inquiry is § 512(m), which provides that safe harbor protection shall not be conditioned on "a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i)." 17 U.S.C. § 512(m)(1). Section 512(m) is explicit: DMCA safe harbor protection cannot be conditioned on affirmative monitoring by a service provider. For that reason, § 512(m) is incompatible with a broad common law duty to monitor or otherwise seek out infringing activity based on general awareness that infringement may be occurring. That fact does not, however, dispose of the abrogation inquiry; as previously noted, willful blindness cannot be defined as an affirmative duty to monitor. Because the statute does not "speak[] directly" to the willful blindness doctrine, § 512(m) limits—but does not abrogate— the doctrine. Accordingly, we hold that the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA.

The District Court cited § 512(m) for the proposition that safe harbor protection does not require affirmative monitoring, but did not expressly address the principle of willful blindness or its relationship to the DMCA safe harbors. As a result, whether the defendants made a "deliberate effort to avoid guilty knowledge," *In re Aimster*, remains a fact question for the District Court to consider in the first instance on remand.

B. Control and Benefit: § 512(c)(1)(B)

Apart from the foregoing knowledge provisions, the § 512(c) safe harbor provides that an eligible service provider must "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." 17 U.S.C. § 512(c)(1)(B). The District Court addressed this issue in

a single paragraph, quoting from § 512(c)(1)(B), the so-called "control and benefit" provision, and concluding that "[t]he 'right and ability to control' the activity requires knowledge of it, which must be item-specific." For the reasons that follow, we hold that the District Court erred by importing a specific knowledge requirement into the control and benefit provision, and we therefore remand for further fact-finding on the issue of control.

1. "Right and Ability to Control" Infringing Activity

On appeal, the parties advocate two competing constructions of the "right and ability to control" infringing activity. 17 U.S.C. § 512(c)(1)(B). Because each is fatally flawed, we reject both proposed constructions in favor of a fact-based inquiry to be conducted in the first instance by the District Court.

The first construction, pressed by the defendants, is the one adopted by the District Court, which held that "the provider must know of the particular case before he can control it." The Ninth Circuit recently agreed, holding that "until [the service provider] becomes aware of specific unauthorized material, it cannot exercise its 'power or authority' over the specific infringing item. In practical terms, it does not have the kind of ability to control infringing activity the statute contemplates." *UMG Recordings, Inc. v. Shelter Capital Partners LLC* (9th Cir. 2011). The trouble with this construction is that importing a specific knowledge requirement into § 512(c)(1)(B) renders the control provision duplicative of § 512(c)(1)(A). Any service provider that has item-specific knowledge of infringing activity and thereby obtains financial benefit would already be excluded from the safe harbor under § 512(c)(1)(A) for having specific knowledge of infringing material and failing to effect expeditious removal. No additional service provider would be excluded by § 512(c)(1)(B) that was not already excluded by § 512(c)(1)(A). Because statutory interpretations that render language superfluous are disfavored, we reject the District Court's interpretation of the control provision.

The second construction, urged by the plaintiffs, is that the control provision codifies the common law doctrine of vicarious copyright liability. The common law imposes liability for vicarious copyright infringement "[w]hen the right and ability to supervise coalesce with an obvious and direct financial interest in the exploitation of copyrighted materials—even in the absence of actual knowledge that the copyright mono[poly] is being impaired." *Shapiro, Bernstein & Co. v. H.L. Green Co.* (2d Cir. 1963). To support their codification argument, the plaintiffs rely on a House Report relating to a preliminary version of the DMCA: "The 'right and ability to control' language . . . codifies the second element of vicarious liability. . . . Subparagraph (B) is intended to preserve existing case law that examines all relevant aspects of the relationship between the primary and secondary infringer." H.R.Rep. No. 105-551(I), at 26 (1998). In response, YouTube notes that the codification reference was omitted from the committee reports describing the final legislation, and that Congress ultimately abandoned any attempt to "embark[] upon a wholesale clarification" of vicarious liability, electing instead "to create a series of 'safe harbors' for certain common activities of service providers." S.Rep. No. 105-190, at 19.

Happily, the future of digital copyright law does not turn on the confused legislative history of the control provision. The general rule with respect to common law codification is that when "Congress uses terms that have accumulated settled meaning under the common law, a court must infer, unless the statute otherwise dictates, that Congress means to incorporate the established meaning of those terms." *Neder v. United States* (1999). Under the common law vicarious liability standard, "'[t]he ability to block infringers' access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise.'" *Arista Records LLC v. Usenet.com, Inc.* (S.D.N.Y. 2009). To adopt

that principle in the DMCA context, however, would render the statute internally inconsistent. Section 512(c) actually presumes that service providers have the ability to "block . . . access" to infringing material. Indeed, a service provider who has knowledge or awareness of infringing material or who receives a takedown notice from a copyright holder is required to "remove, or disable access to, the material" in order to claim the benefit of the safe harbor. 17 U.S.C. § 512(c)(1)(A)(iii) & (C). But in taking such action, the service provider would—in the plaintiffs' analysis—be admitting the "right and ability to control" the infringing material. Thus, the prerequisite to safe harbor protection under § 512(c)(1)(A)(iii) & (C) would at the same time be a disqualifier under § 512(c)(1)(B).

Moreover, if Congress had intended § 512(c)(1)(B) to be coextensive with vicarious liability, "the statute could have accomplished that result in a more direct manner." *Shelter Capital*.

It is conceivable that Congress . . . intended that [service providers] which receive a financial benefit directly attributable to the infringing activity would not, under any circumstances, be able to qualify for the subsection (c) safe harbor. But if that was indeed their intention, it would have been far simpler and much more straightforward to simply say as much.

In any event, the foregoing tension—elsewhere described as a "predicament" and a "catch22"—is sufficient to establish that the control provision "dictates" a departure from the common law vicarious liability standard. Accordingly, we conclude that the "right and ability to control" infringing activity under § 512(c)(1)(B) "requires something more than the ability to remove or block access to materials posted on a service provider's website." *MP3tunes, LLC*. The remaining—and more difficult—question is how to define the "something more" that is required.

To date, only one court has found that a service provider had the right and ability to control infringing activity under § 512(c)(1)(B). In *Perfect 10, Inc. v. Cybernet Ventures, Inc.* (C.D.Cal. 2002), the court found control where the service provider instituted a monitoring program by which user websites received "detailed instructions regard[ing] issues of layout, appearance, and content." The service provider also forbade certain types of content and refused access to users who failed to comply with its instructions. Similarly, inducement of copyright infringement under *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* (2005), which "premises liability on purposeful, culpable expression and conduct," might also rise to the level of control under § 512(c)(1)(B). Both of these examples involve a service provider exerting substantial influence on the activities of users, without necessarily—or even frequently—acquiring knowledge of specific infringing activity.

In light of our holding that § 512(c)(1)(B) does not include a specific knowledge requirement, we think it prudent to remand to the District Court to consider in the first instance whether the plaintiffs have adduced sufficient evidence to allow a reasonable jury to conclude that YouTube had the right and ability to control the infringing activity and received a financial benefit directly attributable to that activity. . . .

Questions:

1.) Explain succinctly why the court finds that § 512(c)'s limits are not the same as those imposed by vicarious liability.

2.) Is § 512(c) a limit against direct infringement? Secondary infringement? Both?

3.) Copyright holders in the entertainment industries were outraged by the YouTube ruling. Imagine you are acting for the RIAA and MPAA. What is your principal critique?

4.) Explain what "red flag knowledge" means. Use examples.

5.) YouTube itself has now implemented a fascinating, and apparently effective, system called Content ID, which allows rights-holders to register digital fingerprints of the works they own with YouTube. If such a work is subsequently uploaded to YouTube by someone else, Content ID allows the rights-holder to block, track or monetize the work. Blocking the work keeps it off YouTube. Tracking the work gives the rights-holders a wealth of valuable demographic data from YouTube's files—people who watch Justin Bieber also love Katy Perry. Serves them right. (In the academic literature, this is referred to as "mutually assured desecration.") Those who listen to Tori Amos are likely to have ineffectual constitutional advocates, and so on. Rights holders who choose to "monetize" the videos will get a share of any advertisements played alongside the video. All of this is done through code (software recognition of uploaded video) and contract (agreements with rightsholders). What does all this have to say about the future of copyright law? To the fair use provisions in particular? To the law of secondary liability? To the meaning of § 512?