

**SPRING 2005 SUPPLEMENT TO**

# **CYBERLAW**

**PROBLEMS OF POLICY  
AND JURISPRUDENCE IN THE  
INFORMATION AGE**

**Second Edition**

**By**

**Patricia L. Bellia**

*Associate Professor of Law  
Notre Dame Law School*

**Paul Schiff Berman**

*Professor of Law  
University of Connecticut School of Law*

**David G. Post**

*Professor of Law  
Beasley School of Law, Temple University*

**LAST UPDATED DECEMBER 27, 2004**



# Table of Contents

---

	Page
TABLE OF CASES .....	v
<b>Chapter Three: Problems of Geography and Sovereignty</b> .....	1
B. Jurisdiction to Prescribe .....	1
1. Extraterritorial Regulation of Speech .....	1
2. The “Dormant” Commerce Clause .....	1
C. Jurisdiction to Adjudicate .....	2
2. Jurisdiction Based on Online Interaction .....	2
D. The Power to Enforce .....	3
1. Judgment Recognition and the Power of Persuasion .....	3
<b>Chapter Five: Problems of “Public” versus “Private” Regulation</b> .....	5
C. Government Regulation versus Private Filtering .....	5
1. Government Regulation of Sexually Explicit Speech .....	5
2. Filtering Sexually Explicit Speech .....	6
<b>Chapter Six: Problems of Speakers and Conduits</b> .....	7
B. Open Access .....	7
C. The Role of Internet Service Providers and Other Intermediaries ---	7
2. Copyright Liability .....	7
<i>Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.</i> .....	9
<i>Notes and Questions</i> .....	18
<b>Chapter Seven: Problems of Control over Information</b> .....	19
C. Control of Access to Data and Network Resources .....	19



## Table of Cases

The principal cases are in bold type. Cases cited or discussed in the text are roman type. References are to pages.

Ashcroft v. American Civil Liberties Union, 542 U.S. ___, 124 S. Ct. 2783 (2004), 1, 5, 6	Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003), 19
A & M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001), 11-17	Lewis v. King, [2004] All E.R. (D) 234 (Oct.) (C.A.) (Eng.), 2
A & M Records v. Napster, 284 F.3d 1091 (9th Cir. 2002), 12-14, 16	<b>Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd.</b> , 380 F.3d 1154 (9th Cir.), <i>cert. granted</i> , ___ U.S. ___ (Dec. 10, 2004), 9
ALS Scan v. RemarQ Communities, Inc., 239 F.3d 619 (4th Cir. 2001), 8	Pike v. Bruce Church, 397 U.S. 137 (1970), 1
American Civil Liberties Union v. Ashcroft, 322 F.3d 240 (3d Cir. 2003), 5	Religious Technology Ctr. v. Netcom On-Line Communications Servs., 907 F. Supp. 1361 (N.D. Cal. 1995), 14
Center for Democracy and Technology v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004), 1, 2, 6	Richardson v. Schwarzenegger, [2004] All E.R. (D) 432 (Oct.) (Q.B.) (Eng.), 2
CoStar v. LoopNet, Inc., 373 F.3d 544 (4th Cir. 2004), 7, 8	Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984), 11-13
Ellison v. Robertson, 357 F.3d 1072 (9th Cir. 2004), 8	Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisémitisme, 379 F. 3d 1120 (9th Cir. 2004), 3
Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996), 15, 16	
In re Aimster Copyright Litig., 334 F.3d 643 (7th Cir.2003), 12	



## Chapter Three

---

---

# PROBLEMS OF GEOGRAPHY AND SOVEREIGNTY

---

## SECTION B. JURISDICTION TO PRESCRIBE

### 1. Extraterritorial Regulation of Speech

**Page 104:**

**At the end of note 7, add:**

The Supreme Court subsequently affirmed, though the Court suggested that the Third Circuit had unnecessarily construed various statutory definitions not considered by the district court. *Ashcroft v. American Civil Liberties Union*, 542 U.S. \_\_\_, 124 S. Ct. 2783, 2791 (2004). Accordingly, the Court limited itself to ruling that the district court did not abuse its discretion in granting preliminary injunctive relief. *Id.* at \_\_\_, 124 S. Ct. at 2795. For further discussion, see Casebook p. 429 and Supplement p. 5.

### 2. The “Dormant” Commerce Clause

**Page 121:**

**Delete the last paragraph of note 10 and add:**

In a lawsuit challenging the Pennsylvania statute on these grounds, as well as on First Amendment grounds, a district court concluded that the statute failed the *Pike* balancing test. The court reasoned that the act had minimal local benefit, because those interested in “obtaining or providing child pornography can evade blocking efforts using a number of different methods,” and that the act substantially burdened interstate commerce, because providers seeking to comply with the act were forced to disable sites that did not in fact contain child pornography. *Center for Democracy and Technology v. Pappert*,

337 F. Supp. 2d 606, 662 (E.D. Pa. 2004). The court also concluded that the act “has the practical effect of exporting Pennsylvania’s domestic policies,” because some ISPs are only able to implement blocking orders on a nationwide basis. *Id.* at 645-46, 662-63.

## SECTION C. JURISDICTION TO ADJUDICATE

### 2. Jurisdiction Based on Online Interaction

**Page 164:**

**At the end of note 5, add:**

Subsequent to *Gutnick*, the British House of Lords likewise ruled that internet publication takes place in any jurisdiction where the relevant words are read or downloaded. See *Lewis v. King*, [2004] All E.R. (D) 234 (Oct.) (C.A.) (Eng.); see also *Richardson v. Schwarzenegger*, [2004] All E.R. (D) 432 (Oct.) (Q.B.) (Eng.) (relying on *Lewis* to assert jurisdiction over a libel suit arising from an article in the *Los Angeles Times* that was available online).

**Page 164:**

**At the end of note 6, add:**

The British House of Lords has specifically rejected any reliance on whether the site in question targeted viewers in a specific jurisdiction or not. According to the Lords,

it makes little sense to distinguish between one jurisdiction and another in order to decide which the defendant has “targeted”, when in truth he has “targeted” every jurisdiction where his text may be downloaded. Further, if the exercise required the ascertainment of what it was the defendant subjectively intended to “target”, it would in our judgment be liable to manipulation and uncertainty, and much more likely to diminish than enhance the interests of justice.

*Lewis v. King*, [2004] All E.R. (D) 234 (Oct.) (C.A.) (Eng.), at ¶ 34. Do you find this reasoning convincing? If so, is there any way for judges to devise a test that would help combat such manipulation?

## SECTION D. THE POWER TO ENFORCE

### 1. Judgment Recognition and the Power of Persuasion

Page 174:

Following note 4, insert a new note:

4A. The district court's opinion was subsequently reversed by the United States Court of Appeals for the Ninth Circuit. *See Yahoo!, Inc. v. La Ligue Contre le Racisme et l'Antisémitisme*, 379 F. 3d 1120 (9th Cir. 2004). The appeals court declined to reach the First Amendment question, however, instead ruling only that the district court did not have proper jurisdiction over the French defendants because the defendants had insufficient contact with California. Although this decision was framed as a matter of jurisdiction, it can also be thought of as a ripeness question. After all, part of the reason the French complainants had insufficient contact with California is that they had chosen not to seek an enforcement order in the United States. Thus, dismissing for lack of jurisdiction was functionally equivalent to preventing Yahoo!'s claim from going forward unless and until a U.S. court is actually asked to enforce the French order. At that point, the controversy would become ripe for review, and at the same time jurisdiction would presumably no longer be a problem.



## Chapter Five

---

---

### PROBLEMS OF “PUBLIC” VERSUS “PRIVATE” REGULATION

---

#### SECTION C. GOVERNMENT REGULATION VERSUS PRIVATE FILTERING

##### 1. Government Regulation of Sexually Explicit Speech

**Page 429:**

**In the last paragraph of note 7, delete “On remand . . . First Amendment scrutiny?” and add:**

On remand, the Third Circuit again struck down the statute as unconstitutional. *See American Civil Liberties Union v. Ashcroft*, 322 F.3d 240 (3d Cir. 2003). The Supreme Court subsequently affirmed, though the Court suggested that the Third Circuit had unnecessarily construed various statutory definitions not considered by the district court. *Ashcroft v. American Civil Liberties Union*, 542 U.S. \_\_\_, 124 S. Ct. 2783, 2791 (2004). Accordingly, the Court limited itself to ruling that the district court did not abuse its discretion in granting preliminary injunctive relief. Central to the Court’s conclusion was the fact that the government had failed, at least at the preliminary injunction stage, to show why use of blocking and filtering software would not constitute a less restrictive alternative to COPA. The Court, however, left open the possibility that the district court could conclude, after a full trial on the merits, “that COPA is the least restrictive alternative available to accomplish Congress’ goal.” *Id.* at \_\_\_, 124 S. Ct. at 2795. The next section discusses filtering and blocking technology in greater detail.

## 2. Filtering Sexually Explicit Speech

**Page 437:**

**Following note 3, insert a new note:**

3A. Assuming the government cannot require use of filtering software, is it appropriate for courts to evaluate the availability of filtering technology in examining government attempts to restrict sexually explicit speech? In *Ashcroft v. American Civil Liberties Union*, 542 U.S. \_\_\_, 124 S. Ct. 2783 (2004), the Supreme Court held that a district court did not abuse its discretion in granting preliminary injunctive relief where the government had failed to demonstrate that use of filtering and blocking software did not constitute a less restrictive alternative to the Child Online Protection Act. In dissent, Justice Breyer objected to the Court's treatment of filtering software as an "alternative" to regulation rather than merely as a feature of the technological landscape: "Conceptually speaking, the presence of filtering software is not an *alternative* legislative approach to the problem of protecting children from exposure to commercial pornography. Rather, it is part of the status quo, *i.e.*, the backdrop against which Congress enacted the present statute." 542 U.S. at \_\_\_, 124 S. Ct. at 2801 (Breyer, J., dissenting). Which approach is correct?

**Page 441:**

**At the end of note 2, add:**

In either case, of course, the measure may raise significant constitutional concerns: If the ISPs cannot comply with the statute without blocking material that is not child pornography, the statute may burden protected speech. A district court so concluded in *Center for Democracy and Technology v. Pappert*, 337 F. Supp. 2d 606 (E.D. Pa. 2004).

## Chapter Six

---

# PROBLEMS OF SPEAKERS AND CONDUITS

---

## SECTION B. OPEN ACCESS

Page 491:

Following citation to *Brand X Internet Servs. v. FCC*, add:

, *cert. granted*, \_\_\_ U.S. \_\_\_ (Dec. 3, 2004),

## SECTION C. THE ROLE OF INTERNET SERVICE PROVIDERS AND OTHER INTERMEDIARIES

### 2. Copyright Liability

Page 525:

Following note 1, insert a new note:

1A. On the issue of direct infringement, note the district court's observation that Netcom designed a system "that *automatically* and uniformly creates temporary copies of all data sent through it." (Emphasis added.) Is a provider entitled to immunity from direct infringement even when its processes are not fully automatic? In *CoStar v. LoopNet, Inc.*, 373 F.3d 544 (4th Cir. 2004), the court considered whether LoopNet was liable for direct infringement when it allowed real estate brokers to post descriptions of real estate automatically on its web site, but cursorily reviewed all photographs before permitting them to appear on the site so as to avoid obvious copyright infringement. The court held that LoopNet's conduct with respect to the

photographs “does not amount to ‘copying,’ nor does it add volition to LoopNet’s involvement in storing the copy.” *Id.* at 556. One judge dissented on this point, arguing that LoopNet’s “non-passive, volitional conduct” made the *Netcom* defense unavailable. *Id.* at 557 (Gregory, J., dissenting). How would a choice between the majority and dissenting approaches affect a provider’s incentives to prevent infringing material from being posted on or transmitted by its system?

**Page 529:**

**Prior to note 1, insert a new note:**

0. Does *Netcom*’s holding that a provider is not liable for direct infringement when a subscriber posts infringing material survive enactment of the DMCA? In *ALS Scan v. RemarQ Communities, Inc.*, 239 F.3d 619, 622 (4th Cir. 2001), the U.S. Court of Appeals for the Fourth Circuit characterized the DMCA as a “codification” of *Netcom*, thus implying that a provider failing to satisfy the DMCA’s requirements could not rely on *Netcom*’s reasoning to defend against a claim of direct infringement. The same court later held that, whether or not it qualifies for one of the DMCA’s safe harbors, a provider is not liable for direct infringement when passively storing material at the direction of users, because “Congress intended the DMCA’s safe harbor for ISPs to be a floor, not a ceiling, of protection.” *CoStar v. LoopNet*, 373 F.3d 544, 555 (4th Cir. 2004).

**Page 529:**

**Following note 1, insert a new note:**

1A. How does the scope of immunity for a service provider under subsection 512(a) differ from that under subsection 512(c)? In light of those differences, the question whether a service provider’s actions can be characterized as providing “intermediate and transient storage of . . . material in the course of . . . transmitting, routing, or providing connections” under subsection 512(a) or as providing “storage at the direction of the user of material that resides on a system or network controlled by or operated for the service provider” under subsection 512(c) is likely to be crucial. Consider a provider that makes a USENET feed available to its subscribers and stores files related to USENET postings for 14 days. Should a court assess the service provider’s immunity under subsection 512(a) or subsection 512(c)? See *Ellison v. Robertson*, 357 F.3d 1072 (9th Cir. 2004) (remanding for consideration of whether service provider met threshold requirements of subsection 512(i), but concluding that district court otherwise appropriately found that subsection 512(a) applied).

Pages 540–49:

Omit *Metro-Goldwyn-Mayer* and accompanying notes and add:

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

United States Court of Appeals for the Ninth Circuit, 2004  
380 F.3d 1154, *cert. granted*, \_\_ U.S. \_\_ (Dec. 10, 2004)

THOMAS, Circuit Judge.

This appeal presents the question of whether distributors of peer-to-peer file-sharing computer networking software may be held contributorily or vicariously liable for copyright infringements by users. Under the circumstances presented by this case, we conclude that the defendants are not liable for contributory and vicarious copyright infringement and affirm the district court’s partial grant of summary judgment.

I. BACKGROUND

From the advent of the player piano, every new means of reproducing sound has struck a dissonant chord with musical copyright owners, often resulting in federal litigation. This appeal is the latest reprise of that recurring conflict, and one of a continuing series of lawsuits between the recording industry and distributors of file-sharing computer software.

The plaintiffs in the consolidated cases (“Copyright Owners”) are songwriters, music publishers, and motion picture studios who, by their own description, “own or control the vast majority of copyrighted motion pictures and sound recordings in the United States.” Defendants Grokster Ltd. and StreamCast Networks, Inc. (“Software Distributors”) are companies that freely distribute software that allows users to share computer files with each other, including digitized music and motion pictures. The Copyright Owners allege that over 90% of the files exchanged through use of the “peer-to-peer” file-sharing software offered by the Software Distributors involves copyrighted material, 70% of which is owned by the Copyright Owners. Thus, the Copyright Owners argue, the Software Distributors are liable for vicarious and contributory copyright infringement pursuant to 17 U.S.C. §§ 501-13 (2000), for which the Copyright Owners are entitled to monetary and injunctive relief. The district court granted the Software Distributors partial summary judgment as to liability arising from present activities and certified the resolved questions for appeal pursuant to Fed. R. Civ. P. 54(b).

To analyze the legal issues properly, a rudimentary understanding of the peer-to-peer file-sharing software at issue is required—particularly because peer-to-peer file sharing differs from typical internet use. In a routine internet transaction, a user will connect via the internet with a website to obtain information or transact business. In computer terms, the personal computer used by the consumer is considered the “client” and the computer that hosts the web page is the “server.” The client is obtaining information from a centralized source, namely the server.

In a peer-to-peer distribution network, the information available for access does not reside on a central server. No one computer contains all of the information that is available to all of the users. Rather, each computer makes information available to every other computer in the peer-to-peer network. In other words, in a peer-to-peer network, each computer is both a server and a client.

Because the information is decentralized in a peer-to-peer network, the software must provide some method of cataloguing the available information so that users may access it. The software operates by connecting, via the internet, to other users of the same or similar software. At any given moment, the network consists of other users of similar or the same software online at that time. Thus, an index of files available for sharing is a critical component of peer-to-peer file-sharing networks.

At present, there are three different methods of indexing: (1) a centralized indexing system, maintaining a list of available files on one or more centralized servers; (2) a completely decentralized indexing system, in which each computer maintains a list of files available on that computer only; and (3) a “supernode” system, in which a select number of computers act as indexing servers.

The first Napster system employed a proprietary centralized indexing software architecture in which a collective index of available files was maintained on servers it owned and operated. A user who was seeking to obtain a digital copy of a recording would transmit a search request to the Napster server, the software would conduct a text search of the centralized index for matching files, and the search results would be transmitted to the requesting user. If the results showed that another Napster user was logged on to the Napster server and offering to share the requested recording, the requesting user could then connect directly with the offering user and download the music file.

Under a decentralized index peer-to-peer file-sharing model, each user maintains an index of only those files that the user wishes to make available to other network users. Under this model, the software broadcasts a search request to all the computers on the network and a search of the individual index files is conducted, with the collective results routed back to the requesting computer. This model is employed by the Gnutella software system and is the type of architecture now used by defendant StreamCast. Gnutella is open-source software, meaning that the source code is either in the public domain or is copyrighted and distributed under an open-source license that allows modification of the software, subject to some restrictions.

The third type of peer-to-peer file-sharing network at present is the “supernode” model, in which a number of select computers on the network are designated as indexing servers. The user initiating a file search connects with the most easily accessible supernode, which conducts the search of its index and supplies the user with the results. Any computer on the network could function as a supernode if it met the technical requirements, such as processing speed. The “supernode” architecture was

developed by KaZaa BV, a Dutch company, and licensed under the name of “FastTrack” technology.

Both Grokster and StreamCast initially used the FastTrack technology. However, StreamCast had a licensing dispute with KaZaa, and now uses its own branded “Morpheus” version of the open-source Gnutella code. StreamCast users connect to other users of Gnutella-based peer-to-peer file-sharing software. Both Grokster and StreamCast distribute their separate softwares free of charge. Once downloaded onto a user’s computer, the software enables the user to participate in the respective peer-to-peer file-sharing networks over the internet.

Users of the software share digital audio, video, picture, and text files. Some of the files are copyrighted and shared without authorization, others are not copyrighted (such as public domain works), and still others are copyrighted, but the copyright owners have authorized software users in peer-to-peer file-sharing networks to distribute their work. The Copyright Owners assert, without serious contest by the Software Distributors, that the vast majority of the files are exchanged illegally in violation of copyright law.

## II. ANALYSIS

\* \* \*

### A. *Contributory Copyright Infringement*

The three elements required to prove a defendant liable under the theory of contributory copyright infringement are: (1) direct infringement by a primary infringer, (2) knowledge of the infringement, and (3) material contribution to the infringement. The element of direct infringement is undisputed in this case.

#### 1. *Knowledge*

Any examination of contributory copyright infringement must be guided by the seminal case of *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984) (“*Sony-Betamax*”). In *Sony-Betamax*, the Supreme Court held that the sale of video tape recorders could not give rise to contributory copyright infringement liability even though the defendant knew the machines were being used to commit infringement. In analyzing the contours of contributory copyright infringement, the Supreme Court drew on the “staple article of commerce” doctrine from patent law. Under that doctrine, it would be sufficient to defeat a claim of contributory copyright infringement if the defendant showed that the product was “capable of substantial” or “commercially significant noninfringing uses.” In applying this doctrine, the Court found that because Sony’s Betamax video tape recorder was capable of commercially significant noninfringing uses, constructive knowledge of the infringing activity could not be imputed from the fact that Sony knew the recorders, as a general matter, could be used for infringement. *Id.* at 442.

In [*A & M Records v. Napster*, 239 F.3d 1004 (9th Cir. 2001) (“*Napster I*”)], we construed *Sony-Betamax* to apply to the knowledge element of

contributory copyright infringement. *Napster I* held that if a defendant could show that its product was capable of substantial or commercially significant noninfringing uses, then constructive knowledge of the infringement could not be imputed. Rather, if substantial noninfringing use was shown, the copyright owner would be required to show that the defendant had reasonable knowledge of specific infringing files. *Id.* at 1027; see also *A & M Records v. Napster*, 284 F.3d 1091, 1095-96 (9th Cir. 2002) (“*Napster II*”).

Thus, in order to analyze the required element of knowledge of infringement, we must first determine what level of knowledge to require. If the product at issue is not capable of substantial or commercially significant noninfringing uses, then the copyright owner need only show that the defendant had constructive knowledge of the infringement. On the other hand, if the product at issue *is* capable of substantial or commercially significant noninfringing uses, then the copyright owner must demonstrate that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement.

In this case, the district court found it undisputed that the software distributed by each defendant was capable of substantial noninfringing uses. A careful examination of the record indicates that there is no genuine issue of material fact as to noninfringing use. Indeed, the Software Distributors submitted numerous declarations by persons who permit their work to be distributed via the software, or who use the software to distribute public domain works. \* \* \* Indeed, the record indicates that thousands of \* \* \* musical groups have authorized free distribution of their music through the internet. In addition to music, the software has been used to share thousands of public domain literary works made available through Project Gutenberg as well as historic public domain films released by the Prelinger Archive. In short, from the evidence presented, the district court quite correctly concluded that the software was capable of substantial noninfringing uses and, therefore, that the *Sony-Betamax* doctrine applied.

The Copyright Owners submitted no evidence that could contradict these declarations. Rather, the Copyright Owners argue that the evidence establishes that the vast majority of the software use is for copyright infringement. This argument misapprehends the *Sony* standard as construed in *Napster I*, which emphasized that in order for limitations imposed by *Sony* to apply, a product need only be *capable* of substantial noninfringing uses. *Napster I*, 239 F.3d at 1021.<sup>9</sup> In this case, the Software

---

9. We are mindful that the Seventh Circuit has read *Sony*'s substantial noninfringing use standard differently. *In re Aimster Copyright Litig.*, 334 F.3d 643, 651 (7th Cir. 2003). It determined that an important additional factor is how “probable” the noninfringing uses of a product are. *Id.* at 653. The Copyright Owners urge us to adopt the *Aimster* rationale. However, *Aimster* is premised specifically on a fundamental disagreement with *Napster I*'s reading of *Sony-Betamax*. We are not free to reject our own Circuit's binding precedent. Even if we were free to do so, we do not read *Sony-Betamax*'s holding as narrowly as does the Seventh Circuit. Regardless, it is not clear that application of the *Aimster* rationale would

Distributors have not only shown that their products are capable of substantial noninfringing uses, but that the uses have commercial viability. Thus, applying *Napster I*, *Napster II*, and *Sony-Betamax* to the record, the district court correctly concluded that the Software Distributors had established that their products were capable of substantial or commercially significant noninfringing uses. Therefore, the district correctly reasoned, the Software Distributors could not be held liable for constructive knowledge of infringement, and the Copyright Owners were required to show that the Software Distributors had reasonable knowledge of specific infringement to satisfy the threshold knowledge requirement.

Having determined that the “reasonable knowledge of specific infringement” requirement applies here, we must then decide whether the Copyright Owners have raised sufficient genuine issues of material fact to satisfy that higher standard. As the district court correctly concluded, the time at which such knowledge is obtained is significant. Because contributory copyright infringement requires knowledge *and* material contribution, the Copyright Owners were required to establish that the Software Distributors had “specific knowledge of infringement at a time at which they contribute[d] to the infringement, and [ ] fail[ed] to act upon that information.” As the district court correctly observed, and as we explain further in our discussion of material contribution, “Plaintiffs’ notices of infringing conduct are irrelevant,” because “they arrive when Defendants do nothing to facilitate, and cannot do anything to stop, the alleged infringement” of specific copyrighted content.

In the context of this case, the software design is of great import. As we have discussed, the software at issue in *Napster I* and *Napster II* employed a centralized set of servers that maintained an index of available files. In contrast, under both StreamCast’s decentralized, Gnutella-type network and Grokster’s quasi-decentralized, supernode, KaZaa-type network, no central index is maintained. Indeed, at present, neither StreamCast nor Grokster maintains control over index files. As the district court observed, even if the Software Distributors “closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or no interruption.”

Therefore, we agree with the district court that the Software Distributors were entitled to partial summary judgment on the element of knowledge.

## 2. *Material Contribution*

We also agree with the district court that with respect to their current software distribution and related activities, defendants do not materially contribute to copyright infringement.

---

assist the Copyright Owners here. Implicit in the *Aimster* analysis is that a finding of substantial noninfringing use, including potential use, would be fatal to a contributory infringement claim, regardless of the level of knowledge possessed by the defendant. In *Aimster*, no evidence was tendered of any noninfringing product use.

In *Napster I*, we found material contribution after reciting the district court's factual finding that "Napster is an integrated service." 239 F.3d at 1022. We "agree[d] that Napster provides the site and facilities for direct infringement." *Id.* (internal quotation marks omitted). \* \* \* While material contribution can be established through provision of site and facilities for infringement, followed by a failure to stop specific instances of infringement once knowledge of those infringements is acquired, the Software Distributors have not provided the site and facilities for infringement in the first place. If the Software Distributors were true access providers, failure to disable that access after acquiring specific knowledge of a user's infringement might be material contribution. *Religious Technology Ctr. v. Netcom On-Line Communications Servs.*, 907 F. Supp. 1361, 1375 (N.D. Cal. 1995). Or, if the Software Distributors stored files or indices, failure to delete the offending files or offending index listings might be material contribution. *Napster I*, 239 F.3d at 1022. However, the Software Distributors here are not access providers, and they do not provide file storage and index maintenance. Rather, it is the users of the software who, by connecting to each other over the internet, create the network and provide the access. "Failure" to alter software located on another's computer is simply not akin to the failure to delete a filename from one's own computer, to the failure to cancel the registration name and password of a particular user from one's user list, or to the failure to make modifications to software on one's own computer.

The Copyright Owners have not provided evidence that defendants materially contribute in any other manner. StreamCast maintains an [Extensible Markup Language ("XML")] file from which user software periodically retrieves parameters. These values may include the addresses of websites where lists of active users are maintained. The owner of the FastTrack software, Sharman, maintains root nodes containing lists of currently active supernodes to which users can connect. Both defendants also communicate with users incidentally, but not to facilitate infringement. All of these activities are too incidental to any direct copyright infringement to constitute material contribution. No infringing files or lists of infringing files are hosted by defendants, and the defendants do not regulate or provide access.

While Grokster and StreamCast in particular may seek to be the "next Napster," the peer-to-peer file-sharing technology at issue is not simply a tool engineered to get around the holdings of *Napster I* and *Napster II*. The technology has numerous other uses, significantly reducing the distribution costs of public domain and permissively shared art and speech, as well as reducing the centralized control of that distribution. Especially in light of the fact that liability for contributory copyright infringement does not require proof of any direct financial gain from the infringement, we decline to expand contributory copyright liability in the manner that the Copyright Owners request.

B. *Vicarious Copyright Infringement*

Three elements are required to prove a defendant vicariously liable for copyright infringement: (1) direct infringement by a primary party, (2) a direct financial benefit to the defendant, and (3) the right and ability to supervise the infringers. *Napster I*, 239 F.3d at 1022. “Vicarious copyright liability is an ‘outgrowth’ of respondeat superior,” imposing liability on those with a sufficiently supervisory relationship to the direct infringer. *Id.* (citing *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996)). In *Napster I*, we held that *Sony-Betamax* “has no application to . . . vicarious copyright infringement” because the issue of vicarious liability was “not before the Supreme Court” in that case. *Id.*

The elements of direct infringement and a direct financial benefit, via advertising revenue, are undisputed in this case.

1. *Right and Ability To Supervise*

We agree with the district court that there is no issue of material fact as to whether defendants have the right and ability to supervise the direct infringers in this case. Allocation of liability in vicarious copyright liability cases has developed from a historical distinction between the paradigmatic “dance hall operator” and “landlord” defendants. *Cherry Auction*, 76 F.3d at 262. The dance hall operator is liable, while the landlord escapes liability, because the dance hall operator has the right and ability to supervise infringing conduct while the landlord does not. *Id.* Thus, the “right and ability to supervise” describes a relationship between the defendant and the direct infringer.

A salient characteristic of that relationship often, though not always, is a formal licensing agreement between the defendant and the direct infringer. Indeed, *Napster I* found especially important the fact that Napster had an express policy reserving the right to block infringers’ access for any reason. 239 F.3d at 1023 (“[A]bility to block infringers’ access to a particular environment for any reason whatsoever is evidence of the right and ability to supervise.”).

In *Cherry Auction*, we held that the right and ability to supervise existed where a swap meet operator reserved the right to terminate vendors for any reason, promoted the swap meet, controlled access by customers, patrolled the meet, and could control direct infringers through its rules and regulations. 76 F.3d at 262-63. Similarly in *Napster I*, we found Napster had the right and ability to supervise Napster users because it controlled the central indices of files, users were required to register with Napster, and access to the system depended on the validity of a user’s registration. 239 F.3d at 1011-12, 1023-24.

It does not appear from any of the evidence in the record that either of the defendants has the ability to block access to individual users. Grokster nominally reserves the right to terminate access, while StreamCast does not maintain a licensing agreement with persons who download Morpheus. However, given the lack of a registration and log-in

process, even Grokster has no ability to actually terminate access to filesharing functions, absent a mandatory software upgrade to all users that the particular user refuses, or IP address-blocking attempts.<sup>12</sup> It is also clear that none of the communication between defendants and users provides a point of access for filtering or searching for infringing files, since infringing material and index information do not pass through defendants' computers.

In the case of StreamCast, shutting down its XML file altogether would not prevent anyone from using the Gnutella network. In the case of Grokster, its licensing agreement with KaZaa/Sharman does not give it the ability to mandate that root nodes be shut down. Moreover, the alleged ability to shut down operations altogether is more akin to the ability to close down an entire swap meet or stop distributing software altogether, rather than the ability to exclude individual participants, a practice of policing aisles, an ability to block individual users directly at the point of log-in, or an ability to delete individual filenames from one's own computer. See *Napster I*, 239 F.3d at 1023-24; *Cherry Auction*, 76 F.3d at 261-62. The sort of monitoring and supervisory relationship that has supported vicarious liability in the past is completely absent in this case.

The district court here found that unlike Napster, Grokster and StreamCast do not operate and design an "integrated service" which they monitor and control. We agree. The nature of the relationship between Grokster and StreamCast and their users is significantly different from the nature of the relationship between a swap meet operator and its participants, or prior versions of Napster and its users, since Grokster and StreamCast are more truly decentralized, peer-to-peer file-sharing networks.

The district court correctly characterized the Copyright Owners' evidence of the right and ability to supervise as little more than a contention that "the software itself could be altered to prevent users from sharing copyrighted files." In arguing that this ability constitutes evidence of the right and ability to supervise, the Copyright Owners confuse the right and ability to supervise with the strong duty imposed on entities that have already been determined to be liable for vicarious copyright infringement; such entities have an obligation to exercise their policing powers to the fullest extent, which in Napster's case included implementation of new filtering mechanisms. *Napster II*, 284 F.3d at 1098 ("The tolerance standard announced *applies only to copyrighted works which Plaintiffs have properly noticed* as required by the modified preliminary injunction. That is, Napster must do everything feasible to block files from its system which contain noticed copyrighted works.") (emphasis added). But the potential duty a district court may place on a vicariously liable defendant is not the

---

<sup>12</sup> IP address-blocking will not be effective against a user who, like most persons, does not have a permanent IP address, but is rather assigned one each time he connects to the Internet.

same as the “ability” contemplated by the “right and ability to supervise” test. Moreover, a duty to alter software and files located on one’s own computer system is quite different in kind from a duty to alter software located on another person’s computer. We agree with the district court that possibilities for upgrading software located on another person’s computer are irrelevant to determining whether vicarious liability exists. *See also Napster I*, 239 F.3d at 1024 (“Napster’s reserved ‘right and ability’ to police is cabined by the system’s current architecture.”).

C. *Turning a “Blind Eye” to Infringement*

The Copyright Owners finally argue that Grokster and StreamCast should not be able to escape vicarious liability by turning a “blind eye” to the infringement of their users, and that “[t]urning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability.” *Napster I*, 239 F.3d at 1023. If the Software Distributors had a right and ability to control and supervise that they proactively refused to exercise, such refusal would not absolve them of liability. *See id.* However, although that rhetoric has occasionally been employed in describing vicarious copyright infringement, there is no separate “blind eye” theory or element of vicarious liability that exists independently of the traditional elements of liability. Thus, this theory is subsumed into the Copyright Owners’ claim for vicarious copyright infringement and necessarily fails for the same reasons.

III.

Resolution of these issues does not end the case. As the district court clearly stated, its decision was limited to the specific software in use at the time of the district court decision. The Copyright Owners have also sought relief based on previous versions of the software, which contain significant—and perhaps crucial—differences from the software at issue. We express no opinion as to those issues.

As to the question at hand, the district court’s grant of partial summary judgment to the Software Distributors is clearly dictated by applicable precedent. The Copyright Owners urge a re-examination of the law in the light of what they believe to be proper public policy, expanding exponentially the reach of the doctrines of contributory and vicarious copyright infringement. Not only would such a renovation conflict with binding precedent, it would be unwise. Doubtless, taking that step would satisfy the Copyright Owners’ immediate economic aims. However, it would also alter general copyright law in profound ways with unknown ultimate consequences outside the present context.

Further, as we have observed, we live in a quicksilver technological environment with courts ill-suited to fix the flow of internet innovation. The introduction of new technology is always disruptive to old markets, and particularly to those copyright owners whose works are sold through well-established distribution mechanisms. Yet, history has shown that time and market forces often provide equilibrium in balancing interests, whether the new technology be a player piano, a copier, a tape recorder, a video

recorder, a personal computer, a karaoke machine, or an MP3 player. Thus, it is prudent for courts to exercise caution before restructuring liability theories for the purpose of addressing specific market abuses, despite their apparent present magnitude.

Indeed, the Supreme Court has admonished us to leave such matters to Congress. In *Sony-Betamax*, the Court spoke quite clearly about the role of Congress in applying copyright law to new technologies. As the Supreme Court stated in that case, “The direction of Art. I is that *Congress* shall have the power to promote the progress of science and the useful arts. When, as here, the Constitution is permissive, the sign of how far Congress has chosen to go can come only from Congress.” 464 U.S. at 456.

In this case, the district court correctly applied applicable law and properly declined the invitation to alter it. We affirm the district court, and remand for resolution of the remaining issues.

### ***Notes and Questions***

1. How does the Ninth Circuit distinguish this case from its decision in *Napster*? Why does the Supreme Court’s rule in *Sony* help the defendants in this case, while it did not help Napster?

2. The *Napster* court ruled “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.” Why is that not the case here? After all, the defendants apparently received many notices from the plaintiffs, identifying various specific infringements. Thus, even if the defendants had no knowledge of infringement *prior* to receiving the notices, they certainly had knowledge *afterwards*. Why isn’t this knowledge enough to render the defendants liable?

3. To what degree does the court rely solely on whether a centralized service exists? Should this be relevant? If users are infringing copyright by employing a particular technology, should it matter whether or not they access a centralized “site and facility” to do so? On the other hand, if the defendants had been deemed liable for infringement in this case, how would you distinguish video cassette recorders or photocopy machines, which also facilitate decentralized copying?

4. If you were counsel for the plaintiffs, what steps would you advise your clients to take, given the decision in *Grokster*? In the conclusion, the court suggests that the plaintiffs’ only recourse is to seek legislative change. How would you draft a statute to hold services like Grokster and StreamCast liable for copyright infringement without running afoul of *Sony* or opening the door to overly broad liability? Assuming such legislation could be crafted, do you think it would be a good idea? How would it be enforced?

5. Consider the relationship between legal and technological regulation discussed in Chapter Four. Does the result in this case indicate that new technology can always foil legal rules?

## Chapter Seven

---

---

### PROBLEMS OF CONTROL OVER INFORMATION

---

#### SECTION C. CONTROL OF ACCESS TO DATA AND NETWORK RESOURCES

**Page 645:**

**Replace the second paragraph of note 3 with the following:**

In *Kelly*, the Ninth Circuit ultimately withdrew the opinion discussed by the *Ticketmaster* court. In its new opinion, the Ninth Circuit avoided resolving whether Arriba Soft's linking to or framing of the full-sized images violated Kelly's copyright, concluding that, since the parties did not request summary judgment on that issue, the district court erred in granting summary judgment to Arriba Soft. *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 822 (9th Cir. 2003).