

**FALL 2003 SUPPLEMENT TO**

**CYBERLAW**

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

**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 JULY 15, 2003**



# Table of Contents

---

	Page	
TABLE OF CASES .....	v	
TABLE OF AUTHORITIES .....	vii	
 <b>Chapter Two: Problems of Metaphor and Analogy:</b>		
<b>Introductory Case Studies</b> .....	1	
A. Trespass to Chattels in Cyberspace .....	1	
<i>Notes and Questions</i> .....	1	
<i>Intel Corporation v. Hamidi</i> .....	3	
<i>Notes and Questions</i> .....	16	
B. Consumer Confusion and Online Trademarks .....	18	
 <b>Chapter Three: Problems of Geography and Sovereignty</b> .....		19
A. The Theoretical Debate .....	19	
D. The Power to Enforce .....	19	
1. Judgment Recognition and the Power of Persuasion .....	19	
 <b>Chapter Four: Problems of Legal versus Technological Regulation</b> .....		21
B. Law, Technology, and Regulatory Outcomes .....	21	
2. Copyright Protection .....	21	
b. Digital Rights Management Systems .....	21	
 <b>Chapter Five: Problems of “Public” versus “Private” Regulation</b> .....		23
B. The Role of Private Regulatory Entities in Cyberspace .....	23	
3. Corporate Self-Help .....	23	
C. Government Regulation versus Private Filtering .....	24	
3. Use of Filtering Technology in Public Settings .....	24	
<i>United States v. American Library Association</i> .....	24	
<i>Notes and Questions</i> .....	36	
 <b>Chapter Six: Problems of Speakers and Conduits</b> .....		37
C. The Role of Internet Service Providers and Other Intermediaries .....	37	
1. Liability for Defamatory Content .....	37	
2. Copyright Liability .....	37	

<b>Chapter Seven: Problems of Individual Autonomy and Commercial Control</b> .....	39
B. Control of Personal Information .....	39
2. The Legal Framework .....	39
b. Online Profiling and the Collection and Use of Personal Data	39
<i>In re DoubleClick, Inc. Privacy Litigation</i> .....	39
<i>Notes and Questions</i> .....	49
<i>In re Pharmatrak, Inc. Privacy Litigation</i> .....	50
<i>Notes and Questions</i> .....	57
C. Controlling Access to Data .....	57
<i>Ticketmaster Corporation v. Tickets.com, Inc.</i> .....	57
<i>Kelly v. Arriba Soft Corp.</i> .....	63
<i>Notes and Questions</i> .....	67

## Table of Cases

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

- A & M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001), 66
- American Library Ass'n v. United States, 201 F. Supp. 2d 401 (E.D. Pa. 2002), 24
- Arkansas Ed. Television Comm'n v. Forbes, 523 U. S. 666 (1998), 25, 26
- Batzel v. Smith, \_\_\_ F.3d \_\_\_, 2003 WL 21453358 (9th Cir. 2003), 37
- Board of Comm'rs, Wabaunsee Cty. v. Umbehr, 518 U. S. 668 (1996), 28
- Board of Ed., Island Trees Union Free School Dist. No. 26 v. Pico, 457 U.S. 853 (1982), 34, 35
- Campbell v. Acuff-Rose Music, 510 U.S. 569 (1994), 61
- Chance v. Avenue A, 165 F. Supp. 2d 1153 (W.D. Wash. 2001), 49, 54, 55
- CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997), 6, 11, 17
- Cornelius v. NAACP Legal Defense & Ed. Fund, Inc., 473 U. S. 788 (1985), 26
- Dr. Seuss Enters., L.P. v. Penguin Books USA, 109 F.3d 1394 (9th Cir. 1997), 65
- eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000), 6, 12
- Feist Publications v. Rural Tel. Serv. Co., 499 U.S. 340 (1991), 60
- Gilday v. Dubois, 124 F.3d 277 (1st Cir. 1997), 55
- Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990), 54
- In re Aimster Copyright Litigation, \_\_\_ F.3d \_\_\_, 2003 WL 21488143 (7th Cir. 2003), 38
- In re DoubleClick Inc. Privacy Litigation**, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), 39, 54, 55
- In re Intuit Privacy Litigation, 138 F. Supp. 2d 1272 (C.D. Cal. 2001), 50
- In re Pharmatrak, Inc. Privacy Litigation, 220 F. Supp. 2d 4 (D. Mass. 2002), 50
- In re Pharmatrak, Inc. Privacy Litigation**, 329 F.3d 9 (1st Cir. 2003), 50
- Intel Corporation v. Hamidi**, 2003 WL 21488209 (Cal. 2003), 3
- International Soc. for Krishna Consciousness, Inc. v. Lee, 505 U. S. 672 (1992), 26
- J.K. Harris & Co. v. Kassel, 253 F. Supp. 2d 1120 (N.D. Cal. 2003), 18
- Kelly v. Arriba Soft Corp.**, \_\_\_ F.3d \_\_\_, 2003 WL 21518002 (9th Cir. 2003), 63
- Kelly v. Arriba Soft Corp., 280 F.3d 934 (9th Cir. 2002), 61, 62
- National Endowment for Arts v. Finley, 524 U. S. 569 (1998), 25, 32
- Noah v. AOL Time Warner, Inc., \_\_\_ F. Supp. 2d \_\_\_, 2003 WL 21135701 (E.D. Va. 2003), 23
- Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000), 6
- Reno v. American Civil Liberties Union, 521 U. S. 844 (1997), 32
- Rosenberger v. Rector and Visitors of Univ. of Va., 515 U. S. 819 (1995), 26
- Rossi v. Motion Picture Ass'n of Am., Civ. 0200239 (D. Hawaii, Apr. 29, 2003), 38
- Rust v. Sullivan, 500 U. S. 173 (1991), 28, 32
- Sega Enters. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992), 60
- Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000), 60
- South Dakota v. Dole, 483 U. S. 203 (1987), 25
- Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994), 56
- Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 54 Cal. Rptr. 2d 468 (1996), 4, 6, 14
- Ticketmaster Corp. v. Tickets.com, Inc., 2000 WL 1887522 (C.D. Cal. 2000), 6
- Ticketmaster Corporation v. Tickets.com, Inc.**, 2003 U.S. Dist. LEXIS 6483 (C.D. Cal. 2003), 57
- United States v. American Library Association**, 123 S. Ct. 2297 (2003), 24
- Watchtower Bible & Tract Soc. of N. Y., Inc. v. Village of Stratton, 536 U.S. 150 (2002), 31
- Worldwide Church of God v. Philadelphia Church of God, 227 F.3d 1110 (9th Cir. 2000), 66



## Table of Authorities

---

---

- |   |  |
|---|--|
| Bell, Tom W., <i>Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright's Fair Use Doctrine</i> , 76 N.C. L. Rev. 557 (1998), 2 | Heller, Michael A., <i>The Tragedy of the Anticommons: Property in the Transition from Marx to Markets</i> , 111 Harv. L. Rev. 621 (1998), 2 |
| Burk, Dan L., <i>The Trouble with Trespass</i> , 4 J. Small & Emerging Bus. L. 27 (2000), 2, 16   | Prosser and Keeton, <i>Torts</i> (5th ed. 1984), 4<br>Restatement (Second) of Torts (1965), 4, 5, 11, 13                                     |
| Cardozo, Benjamin, <i>The Nature of the Judicial Process</i> (1921), 16   | Sorkin, Andrew Ross, <i>Software Bullet is Sought to Kill Musical Piracy</i> , <i>New York Times</i> , May 4, 2003, at 1, 21                 |
| Cohen, Julie E., <i>Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management"</i> , 97 Mich. L. Rev. 462 (1998), 2                       | Warner, Richard, <i>Border Disputes: Trespass to Chattels on the Internet</i> , 47 Vill. L. Rev. 117 (2002), 2                               |
| Hardy, I. Trotter, <i>Property (and Copyright) in Cyberspace</i> , 1996 U. Chi. Legal F. 217, 2   |  |



## Chapter Two

---

---

# PROBLEMS OF METAPHOR AND ANALOGY: INTRODUCTORY CASE STUDIES

---

### SECTION A. TRESPASS TO CHATTELS IN CYBERSPACE

Pages 24-40:

Reverse the order of *Intel Corporation v. Hamidi* and *eBay v. Bidder's Edge, Inc.* and insert the following notes and questions after *Bidder's Edge*:

#### *Notes and Questions*

1. Assume Denise's Drugs is a "brick and mortar" drug store. Dave's Discount Pharmacy opens a discount store next door. Each week, an employee of Dave's enters Denise's, walks around the store, and writes down the prices Denise's charges for various items, perhaps purchasing a couple of items as well so as to appear like a regular customer. Armed with this information, Dave's offers many of the same products at a lower price. If Denise finds out about this practice, can she sue Dave on a trespass theory? What if all Dave does is stand on the sidewalk and look at the sale prices displayed in Denise's window? Are these useful analogies to the online context? Why or why not?

2. What about the argument that Internet users have an interest in low-cost, worldwide communication and unimpeded access to information? Indeed, such low-cost communication and open access to information arguably have been critical to the rapid growth and vitality of both the Internet and e-commerce. Does a decision such as *Bidder's Edge* impede this sort of access to information? If so, what is the appropriate solution?

3. Consider arguments based on economics and market efficiency. Some have argued that decisions such as the one in *Bidder's Edge*, by impeding access to information, make the market less efficient:

The Internet has the potential to approximate a perfectly efficient information medium because it can allow buyers to cheaply, easily and

quickly search for items they want. The role of product comparison sites is critical to the benefits of e-commerce. Aggregators of product and price information, “shop-bots” that automate the price comparison process, and comparative product evaluators like Consumer Reports and its online equivalents all reduce transactions costs and improve competition by helping consumers get fast, cheap and accurate information about products and prices. Because search technology and so-called “shop-bots” allow consumers to automatically identify goods in which they are interested, the match between sellers and buyers can approach perfect efficiency. In addition, because there is no practical limit to the number of servers that can be connected to the Internet, there is virtually no upper limit to the number of sellers that can participate in what promises to be near-perfect competition.

Brief of Amici Curiae Mark A. Lemley *et al.*, *eBay, Inc. v. Bidder’s Edge, Inc.*, No. 00-15995 (9th Cir. filed June 22, 2000).

On the other hand, granting sites like eBay the right to exclude aggregators does not necessarily mean that such aggregators will vanish from the scene; rather, they may negotiate license agreements with the auction sites and then continue to offer the same information to consumers. Indeed, some have argued that, by creating a clear property right to exclude unauthorized users from a web site, the law would facilitate efficient bargaining between the parties. *See, e.g.*, Richard Warner, *Border Disputes: Trespass to Chattels on the Internet*, 47 VILL. L. REV. 117, 136-38 (2002). Nevertheless, can you think of any possible barriers to the creation of such licensing agreements?

4. What about search engines? They use crawlers of various sorts to search web sites and index content. Should they be required to negotiate licenses with every site they index? If not, can you think of how you might craft an exception to the rule enunciated in *Bidder’s Edge*? Might the law infer an implied license to index unless sites specifically disclaim permission? Would such an implied license scheme be practical?

5. Is there a danger of “over-propertization” of the online environment? Michael Heller has written of the dilemma that arises when property rights are so finely divided that it becomes essentially impossible to conduct any type of business. *See* Michael A. Heller, *The Tragedy of the Anticommons: Property in the Transition from Marx to Markets*, 111 HARV. L. REV. 621 (1998). In such highly fragmented property systems, myriad licenses must be obtained from many, many owners before any type of large-scale project can be undertaken. The transaction costs involved in locating the rights holders and negotiating separate licenses with each of them might tend to deter complex endeavors. *See* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 49 (2000).

On the other hand, it might be possible to reduce these transaction costs online through automation. Users would then be able electronically to enter into licensing negotiations with the owners of ever more finely-grained levels of network property and then keep track of all the agreements through digital certificates. *See* Trotter Hardy, *Property (and Copyright) in Cyberspace*, 1996 U. CHI. LEGAL F. 217; *see also* Tom W. Bell, *Fair Use vs. Fared Use: The Impact of Automated Rights Management on Copyright’s Fair Use Doctrine*, 76 N.C. L. REV. 557 (1998). *But see* Julie E. Cohen, *Lochner in Cyberspace: The*

*New Economic Orthodoxy of "Rights Management"*, 97 MICH. L. REV. 462 (1998) (offering a critique of this view).

Are either of these visions convincing?

6. Should online trespass actions be based only on the harms arising from increased traffic over computer lines? For example, if company X has greater server capacity than company Y, should it be less able to pursue a trespass action? If not, then are these trespass actions more concerned simply with the right of those who own computer servers or web sites to control access rather than fears about damage to computer systems?

7. In addition to trespass, web site owners have also tried to control access by arguing that unauthorized hypertext links violate copyright. These claims raise similar sorts of concerns. We will consider such claims in Chapter Seven.

Insert the following, to replace *Hamidi*:

### **Intel Corporation v. Hamidi**

Supreme Court of California, 2003  
2003 WL 21488209

WERDEGAR, J.

Intel Corporation (Intel) maintains an electronic mail system, connected to the Internet, through which messages between employees and those outside the company can be sent and received, and permits its employees to make reasonable nonbusiness use of this system. On six occasions over almost two years, Kourosh Kenneth Hamidi, a former Intel employee, sent e-mails criticizing Intel's employment practices to numerous current employees on Intel's electronic mail system. \* \* \* The messages criticized Intel's employment practices, warned employees of the dangers those practices posed to their careers, suggested employees consider moving to other companies, solicited employees' participation in [an organization Hamidi and others founded, Former and Current Employees of Intel (FACE-Intel)], and urged employees to inform themselves further by visiting FACE-Intel's Web site. The messages stated that recipients could, by notifying the sender of their wishes, be removed from FACE-Intel's mailing list; Hamidi did not subsequently send messages to anyone who requested removal.

Each message was sent to thousands of addresses (as many as 35,000 according to FACE-Intel's Web site), though some messages were blocked by Intel before reaching employees. Intel's attempt to block internal transmission of the messages succeeded only in part; Hamidi later admitted he evaded blocking efforts by using different sending computers. When Intel, in March 1998, demanded in writing that Hamidi and FACE-Intel stop sending e-mails to Intel's computer system, Hamidi asserted the organization had a right to communicate with willing Intel employees; he sent a new mass mailing in September 1998.

The summary judgment record contains no evidence Hamidi breached Intel's computer security in order to obtain the recipient addresses for his messages; indeed, internal Intel memoranda show the company's management concluded no security breach had occurred. Hamidi stated he created the recipient address list using an Intel directory on a floppy disk anonymously sent to him. Nor is there any evidence that the receipt or internal distribution of Hamidi's electronic messages damaged Intel's computer system or slowed or impaired its functioning. Intel did present uncontradicted evidence, however, that many employee recipients asked a company official to stop the messages and that staff time was consumed in attempts to block further messages from FACE-Intel. According to the FACE-Intel Web site, moreover, the messages had prompted discussions between "[e]xcited and nervous managers" and the company's human resources department.

Intel sued Hamidi and FACE-Intel, pleading \* \* \* trespass to chattels \* \* \* . [The trial court] granted Intel's motion for summary judgment, permanently enjoining Hamidi, FACE-Intel, and their agents from sending unsolicited e-mail to addresses on Intel's computer systems. \* \* \* The Court of Appeal, with one justice dissenting, affirmed the grant of injunctive relief. The majority took the view that the use of or intermeddling with another's personal property is actionable as a trespass to chattels without proof of any actual injury to the personal property; even if Intel could not show any damages resulting from Hamidi's sending of messages, it showed he was disrupting its business by using its property and therefore is entitled to injunctive relief based on a theory of trespass to chattels. The dissenting justice warned that the majority's application of the trespass to chattels tort to unsolicited electronic mail that causes no harm to the private computer system that receives it would expand the tort of trespass to chattel in untold ways and to unanticipated circumstances.

We granted Hamidi's petition for review.

#### DISCUSSION

##### I. Current California Tort Law

\* \* \* [T]he tort of trespass to chattels allows recovery for interferences with possession of personal property not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered. PROSSER & KEETON, TORTS § 14, at 85-86 (5th ed. 1984). Though not amounting to conversion, the defendant's interference must, to be actionable, have caused some injury to the chattel or to the plaintiff's rights in it. Under California law, trespass to chattels lies where an intentional interference with the possession of personal property *has proximately caused injury*. *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal. App. 4th 1559, 1566, 54 Cal. Rptr. 2d 468 (1996) (italics added).

The Restatement, too, makes clear that some actual injury must have occurred in order for a trespass to chattels to be actionable. Under section 218 of the Restatement Second of Torts, dispossession alone, without

further damages, is actionable, *see id.*, par. (a) & com. d, at 420-421, but other forms of interference require some additional harm to the personal property or the possessor's interests in it. *Id.*, pars. (b)-(d).

The interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor. *Therefore, one who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is harmful to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel, or if the possessor is deprived of the use of the chattel for a substantial time, or some other legally protected interest of the possessor is affected as stated in Clause (c).* Sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.

*Id.*, com. e, at 421-422 (italics added). \* \* \*

The dispositive issue in this case, therefore, is whether the undisputed facts demonstrate Hamidi's actions caused or threatened to cause damage to Intel's computer system, or injury to its rights in that personal property, such as to entitle Intel to judgment as a matter of law. To review, the undisputed evidence revealed no actual or threatened damage to Intel's computer hardware or software and no interference with its ordinary and intended operation. Intel was not dispossessed of its computers, nor did Hamidi's messages prevent Intel from using its computers for any measurable length of time. Intel presented no evidence its system was slowed or otherwise impaired by the burden of delivering Hamidi's electronic messages. Nor was there any evidence transmission of the messages imposed any marginal cost on the operation of Intel's computers. In sum, no evidence suggested that in sending messages through Intel's Internet connections and internal computer system Hamidi used the system in any manner in which it was not intended to function or impaired the system in any way. \* \* \*

Relying on a line of decisions, most from federal district courts, applying the tort of trespass to chattels to various types of unwanted electronic contact between computers, Intel contends that, while its computers were not damaged by receiving Hamidi's messages, its interest in the physical condition, quality or value of the computers was harmed. We disagree. The cited line of decisions does not persuade us that the mere sending of electronic communications that assertedly cause injury only because of their contents constitutes an actionable trespass to a computer system through which the messages are transmitted. Rather, the decisions finding electronic contact to be a trespass to computer systems have

generally involved some actual or threatened interference with the computers' functioning.

In *Thrifty-Tel, Inc. v. Bezenek, supra*, 46 Cal. App. 4th at 1566-1567, 54 Cal. Rptr. 2d 468 (*Thrifty-Tel*), the California Court of Appeal held that evidence of automated searching of a telephone carrier's system for authorization codes supported a cause of action for trespass to chattels. The defendant's automated dialing program overburdened the [plaintiff's] system, denying some subscribers access to phone lines, *Thrifty-Tel, supra*, 46 Cal. App. 4th at 1564, 54 Cal. Rptr. 2d 468, showing the requisite injury.

Following *Thrifty-Tel*, a series of federal district court decisions held that sending [unsolicited commercial e-mail (UCE)] through an ISP's equipment may constitute trespass to the ISP's computer system. \* \* \* In each of these spamming cases, the plaintiff showed, or was prepared to show, some interference with the efficient functioning of its computer system. In [the leading case, *CompuServe, Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1021-1023 (S.D. Ohio 1997), for example], the plaintiff ISP's mail equipment monitor stated that mass UCE mailings, especially from nonexistent addresses such as those used by the defendant, placed a tremendous burden on the ISP's equipment, using disk space and drain[ing] the processing power, making those resources unavailable to serve subscribers. \* \* \*

Building on the spamming cases, in particular *CompuServe*, three even more recent district court decisions addressed whether unauthorized robotic data collection from a company's publicly accessible Web site is a trespass on the company's computer system. *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1069-1072 (N.D. Cal. 2000) (*eBay*); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 248-251 (S.D.N.Y. 2000); *Ticketmaster Corp. v. Tickets.com, Inc.*, 2000 WL 1887522, at \*4 (C.D. Cal. 2000). The two district courts that found such automated data collection to constitute a trespass relied, in part, on the deleterious impact this activity could have, especially if replicated by other searchers, on the functioning of a Web site's computer equipment.

In the leading case, *eBay*, the defendant Bidder's Edge (BE), operating an auction aggregation site, accessed the eBay Web site about 100,000 times per day, accounting for between 1 and 2 percent of the information requests received by eBay and a slightly smaller percentage of the data transferred by eBay. The district court rejected eBay's claim that it was entitled to injunctive relief because of the defendant's unauthorized presence alone, or because of the incremental cost the defendant had imposed on operation of the eBay site, but found sufficient proof of *threatened* harm in the potential for others to imitate the defendant's activity: "If BE's activity is allowed to continue unchecked, it would encourage other auction aggregators to engage in similar recursive searching of the eBay system such that eBay would suffer irreparable harm from reduced system performance, system unavailability, or data losses." 100 F. Supp. 2d at 1066. \* \* \* Here, \* \* \* Intel has demonstrated neither any appreciable effect on the operation of

its computer system from Hamidi's messages, nor any likelihood that Hamidi's actions will be replicated by others if found not to constitute a trespass.

That Intel does not claim the type of functional impact that spammers and robots have been alleged to cause is not surprising in light of the differences between Hamidi's activities and those of a commercial enterprise that uses sheer quantity of messages as its communications strategy. Though Hamidi sent thousands of copies of the same message on six occasions over 21 months, that number is minuscule compared to the amounts of mail sent by commercial operations. \* \* \*

Intel relies on language in the *eBay* decision suggesting that unauthorized use of another's chattel is actionable even without any showing of injury: "Even if, as [defendant] BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property." *eBay*, 100 F. Supp. 2d at 1071. But as the *eBay* court went on immediately to find that the defendant's conduct, if widely replicated, *would* likely impair the functioning of the plaintiff's system, we do not read the quoted remarks as expressing the court's complete view of the issue. In isolation, moreover, they would not be a correct statement of California or general American law on this point. While one may have no *right* temporarily to use another's personal property, such use is actionable as a trespass only if it has proximately caused injury. \* \* \* That Hamidi's messages temporarily used some portion of the Intel computers' processors or storage is, therefore, not enough; Intel must, but does not, demonstrate some measurable loss from the use of its computer system.

In addition to impairment of system functionality, *CompuServe* and its progeny also refer to the ISP's loss of business reputation and customer goodwill, resulting from the inconvenience and cost that spam causes to its members, as harm to the ISP's legally protected interests in its personal property. Intel argues that its own interest in employee productivity, assertedly disrupted by Hamidi's messages, is a comparable protected interest in its computer system. We disagree.

Whether the economic injuries identified in *CompuServe* were properly considered injuries to the ISP's possessory interest in its personal property, the type of property interest the tort is primarily intended to protect, has been questioned. \* \* \* But even if the loss of goodwill identified in *CompuServe* were the type of injury that would give rise to a trespass to chattels claim under California law, Intel's position would not follow, for Intel's claimed injury has even less connection to its personal property than did *CompuServe*'s.

*CompuServe*'s customers were annoyed because the system was inundated with unsolicited commercial messages, making its use for personal communication more difficult and costly. Their complaint, which allegedly led some to cancel their *CompuServe* service, was about *the*

*functioning of CompuServe's electronic mail service.* Intel's workers, in contrast, were allegedly distracted from their work not because of the frequency or quantity of Hamidi's messages, but because of assertions and opinions the messages conveyed. Intel's complaint is thus about *the contents of the messages* rather than the functioning of the company's e-mail system. Even accepting *CompuServe's* economic injury rationale, therefore, Intel's position represents a further extension of the trespass to chattels tort, fictionally recharacterizing the allegedly injurious effect of a communication's *contents* on recipients as an impairment to the device which transmitted the message. \* \* \*

While unwelcome communications, electronic or otherwise, can cause a variety of injuries to economic relations, reputation and emotions, those interests are protected by other branches of tort law; in order to address them, we need not create a fiction of injury to the communication system. Nor may Intel appropriately assert a *property* interest in its employees' time. \* \* \* Whatever interest Intel may have in preventing its employees from receiving disruptive communications, it is not an interest in personal property, and trespass to chattels is therefore not an action that will lie to protect it. Nor, finally, can the fact Intel staff spent time attempting to block Hamidi's messages be bootstrapped into an injury to Intel's possessory interest in its computers. To quote, again, from the dissenting opinion in the Court of Appeal: "[I]t is circular to premise the damage element of a tort solely upon the steps taken to prevent the damage." \* \* \*

Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other companies and individuals. That some communications would, because of their contents, be unwelcome to Intel management was virtually inevitable. Hamidi did nothing but use the e-mail system for its intended purpose—to communicate with employees. The system worked as designed, delivering the messages without any physical or functional harm or disruption. These occasional transmissions cannot reasonably be viewed as impairing the quality or value of Intel's computer system. We conclude, therefore, that Intel has not presented undisputed facts demonstrating an injury to its personal property, or to its legal interest in that property, that support, under California tort law, an action for trespass to chattels.

## II. Proposed Extension of California Tort Law

We next consider whether California common law should be *extended* to cover, as a trespass to chattels, an otherwise harmless electronic communication whose contents are objectionable. We decline to so expand California law. Intel, of course, was not the recipient of Hamidi's messages, but rather the owner and possessor of computer servers used to relay the messages, and it bases this tort action on that ownership and possession. The property rule proposed is a rigid one, under which the sender of an

electronic message would be strictly liable to the owner of equipment through which the communication passes—here, Intel—for any consequential injury flowing from the *contents* of the communication. The arguments of amici curiae and academic writers on this topic, discussed below, leave us highly doubtful whether creation of such a rigid property rule would be wise.

Writing on behalf of several industry groups appearing as amici curiae, Professor Richard A. Epstein of the University of Chicago urges us to excuse the required showing of injury to personal property in cases of unauthorized electronic contact between computers, extending the rules of trespass to real property to all interactive Web sites and servers. The court is thus urged to recognize, for owners of a particular species of personal property, computer servers, the same interest in inviolability as is generally accorded a possessor of land. In effect, Professor Epstein suggests that a company's server should be its castle, upon which any unauthorized intrusion, however harmless, is a trespass.

Epstein's argument derives, in part, from the familiar metaphor of the Internet as a physical space, reflected in much of the language that has been used to describe it: cyberspace, the information superhighway, e-mail addresses, and the like. Of course, \* \* \* [a] major component of the Internet is the World Wide Web, a descriptive term suggesting neither personal nor real property, and cyberspace itself has come to be known by the oxymoronic phrase virtual reality, which would suggest that any real property located in cyberspace must be virtually real property. Metaphor is a two-edged sword. \* \* \*<sup>7</sup>

More substantively, Professor Epstein argues that a rule of computer server inviolability will, through the formation or extension of a market in computer-to-computer access, create the right social result. In most circumstances, he predicts, companies with computers on the Internet will continue to authorize transmission of information through e-mail, Web site searching, and page linking because they benefit by that open access. When a Web site owner does deny access to a particular sending, searching, or

---

7. The tort law discussion in Justice Brown's dissenting opinion similarly suffers from an overreliance on metaphor and analogy. Attempting to find an actionable trespass, Justice Brown analyzes Intel's e-mail system as comparable to the exterior of an automobile, a plot of land, the interior of an automobile, a toothbrush, a head of livestock, and a mooring buoy, while Hamidi is characterized as a vandal damaging a school building or a prankster unplugging and moving employees' computers. These colorful analogies tend to obscure the plain fact that this case involves communications equipment, used by defendant to communicate. Intel's e-mail system was equipment designed for speedy communication between employees and the outside world; Hamidi communicated with Intel employees over that system in a manner entirely consistent with its design; and Intel objected not because of an offense against the integrity or dignity of its computers, but because the communications themselves affected employee-recipients in a manner Intel found undesirable. The proposal that we extend trespass to chattels to cover any communication that the owner of the communications equipment considers annoying or distracting raises, moreover, concerns about control over the flow of information and views that would not be presented by, for example, an injunction against chasing another's cattle or sleeping in her car.

linking computer, a system of simple one-on-one negotiations will arise to provide the necessary individual licenses.

Other scholars are less optimistic about such a complete propertization of the Internet. Professor Mark Lemley of the University of California, Berkeley, writing on behalf of an amici curiae group of professors of intellectual property and computer law, observes that under a property rule of server inviolability, each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel. The consequence for e-mail could be a substantial reduction in the freedom of electronic communication, as the owner of each computer through which an electronic message passes could impose its own limitations on message content or source. \* \* \*

We discuss this debate among the amici curiae and academic writers only to note its existence and contours, not to attempt its resolution. Creating an absolute property right to exclude undesired communications from one's e-mail and Web servers might help force spammers to internalize the costs they impose on ISP's and their customers. But such a property rule might also create substantial new costs, to e-mail and e-commerce users and to society generally, in lost ease and openness of communication and in lost network benefits. In light of the unresolved controversy, we would be acting rashly to adopt a rule treating computer servers as real property for purposes of trespass law. \* \* \* We therefore decline to create an exception \* \* \* to the general rule that a trespass to chattels is not actionable if it does not involve actual or threatened injury to the personal property or to the possessor's legally protected interest in the personal property. No such injury having been shown on the undisputed facts, Intel was not entitled to summary judgment in its favor.

We concur: KENNARD, MORENO, JJ., and PERREN, J.

[Concurring opinion of Justice Kennard omitted.]

Dissenting Opinion of BROWN, J.

Candidate A finds the vehicles that candidate B has provided for his campaign workers, and A spray paints the water soluble message, "Fight corruption, vote for A" on the bumpers. The majority's reasoning would find that notwithstanding the time it takes the workers to remove the paint and the expense they incur in altering the bumpers to prevent further unwanted messages, candidate B does not deserve an injunction unless the paint is so heavy that it reduces the cars' gas mileage or otherwise depreciates the cars' market value. Furthermore, candidate B has an obligation to permit the paint's display, because the cars are driven by workers and not B personally, because B allows his workers to use the cars to pick up their lunch or retrieve their children from school, or because the bumpers display B's own slogans. I disagree.

Intel has invested millions of dollars to develop and maintain a computer system. It did this not to act as a public forum but to enhance the

productivity of its employees. Kourosh Kenneth Hamidi sent as many as 200,000 e-mail messages to Intel employees. The time required to review and delete Hamidi's messages diverted employees from productive tasks and undermined the utility of the computer system. "There may . . . be situations in which the value to the owner of a particular type of chattel may be impaired by dealing with it in a manner that does not affect its physical condition." REST. 2D TORTS, § 218, com. h, at 422. This is such a case. \* \* \*

The majority refuses to protect Intel's interest in maintaining the integrity of its own system, contending that: (1) Hamidi's mailings did not physically injure the system; (2) Intel receives many unwanted messages, of which Hamidi's are but a small fraction; (3) Intel must have contemplated that it would receive some unwanted messages; and (4) Hamidi used the e-mail system for its intended purpose, to communicate with employees. \* \* \*

Intel had the right to exclude the unwanted speaker from its property, which Hamidi does not dispute; he does not argue that he has a to right force unwanted messages on Intel. The instant case thus turns on the question of whether Intel deserves a remedy for the continuing violation of its rights. I believe it does, and as numerous cases have demonstrated, an injunction to prevent a trespass to chattels is an appropriate means of enforcement. \* \* \*

#### HARMLESS TRESPASSES TO CHATTELS MAY BE PREVENTED

\* \* \* Regardless of whether property is real or personal, it is beyond dispute that an individual has the right to have his personal property free from interference. There is some division among authorities regarding the available remedy, particularly whether a harmless trespass supports a claim for nominal damages. \* \* \* But the Restatement expressly refutes defendant's assertion that only real property is inviolable. From the modest distinction holding that only victims of a trespass to land may profit in the form of damages exceeding actual harm, defendant offers the position that only trespasses to land may be *prevented*. The law is to the contrary; numerous cases have authorized injunctive relief to safeguard the inviolability of personal property. \* \* \*

The *CompuServe* court \* \* \* authoriz[ed] an injunction to prevent the delivery of unwanted e-mail messages. The majority summarily distinguishes *CompuServe* and its progeny by noting "there the plaintiff showed, or was prepared to show, some interference with the efficient functioning of its computer system." But although *CompuServe* did note the impairment imposed by the defendant's unsolicited e-mail, this was not part of its holding. Just before beginning its analysis, the court summarized its ruling without mentioning impairment. "[T]his Court holds that where defendants engaged in a course of conduct of transmitting a substantial volume of electronic data in the form of unsolicited e-mail to plaintiff's proprietary computer equipment, where defendants continued such practice after repeated demands to cease and desist, and where defendants

deliberately evaded plaintiff's affirmative efforts to protect its computer equipment from such use, plaintiff has a viable claim for trespass to personal property and is entitled to injunctive relief to protect its property." *CompuServe*, 962 F. Supp. at 1017. The cited criteria apply fully to Hamidi's conduct. Likewise, the conclusion of *CompuServe*'s analysis fully applies here: "Defendants' intentional use of plaintiff's proprietary computer equipment exceeds plaintiff's consent and, indeed, continued after repeated demands that defendants cease. Such use is an actionable trespass to plaintiff's chattel." *Id.* at p. 1027.

Post-*CompuServe* case law has emphasized that unauthorized use of another's property establishes a trespass, even without a showing of physical damage. "Although eBay appears unlikely to be able to show a substantial interference at this time, such a showing is not required. Conduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel." *eBay, Inc. v. Bidder's Edge, Inc.* 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000). While the *eBay* decision could be read to require an interference that was more than negligible, \* \* \* this Court concludes that *eBay*, in fact, imposes no such requirement. Ultimately, the court in that case concluded that the defendant's conduct was sufficient to establish a cause of action for trespass not because the interference was "substantial" but simply because the defendant's conduct amounted to "use" of Plaintiff's computer. An intruder is not entitled to sleep in his neighbor's car, even if he does not chip the paint.

Hamidi concedes Intel's legal entitlement to block the unwanted messages. The problem is that although Intel has resorted to the cyberspace version of reasonable force, it has so far been unsuccessful in determining how to resist the unwanted use of its system. Thus, while Intel has the legal right to exclude Hamidi from its system, it does not have the physical ability. It *may* forbid Hamidi's use, but it *can* not prevent it.

To the majority, Hamidi's ability to outwit Intel's cyber defenses justifies denial of Intel's claim to exclusive use of its property. Under this reasoning, it is not right but might that determines the extent of a party's possessory interest. Although the world often works this way, the legal system should not.

#### INTEL SUFFERED INJURY

Even if *CompuServe* and its progeny deem injury a prerequisite for injunctive relief, such injury occurred here. Intel suffered not merely an affront to its dignitary interest in ownership but tangible economic loss. Furthermore, notwithstanding the calendar's doubts, it is entirely consistent with the Restatement and case law to recognize a property interest in the subjective utility of one's property. Finally, case law further recognizes as actionable the loss that occurs when one party maintains property for its own use and another party uses it, even if the property does not suffer damage as a result.

*Intel Suffered Economic Loss*

Courts have recognized the tangible costs imposed by the receipt of unsolicited bulk e-mail (UBE). \* \* \* Although Hamidi claims he sent only six e-mails, he sent them to between 8,000 and 35,000 employees, thus sending from 48,000 to 210,000 messages. Since it is the effect on Intel that is determinative, it is the number of messages received, not sent, that matters. In any event, Hamidi *sent* between 48,000 and 210,000 messages; the six refers only to the number of distinct texts Hamidi sent. Even if it takes little time to determine the author of a message and then delete it, this process, multiplied hundreds of thousands of times, amounts to a substantial loss of employee time, and thus work product. If Intel received 200,000 messages, and each one could be skimmed and deleted in six seconds, it would take approximately 333 hours, or 42 business days, to delete them all. In other words, if Intel hired an employee to remove all unwanted mail, it would take that individual two entire months to finish.

*Intel's Injury is Properly Related to the Chattel*

The majority does not dispute that Intel suffered a loss of work product as a matter of fact, so much as it denies that this loss may constitute the requisite injury as a matter of law. According to the majority, the reduced utility of the chattel to the owner does not constitute a sufficiently cognizable injury, which exists only where the chattel itself suffers injury, i.e., its market value falls. The Restatement and related case law are to the contrary.

The Restatement recognizes that the measure of impairment may be subjective; a cognizable injury may occur not only when the trespass reduces the chattel's market value but also when the trespass affects its value to the owner. \* \* \* *CompuServe* is in accord, as it observed how a bundle of unwanted messages decreased the utility of the server. Here, Intel maintains a possessory interest in the efficient and productive use of its system—which it spends millions of dollars to acquire and maintain. Hamidi's conduct has impaired the system's optimal functioning for Intel's business purposes. As the Restatement supports liability where "harm is caused to . . . some . . . thing in which the possessor has a legally protected interest," REST. 2D TORTS, § 218, subd. (d), Hamidi has trespassed upon Intel's chattel.

*The Unlawful Use of Another's Property is a Trespass, Regardless of Its Effect on the Property's Utility to the Owner*

Finally, even if Hamidi's interference did not affect the server's utility to Intel, it would still amount to a trespass. Intel has poured millions of dollars into a resource that Hamidi has now appropriated for his own use. \* \* \* Intel has paid for thousands of computers, as well as the costs of maintaining a server. \* \* \* Hamidi has \* \* \* acted as a free rider in enjoying the use of not only Intel's computer system but the extra storage capacity needed to accommodate his messages. \* \* \* Hamidi has thus unlawfully shifted the costs of his speaking to Intel.

Moreover, even such free ridership is not necessary to establish a trespass to chattels. \* \* \* “[N]either injury to the trespasser nor benefit to the trespasser is an element of trespass to chattel. [T]respass to chattel has evolved considerably from its original common law application—concerning the asportation of another’s tangible property—to include even the unauthorized *use* of personal property.” *Thrifty Tel, supra*, 46 Cal. App. 4th at 1566, 54 Cal. Rptr. 2d 468.

As in those cases in which courts have granted injunctions to prevent the delivery of unwanted mail, paper or electronic, Intel is not attempting to *profit* from its trespass action by receiving nominal damages. Rather, it seeks an injunction to *prevent* further trespass. Moreover, Intel suffered the requisite injury by losing a great deal of work product, a harm properly related to the property itself, as well as the money it spent in maintaining the system, which Hamidi wrongfully expropriated.

#### CONCLUSION

Those who have contempt for grubby commerce and reverence for the rarified heights of intellectual discourse may applaud today’s decision, but even the flow of ideas will be curtailed if the right to exclude is denied. \* \* \* The principles of both personal liberty and social utility should counsel us to usher the common law of property into the digital age.

#### Dissenting Opinion by MOSK, J.

In my view, the repeated transmission of bulk e-mails by appellant \* \* \* Hamidi to the employees of Intel \* \* \* on its proprietary confidential e-mail lists, despite Intel’s demand that he cease such activities, constituted an actionable trespass to chattels. The majority fail to distinguish open communication in the public commons of the Internet from unauthorized intermeddling on a private, proprietary intranet. Hamidi is not communicating in the equivalent of a town square or of an unsolicited junk mailing through the United States Postal Service. His action, in crossing from the public Internet into a private intranet, is more like intruding into a private office mailroom, commandeering the mail cart, and dropping off unwanted broadsides on 30,000 desks. Because Intel’s security measures have been circumvented by Hamidi, the majority leave Intel, which has exercised all reasonable self-help efforts, with no recourse unless he causes a malfunction or systems crash. Hamidi’s repeated intrusions did more than merely prompt[ ] discussions between “[e]xcited and nervous managers” and the company’s human resource department; they also constituted a misappropriation of Intel’s private computer system contrary to its intended use and against Intel’s wishes.

The law of trespass to chattels has not universally been limited to physical damage. I believe it is entirely consistent to apply that legal theory to these circumstances—that is, when a proprietary computer system is being used contrary to its owner’s purposes and expressed desires, and self-help has been ineffective. Intel correctly expects protection from an intruder who misuses its proprietary system, its nonpublic directories, and

its supposedly controlled connection to the Internet to achieve his bulk mailing objectives—incidentally, without even having to pay postage. \* \* \*

Hamidi's deliberate and continued intermeddling, and threatened intermeddling, with Intel's proprietary computer system for his own purposes that were hostile to Intel, certainly impaired the quality and value of the system as an internal business device for Intel and forced Intel to incur costs to try to maintain the security and integrity of its server—efforts that proved ineffective. These included costs incurred to mitigate injuries that had already occurred. It is not a matter of bootstrapp[ing] to consider those costs a damage to Intel. Indeed, part of the value of the proprietary computer system is the ability to exclude intermeddlers from entering it for significant uses that are disruptive to its owner's business operations.

If Intel, a large business with thousands of former employees, is unable to prevent Hamidi from continued intermeddling, it is not unlikely that other outsiders who obtain access to its proprietary electronic mail addresses would engage in similar conduct, further reducing the value of, and perhaps debilitating, the computer system as a business productivity mechanism. Employees understand that a firewall is in place and expect that the messages they receive are from senders permitted by the corporation. Violation of this expectation increases the internal disruption caused by messages that circumvent the company's attempt to exclude them. The time that each employee must spend to evaluate, delete or respond to the message, when added up, constitutes an amount of compensated time that translates to quantifiable financial damage.

All of these costs to protect the integrity of the computer system and to deal with the disruptive effects of the transmissions and the expenditures attributable to employee time, constitute damages sufficient to establish the existence of a trespass to chattels, even if the computer system was not overburdened to the point of a crash by the bulk electronic mail. \* \* \*

The majority suggest that Intel is not entitled to injunctive relief because it chose to allow its employees access to e-mail through the Internet and because Hamidi has apparently told employees that he will remove them from his mailing list if they so request. They overlook the proprietary nature of Intel's intranet system; Intel's system is not merely a conduit for messages to its employees. As the owner of the computer system, it is Intel's request that Hamidi stop that must be respected. The fact that, like most large businesses, Intel's intranet includes external e-mail access for essential business purposes does not logically mean, as the majority suggest, that Intel has forfeited the right to determine who has access to its system. Its intranet is not the equivalent of a common carrier or public communications licensee that would be subject to requirements to provide service and access. Just as Intel can, and does, regulate the use of its computer system by its employees, it should be entitled to control its use by outsiders and to seek injunctive relief when self-help fails. \* \* \*

As discussed above, I believe that existing legal principles are adequate to support Intel's request for injunctive relief. But even if the injunction in this case amounts to an extension of the traditional tort of trespass to chattels, this is one of those cases in which, as Justice Cardozo suggested, "[t]he creative element in the judicial process finds its opportunity and power in the development of the law." CARDOZO, *NATURE OF THE JUDICIAL PROCESS* 165 (1921).

The law has evolved to meet economic, social, and scientific changes in society. The industrial revolution, mass production, and new transportation and communication systems all required the adaptation and evolution of legal doctrines.

The age of computer technology and cyberspace poses new challenges to legal principles. \* \* \* The court must now grapple with proprietary interests, privacy, and expression arising out of computer-related disputes. \* \* \* That the Legislature has dealt with some aspects of commercial unsolicited bulk e-mail should not inhibit the application of common law tort principles to deal with e-mail transgressions not covered by the legislation.

Before the computer, a person could not easily cause significant disruption to another's business or personal affairs through methods of communication without significant cost. With the computer, by a mass mailing, one person can at no cost disrupt, damage, and interfere with another's property, business, and personal interests. Here, the law should allow Intel to protect its computer-related property from the unauthorized, harmful, free use by intruders.

### *Notes and Questions*

1. The common law actions for trespass to land and trespass to chattels are distinctly different. As one commentator has pointed out:

Conflating these two types of trespass has serious consequences; they may share a common history, and even a common name, but they secure entirely different interests. Trespass to chattels exists as "the little brother of conversion." The gravamen of both actions lies in the dispossession of the property from its owner. In conversion, the dispossession is total; in trespass to chattels, the dispossession is only partial. Neither entails the interest in inviolability that attends trespass to land. Indeed, even in the context of real property, impinging ephemeral substances such as smoke, or intangibles such as sound or light, typically have been addressed under doctrines of nuisance rather than doctrines of trespass.

Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 33 (2000). Thus, as the majority points out, there is at least some question whether electronic signals sent via e-mail cause a sufficiently tangible interference to a computer system to give rise to a trespass to chattels cause of action.

2. Notice that the majority and dissenting opinions disagree both about the extent of harm Intel suffered as a result of Hamidi's e-mail and whether Intel even needs to show harm at all. What are the possible harms to Intel that the dissents identify? Why does the majority reject these allegations of harm?

3. The broader question is whether the idea of trespass should be applied to the *Hamidi* case. In what ways do you find the analogy to trespass useful? In what ways is the online context distinctively different? Do the differences render the analogy inappropriate? What about common law nuisance? Would that be a better analogy, or does it replicate the problems of trespass?

4. Notice the variety of metaphors employed by the three *Hamidi* opinions excerpted above. Are any of these metaphors useful or persuasive? Or would the justices be better off saying that this is simply a new kind of harm that tort law either should or should not protect?

5. Are there other available ways, short of legal action, for Intel to stop Hamidi? The majority appears to conclude that Intel would be free to use self-help to block Hamidi's e-mails. What kinds of "self-help" alternatives are open to Intel? How effective are these alternatives? Suppose that Intel could take a very simple action—putting one line of code into its mail server's routing program—that would make it impossible for Hamidi to get his e-mail onto that server; should that affect the court's decision about whether Intel also has a legal right of action against Hamidi?

6. Does the dissents' logic lead to the conclusion that unwanted postal mail is also a trespass? How does Justice Mosk attempt to distinguish postal mail? Is his effort convincing?

7. Is there any reason to treat e-mail differently from other forms of trespass? Can you think of specific attributes of e-mail communication that make the need to stop people like Hamidi more pressing? How about specific attributes of e-mail that make the need to stop people like Hamidi *less* pressing?

8. Why do the dissenting justices find it important that Intel created a private intranet system for its own employees and did not "open up" such a system to the public? If indeed it is important to analyze the degree to which a system is open to the public, would that mean that Bidder's Edge did *not* trespass (because eBay was open to the public)?

9. As discussed in *Hamidi*, courts have used trespass theories to enjoin the sending of unsolicited business e-mails (also known as "spam") over computer networks. For example, in *CompuServe v. Cyber Promotions*, 962 F. Supp. 1015 (S.D. Ohio 1997), CompuServe was granted an injunction preventing Cyber Promotions from sending bulk e-mail over CompuServe's system. Should Hamidi's e-mail messages be treated differently from commercial bulk e-mail? If so, is there any way to draw a useful distinction? Is the majority's effort to distinguish *CompuServe* persuasive?

10. One possible concern is that a private trespass action will permit web site operators and service providers to stifle speech. For example, if trespass can be used to clear a system of spam, one could imagine an ISP similarly deciding to clear its networks of undesirable internet web content, such as transmissions from pornographic or white supremacist web sites (or even sites espousing political views with which the CEO of the ISP disagrees). Do you think this is a problem? Or do you think such speech restrictions are

permissible because the web sites are sending electronic signals over the ISP's "private" property? Although such actions might raise free speech concerns, the First Amendment has often been interpreted to reach only governmental censorship rather than censorship by private property owners. Should cyberspace be deemed private property or has it replaced the traditional town square, making it effectively public? This issue is explored in more detail in Chapter Five.

## SECTION B. CONSUMER CONFUSION AND ONLINE TRADEMARKS

**Pages 56-57:**

**At the end of note 4, add:**

In this regard, consider the following situation. Two companies are direct business competitors. Company X repeatedly uses Company Y's trade name on its site and in metatags so that, when users run a search for Company X, Company Y's site gets prominently listed in the search results as well. If Company Y is successful at diverting business to its site in this way, is there a trademark violation? In a case raising this question, a court distinguished *Brookfield* on the grounds that the company using the competitor's trade name on its site was doing so in order to criticize that company, and there would be no way to criticize the company without using its name. See *J.K. Harris & Co. v. Kassel*, 253 F. Supp. 2d 1120 (N.D. Cal. 2003). The logic of this decision seems to imply that, if Bucci or Doughney register new domain names, but then use the words "Planned Parenthood" or "People for the Ethical Treatment of Animals" many times on their sites in order both to criticize those organizations and to divert traffic, such use might be permissible. Is this a sensible result?

## **Chapter Three**

---

---

### **PROBLEMS OF GEOGRAPHY AND SOVEREIGNTY**

---

#### **SECTION A. THE THEORETICAL DEBATE**

**Page 83:**

In the last sentence of note 6, change “expedition” to “extradition.”

#### **SECTION D. THE POWER TO ENFORCE**

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

**Page 166:**

**Add a new note 3 as follows:**

3. Recently, QWest Communications, Zündel’s U.S. internet service provider, decided to remove Zündel’s site from its service after being alerted to the controversy by the Canadian Human Rights Commission decision. Does Quest’s decision indicate that the Commission’s ruling had an attenuated form of enforcement power?



## Chapter Four

---

---

### PROBLEMS OF LEGAL VERSUS TECHNOLOGICAL REGULATION

#### SECTION B. LAW, TECHNOLOGY AND REGULATORY OUTCOMES

##### 2. Copyright Protection

##### b. Digital Rights Management Systems

Page 311:

Add note 8, as follows:

8. Regardless of the DMCA, what do you think about content providers employing technological self-help to combat online copying? For example, the music industry is currently financing the development and testing of software programs that would sabotage the computers and internet connections of people who download pirated music. *See, e.g.*, Andrew Ross Sorkin, *Software Bullet is Sought to Kill Musical Piracy*, N.Y. TIMES, at 1 (May 4, 2003). Is this an appropriate and commensurate response to online file-sharing or a problematic escalation in an unhealthy technological arms race? How, if at all, should law respond to such uses of technology?



## Chapter Five

---

---

# PROBLEMS OF “PUBLIC” VERSUS “PRIVATE” REGULATION

---

## SECTION B. THE ROLE OF PRIVATE REGULATORY ENTITIES

### 3. Corporate Self-Help

**Page 378:**

**Add a new note, in between notes 4 and 5, as follows:**

Even if AOL is not subject to the First Amendment, might federal law nevertheless require AOL either to take certain actions to control content on its service or, conversely, to refrain from censoring speech in any way? For example, assume a Muslim-American man is a frequent participant in AOL chat rooms on Islam and the Koran. Over a two-and-a-half year period, many participants in the chat room submit offensive comments to the site that harass, insult, threaten, ridicule, and slander Muslims. The man complains to AOL, but AOL refuses to exercise its authority to stop the offending practices. Can the Muslim-American sue under Title II of the Civil Rights Act of 1964, which prohibits discrimination on the basis of race, color, religion, or national origin in a “place of public accommodation”? The answer to this question turns in part on whether a chat room is deemed to be a “place of public accommodation.” Faced with this scenario, one court rejected the Title II claim, holding that, “although a chat room or other online forum might be referred to metaphorically as a ‘location’ or ‘place,’ it lacks the physical presence necessary to constitute a place of public accommodation under Title II.” *See Noah v. AOL Time Warner, Inc.*, \_\_\_ F. Supp. 2d \_\_\_, 2003 WL 21135701 (E.D. Va. 2003). This conclusion focuses on the “place-ness” of a chat room. What about the room’s “public-ness”? Is there any argument that if people are engaged in a public dialogue—no matter where it is or under whose auspices—Title II should apply? After all, wouldn’t Title II apply to a shopping mall that tolerated similar behavior?

## SECTION C. GOVERNMENT REGULATION VERSUS PRIVATE FILTERING

### 3. Use of Filtering Technology in Public Settings

Pages 440-44:

Omit *Mainstream Loudoun v. Board of Trustees of the Loudoun County Public Library (Loudoun II)*.

Page 457:

Insert after note 5:

#### **United States v. American Library Association**

Supreme Court of the United States, 2003

\_\_\_ U.S. \_\_\_, 123 S. Ct. 2297

CHIEF JUSTICE REHNQUIST announced the judgment of the Court and delivered an opinion, in which JUSTICE O’CONNOR, JUSTICE SCALIA, and JUSTICE THOMAS joined.

The District Court held that Congress had exceeded its authority under the Spending Clause because, in the court’s view, “any public library that complies with [the Children’s Internet Protection Act (CIPA)] conditions will necessarily violate the First Amendment.” *American Library Ass’n v. United States*, 201 F. Supp. 2d 401, 453 (E.D. Pa. 2002). The court acknowledged that “generally the First Amendment subjects libraries’ content-based decisions about which print materials to acquire for their collections to only rational [basis] review.” *Id.*, at 462. But it distinguished libraries’ decisions to make certain Internet material inaccessible. “The central difference,” the court stated, “is that by providing patrons with even filtered Internet access, the library permits patrons to receive speech on a virtually unlimited number of topics, from a virtually unlimited number of speakers, without attempting to restrict patrons’ access to speech that the library, in the exercise of its professional judgment, determines to be particularly valuable.” *Ibid.* Reasoning that “the provision of Internet access within a public library . . . is for use by the public . . . for expressive activity,” the court analyzed such access as a “designated public forum.” *Id.*, at 457 (citation and internal quotation marks omitted). The District Court also likened Internet access in libraries to “traditional public fora . . . such as sidewalks and parks” because it “promotes First Amendment values in an analogous manner.” *Id.*, at 466.

Based on both of these grounds, the court held that the filtering software contemplated by CIPA was a content-based restriction on access to a public forum, and was therefore subject to strict scrutiny. Applying this standard, the District Court held that, although the Government has

a compelling interest “in preventing the dissemination of obscenity, child pornography, or, in the case of minors, material harmful to minors,” *id.*, at 471, the use of software filters is not narrowly tailored to further those interests. We noted probable jurisdiction and now reverse.

Congress has wide latitude to attach conditions to the receipt of federal assistance in order to further its policy objectives. *South Dakota v. Dole*, 483 U. S. 203, 206 (1987). But Congress may not “induce” the recipient “to engage in activities that would themselves be unconstitutional.” *Id.*, at 210. To determine whether libraries would violate the First Amendment by employing the filtering software that CIPA requires, we must first examine the role of libraries in our society.

Public libraries pursue the worthy missions of facilitating learning and cultural enrichment. \* \* \* To fulfill their traditional missions, public libraries must have broad discretion to decide what material to provide to their patrons. Although they seek to provide a wide array of information, their goal has never been to provide “universal coverage.” 201 F. Supp. 2d at 421. Instead, public libraries seek to provide materials “that would be of the greatest direct benefit or interest to the community.” *Ibid.* To this end, libraries collect only those materials deemed to have “requisite and appropriate quality.” *Ibid.*

We have held in two analogous contexts that the government has broad discretion to make content-based judgments in deciding what private speech to make available to the public. In *Arkansas Ed. Television Comm’n v. Forbes*, 523 U. S. 666, 672-673 (1998), we held that public forum principles do not generally apply to a public television station’s editorial judgments regarding the private speech it presents to its viewers. “[B]road rights of access for outside speakers would be antithetical, as a general rule, to the discretion that stations and their editorial staff must exercise to fulfill their journalistic purpose and statutory obligations.” *Id.*, at 673. Recognizing a broad right of public access “would [also] risk implicating the courts in judgments that should be left to the exercise of journalistic discretion.” *Id.*, at 674.

Similarly, in *National Endowment for Arts v. Finley*, 524 U. S. 569 (1998), we upheld an art funding program that required the National Endowment for the Arts (NEA) to use content-based criteria in making funding decisions. We explained that “[a]ny content-based considerations that may be taken into account in the grant-making process are a consequence of the nature of arts funding.” *Id.*, at 585. In particular, “[t]he very assumption of the NEA is that grants will be awarded according to the ‘artistic worth of competing applicants,’ and absolute neutrality is simply inconceivable.” *Ibid.* (some internal quotation marks omitted). We expressly declined to apply forum analysis, reasoning that it would conflict with “NEA’s mandate . . . to make esthetic judgments, and the inherently content-based ‘excellence’ threshold for NEA support.” *Id.*, at 586.

The principles underlying *Forbes* and *Finley* also apply to a public library’s exercise of judgment in selecting the material it provides to its

patrons. Just as forum analysis and heightened judicial scrutiny are incompatible with the role of public television stations and the role of the NEA, they are also incompatible with the discretion that public libraries must have to fulfill their traditional missions. Public library staffs necessarily consider content in making collection decisions and enjoy broad discretion in making them.

The public forum principles on which the District Court relied are out of place in the context of this case. Internet access in public libraries is neither a “traditional” nor a “designated” public forum. See *Cornelius v. NAACP Legal Defense & Ed. Fund, Inc.*, 473 U. S. 788, 802 (1985) (describing types of forums). First, this resource—which did not exist until quite recently—has not “immemorially been held in trust for the use of the public and, time out of mind, \* \* \* been used for purposes of assembly, communication of thoughts between citizens, and discussing public questions.” *International Soc. for Krishna Consciousness, Inc. v. Lee*, 505 U. S. 672, 679 (1992) (internal quotation marks omitted). We have “rejected the view that traditional public forum status extends beyond its historic confines.” *Forbes, supra*, at 678. The doctrines surrounding traditional public forums may not be extended to situations where such history is lacking.

Nor does Internet access in a public library satisfy our definition of a “designated public forum.” To create such a forum, the government must make an affirmative choice to open up its property for use as a public forum. “The government does not create a public forum by inaction or by permitting limited discourse, but only by intentionally opening a non-traditional forum for public discourse.” *Cornelius, supra*, at 802. The District Court likened public libraries’ Internet terminals to the forum at issue in *Rosenberger v. Rector and Visitors of Univ. of Va.*, 515 U. S. 819 (1995). In *Rosenberger*, we considered the “Student Activity Fund” established by the University of Virginia that subsidized all manner of student publications except those based on religion. We held that the fund had created a limited public forum by giving public money to student groups who wished to publish, and therefore could not discriminate on the basis of viewpoint.

The situation here is very different. A public library does not acquire Internet terminals in order to create a public forum for Web publishers to express themselves, any more than it collects books in order to provide a public forum for the authors of books to speak. It provides Internet access, not to “encourage a diversity of views from private speakers,” *Rosenberger, supra*, at 834, but for the same reasons it offers other library resources: to facilitate research, learning, and recreational pursuits by furnishing materials of requisite and appropriate quality. As Congress recognized, “[t]he Internet is simply another method for making information available in a school or library.” S. Rep. No. 106-141, p. 7 (1999). It is “no more than a technological extension of the book stack.” *Ibid.*

The District Court disagreed because, whereas a library reviews and affirmatively chooses to acquire every book in its collection, it does not review every Web site that it makes available. Based on this distinction, the court reasoned that a public library enjoys less discretion in deciding which Internet materials to make available than in making book selections. We do not find this distinction constitutionally relevant. A library's failure to make quality-based judgments about all the material it furnishes from the Web does not somehow taint the judgments it does make. A library's need to exercise judgment in making collection decisions depends on its traditional role in identifying suitable and worthwhile material; it is no less entitled to play that role when it collects material from the Internet than when it collects material from any other source. Most libraries already exclude pornography from their print collections because they deem it inappropriate for inclusion. We do not subject these decisions to heightened scrutiny; it would make little sense to treat libraries' judgments to block online pornography any differently, when these judgments are made for just the same reason.

Moreover, because of the vast quantity of material on the Internet and the rapid pace at which it changes, libraries cannot possibly segregate, item by item, all the Internet material that is appropriate for inclusion from all that is not. While a library could limit its Internet collection to just those sites it found worthwhile, it could do so only at the cost of excluding an enormous amount of valuable information that it lacks the capacity to review. Given that tradeoff, it is entirely reasonable for public libraries to reject that approach and instead exclude certain categories of content, without making individualized judgments that everything they do make available has requisite and appropriate quality.

Like the District Court, the dissents fault the tendency of filtering software to "overblock"—that is, to erroneously block access to constitutionally protected speech that falls outside the categories that software users intend to block. Due to the software's limitations, "[m]any erroneously blocked [Web] pages contain content that is completely innocuous for both adults and minors, and that no rational person could conclude matches the filtering companies' category definitions, such as 'pornography' or 'sex.'" 201 F. Supp. 2d, at 449. Assuming that such erroneous blocking presents constitutional difficulties, any such concerns are dispelled by the ease with which patrons may have the filtering software disabled. When a patron encounters a blocked site, he need only ask a librarian to unblock it or (at least in the case of adults) disable the filter. As the District Court found, libraries have the capacity to permanently unblock any erroneously blocked site, and the Solicitor General stated at oral argument that a "library may . . . eliminate the filtering with respect to specific sites . . . at the request of a patron." With respect to adults, CIPA also expressly authorizes library officials to "disable" a filter altogether "to enable access for bona fide research or other lawful purposes." 20 U. S. C. §9134(f)(3) (disabling permitted for both adults and minors); 47 U. S. C. §254(h)(6)(D) (disabling permitted for adults). The Solicitor General

confirmed that a “librarian can, in response to a request from a patron, unblock the filtering mechanism altogether,” and further explained that a patron would not “have to explain . . . why he was asking a site to be unblocked or the filtering to be disabled.” The District Court viewed unblocking and disabling as inadequate because some patrons may be too embarrassed to request them. But the Constitution does not guarantee the right to acquire information at a public library without any risk of embarrassment.

Appellees urge us to affirm the District Court’s judgment on the alternative ground that CIPA imposes an unconstitutional condition on the receipt of federal assistance. Under this doctrine, “the government ‘may not deny a benefit to a person on a basis that infringes his constitutionally protected . . . freedom of speech’ even if he has no entitlement to that benefit.” *Board of Comm’rs, Wabaunsee Cty. v. Umbehr*, 518 U. S. 668, 674 (1996) (quoting *Perry v. Sindermann*, 408 U. S. 593, 597 (1972)). Appellees argue that CIPA imposes an unconstitutional condition on libraries that receive E-rate and LSTA subsidies by requiring them, as a condition on their receipt of federal funds, to surrender their First Amendment right to provide the public with access to constitutionally protected speech. The Government counters that this claim fails because Government entities do not have First Amendment rights. \* \* \*

We need not decide this question because, even assuming that appellees may assert an “unconstitutional conditions” claim, this claim would fail on the merits. Within broad limits, “when the Government appropriates public funds to establish a program it is entitled to define the limits of that program.” *Rust v. Sullivan*, 500 U. S. 173, 194 (1991). \* \* \* The E-rate and LSTA programs were intended to help public libraries fulfill their traditional role of obtaining material of requisite and appropriate quality for educational and informational purposes. Congress may certainly insist that these “public funds be spent for the purposes for which they were authorized.” *Ibid.* Especially because public libraries have traditionally excluded pornographic material from their other collections, Congress could reasonably impose a parallel limitation on its Internet assistance programs. As the use of filtering software helps to carry out these programs, it is a permissible condition under *Rust*.

JUSTICE STEVENS asserts the premise that “[a] federal statute penalizing a library for failing to install filtering software on every one of its Internet-accessible computers would unquestionably violate [the First] Amendment.” But—assuming again that public libraries have First Amendment rights—CIPA does not “penalize” libraries that choose not to install such software, or deny them the right to provide their patrons with unfiltered Internet access. Rather, CIPA simply reflects Congress’ decision not to subsidize their doing so. To the extent that libraries wish to offer unfiltered access, they are free to do so without federal assistance. “A refusal to fund protected activity, without more, cannot be equated with the imposition of a ‘penalty’ on that activity.” *Rust, supra*, at 193 (quoting *Harris v. McRae*, 448 U. S. 297, 317, n. 19 (1980)). “[A] legislature’s

decision not to subsidize the exercise of a ‘fundamental’ right does not infringe the right.” *Rust, supra*, at 193 (quoting *Regan v. Taxation With Representation of Wash.*, 461 U. S. 540, 549 (1983)). \* \* \*

Because public libraries’ use of Internet filtering software does not violate their patrons’ First Amendment rights, CIPA does not induce libraries to violate the Constitution, and is a valid exercise of Congress’ spending power. Nor does CIPA impose an unconstitutional condition on public libraries. Therefore, the judgment of the District Court for the Eastern District of Pennsylvania is

*Reversed.*

JUSTICE KENNEDY, concurring in the judgment.

If, on the request of an adult user, a librarian will unblock filtered material or disable the Internet software filter without significant delay, there is little to this case. The Government represents this is indeed the fact. \* \* \* If some libraries do not have the capacity to unblock specific Web sites or to disable the filter or if it is shown that an adult user’s election to view constitutionally protected Internet material is burdened in some other substantial way, that would be the subject for an as-applied challenge, not the facial challenge made in this case.

JUSTICE BREYER, concurring in the judgment.

In ascertaining whether the statutory provisions are constitutional, I would apply a form of heightened scrutiny, examining the statutory requirements in question with special care. The Act directly restricts the public’s receipt of information. And it does so through limitations imposed by outside bodies (here Congress) upon two critically important sources of information—the Internet as accessed via public libraries. \* \* \* For that reason, we should not examine the statute’s constitutionality as if it raised no special First Amendment concern—as if, like tax or economic regulation, the First Amendment demanded only a “rational basis” for imposing a restriction. \* \* \*

At the same time, in my view, the First Amendment does not here demand application of the most limiting constitutional approach—that of “strict scrutiny.” The statutory restriction in question is, in essence, a kind of “selection” restriction (a kind of editing). It affects the kinds and amount of materials that the library can present to its patrons. And libraries often properly engage in the selection of materials, either as a matter of necessity (*i.e.*, due to the scarcity of resources) or by design (*i.e.*, in accordance with collection development policies). To apply “strict scrutiny” to the “selection” of a library’s collection (whether carried out by public libraries themselves or by other community bodies with a traditional legal right to engage in that function) would unreasonably interfere with the discretion necessary to create, maintain, or select a library’s “collection” (broadly defined to include all the information the library makes available). That is to say, “strict scrutiny” implies too limiting and rigid a test for me to believe that the First Amendment requires it in this context.

Instead, I would examine the constitutionality of the Act’s restrictions here as the Court has examined speech-related restrictions in other contexts where circumstances call for heightened, but not “strict,” scrutiny—where, for example, complex, competing constitutional interests are potentially at issue or speech-related harm is potentially justified by unusually strong governmental interests. Typically the key question in such instances is one of proper fit. In such cases the Court has asked whether the harm to speech-related interests is disproportionate in light of both the justifications and the potential alternatives. It has considered the legitimacy of the statute’s objective, the extent to which the statute will tend to achieve that objective, whether there are other, less restrictive ways of achieving that objective, and ultimately whether the statute works speech-related harm that, in relation to that objective, is out of proportion. \* \* \*

The Act’s restrictions satisfy these constitutional demands. The Act seeks to restrict access to obscenity, child pornography, and, in respect to access by minors, material that is comparably harmful. These objectives are “legitimate,” and indeed often “compelling.” \* \* \* [T]he Act contains an important exception that limits the speech-related harm that “overblocking” might cause. As the plurality points out, the Act allows libraries to permit any adult patron access to an “overblocked” Web site; the adult patron need only ask a librarian to unblock the specific Web site or, alternatively, ask the librarian, “Please disable the entire filter.”

The Act does impose upon the patron the burden of making this request. But it is difficult to see how that burden (or any delay associated with compliance) could prove more onerous than traditional library practices associated with segregating library materials in, say, closed stacks, or with interlibrary lending practices that require patrons to make requests that are not anonymous and to wait while the librarian obtains the desired materials from elsewhere. Perhaps local library rules or practices could further restrict the ability of patrons to obtain “overblocked” Internet material. But we are not now considering any such local practices. We here consider only a facial challenge to the Act itself.

Given the comparatively small burden that the Act imposes upon the library patron seeking legitimate Internet materials, I cannot say that any speech-related harm that the Act may cause is disproportionate when considered in relation to the Act’s legitimate objectives. I therefore agree with the plurality that the statute does not violate the First Amendment, and I concur in the judgment.

JUSTICE STEVENS, dissenting.

The unchallenged findings of fact made by the District Court reveal fundamental defects in the filtering software that is now available or that will be available in the foreseeable future. Because the software relies on key words or phrases to block undesirable sites, it does not have the capacity to exclude a precisely defined category of images. \* \* \* Given the quantity and ever-changing character of Web sites offering free sexually explicit material, it is inevitable that a substantial amount of such material

will never be blocked. Because of this “underblocking,” the statute will provide parents with a false sense of security without really solving the problem that motivated its enactment. Conversely, the software’s reliance on words to identify undesirable sites necessarily results in the blocking of thousands of pages that “contain content that is completely innocuous for both adults and minors, and that no rational person could conclude matches the filtering companies’ category definitions, such as ‘pornography’ or ‘sex.’” 201 F. Supp. 2d at 449. In my judgment, a statutory blunderbuss that mandates this vast amount of “overblocking” abridges the freedom of speech protected by the First Amendment.

The effect of the overblocking is the functional equivalent of a host of individual decisions excluding hundreds of thousands of individual constitutionally protected messages from Internet terminals located in public libraries throughout the Nation. Neither the interest in suppressing unlawful speech nor the interest in protecting children from access to harmful materials justifies this overly broad restriction on adult access to protected speech. \* \* \* The plurality does not reject [the district court’s] findings. Instead, “[a]ssuming that such erroneous blocking presents constitutional difficulties,” it relies on the Solicitor General’s assurance that the statute permits individual librarians to disable filtering mechanisms whenever a patron so requests. In my judgment, that assurance does not cure the constitutional infirmity in the statute.

Until a blocked site or group of sites is unblocked, a patron is unlikely to know what is being hidden and therefore whether there is any point in asking for the filter to be removed. It is as though the statute required a significant part of every library’s reading materials to be kept in unmarked, locked rooms or cabinets, which could be opened only in response to specific requests. Some curious readers would in time obtain access to the hidden materials, but many would not. Inevitably, the interest of the authors of those works in reaching the widest possible audience would be abridged. Moreover, because the procedures that different libraries are likely to adopt to respond to unblocking requests will no doubt vary, it is impossible to measure the aggregate effect of the statute on patrons’ access to blocked sites. Unless we assume that the statute is a mere symbolic gesture, we must conclude that it will create a significant prior restraint on adult access to protected speech. A law that prohibits reading without official consent, like a law that prohibits speaking without consent, “constitutes a dramatic departure from our national heritage and constitutional tradition.” *Watchtower Bible & Tract Soc. of N. Y., Inc. v. Village of Stratton*, 536 U. S. 150, 166 (2002).

## II

The plurality incorrectly argues that the statute does not impose “an unconstitutional condition on public libraries.” On the contrary, it impermissibly conditions the receipt of Government funding on the restriction of significant First Amendment rights. \* \* \* As the plurality recognizes, we have always assumed that libraries have discretion when

making decisions regarding what to include in, and exclude from, their collections. \* \* \* [A] library’s exercise of judgment with respect to its collection is entitled to First Amendment protection.

A federal statute penalizing a library for failing to install filtering software on every one of its Internet-accessible computers would unquestionably violate that Amendment. Cf. *Reno v. American Civil Liberties Union*, 521 U. S. 844 (1997). I think it equally clear that the First Amendment protects libraries from being denied funds for refusing to comply with an identical rule. An abridgment of speech by means of a threatened denial of benefits can be just as pernicious as an abridgment by means of a threatened penalty. \* \* \*

The plurality argues that the controversial decision in *Rust v. Sullivan*, 500 U. S. 173 (1991), requires rejection of appellees’ unconstitutional conditions claim. But, as subsequent cases have explained, *Rust* only involved and only applies to instances of governmental speech—that is, situations in which the government seeks to communicate a specific message. The discounts under the E-rate program and funding under the Library Services and Technology Act (LSTA) program involved in this case do not subsidize any message favored by the Government. As Congress made clear, these programs were designed “[t]o help public libraries provide their patrons with Internet access,” which in turn “provide[s] patrons with a vast amount of valuable information.” These programs thus are designed to provide access, particularly for individuals in low-income communities, see 47 U. S. C. §254(h)(1), to a vast amount and wide variety of private speech. They are not designed to foster or transmit any particular governmental message. \* \* \*

The plurality’s reliance on *National Endowment for Arts v. Finley*, 524 U. S. 569 (1998), is also misplaced. That case involved a challenge to a statute setting forth the criteria used by a federal panel of experts administering a federal grant program. Unlike this case, the Federal Government was not seeking to impose restrictions on the administration of a nonfederal program. \* \* \* Also unlike *Finley*, the Government does not merely seek to control a library’s discretion with respect to computers purchased with Government funds or those computers with Government-discounted Internet access. CIPA requires libraries to install filtering software on *every* computer with Internet access if the library receives *any* discount from the E-rate program or *any* funds from the LSTA program. \* \* \*

This Court should not permit federal funds to be used to enforce this kind of broad restriction of First Amendment rights, particularly when such a restriction is unnecessary to accomplish Congress’ stated goal. The abridgment of speech is equally obnoxious whether a rule like this one is enforced by a threat of penalties or by a threat to withhold a benefit.

I would affirm the judgment of the District Court.

JUSTICE SOUTER, with whom JUSTICE GINSBURG joins, dissenting.

I have no doubt about the legitimacy of governmental efforts to put a barrier between child patrons of public libraries and the raw offerings on the Internet otherwise available to them there, and if the only First Amendment interests raised here were those of children, I would uphold application of the Act. We have said that the governmental interest in “shielding” children from exposure to indecent material is “compelling,” *Reno v. American Civil Liberties Union*, 521 U. S. 844, 869-870 (1997), and I do not think that the awkwardness a child might feel on asking for an unblocked terminal is any such burden as to affect constitutionality.

Nor would I dissent if I agreed with the majority of my colleagues that an adult library patron could, consistently with the Act, obtain an unblocked terminal simply for the asking. \* \* \* [T]he unblocking provisions simply cannot be construed, even for constitutional avoidance purposes, to say that a library must unblock upon adult request, no conditions imposed and no questions asked. First, the statute says only that a library “may” unblock, not that it must. 20 U. S. C. §9134(f)(3); see 47 U.S.C. §254(h)(6)(D). In addition, it allows unblocking only for a “bona fide research or other lawful purposes,” 20 U. S. C. §9134(f)(3); see 47 U.S.C. §254(h)(6)(D), and if the “lawful purposes” criterion means anything that would not subsume and render the “bona fide research” criterion superfluous, it must impose some limit on eligibility for unblocking. There is therefore necessarily some restriction, which is surely made more onerous by the uncertainty of its terms and the generosity of its discretion to library staffs in deciding who gets complete Internet access and who does not.

We therefore have to take the statute on the understanding that adults will be denied access to a substantial amount of nonobscene material harmful to children but lawful for adult examination, and a substantial quantity of text and pictures harmful to no one. As the plurality concedes, this is the inevitable consequence of the indiscriminate behavior of current filtering mechanisms, which screen out material to an extent known only by the manufacturers of the blocking software.

We likewise have to examine the statute on the understanding that the restrictions on adult Internet access have no justification in the object of protecting children. Children could be restricted to blocked terminals, leaving other unblocked terminals in areas restricted to adults and screened from casual glances. And of course the statute could simply have provided for unblocking at adult request, with no questions asked. The statute could, in other words, have protected children without blocking access for adults or subjecting adults to anything more than minimal inconvenience \* \* \* .

The question for me, then, is whether a local library could itself constitutionally impose these restrictions on the content otherwise available to an adult patron through an Internet connection, at a library terminal provided for public use. The answer is no. A library that chose to block an adult’s Internet access to material harmful to children (and whatever else the indiscriminating filter might interrupt) would be imposing a

content-based restriction on communication of material in the library’s control that an adult could otherwise lawfully see. This would simply be censorship. \* \* \*

## II

The Court’s plurality does not treat blocking affecting adults as censorship, but chooses to describe a library’s act in filtering content as simply an instance of the kind of selection from available material that every library (save, perhaps, the Library of Congress) must perform.

Public libraries are indeed selective in what they acquire to place in their stacks, as they must be. There is only so much money and so much shelf space, and the necessity to choose some material and reject the rest justifies the effort to be selective with an eye to demand, quality, and the object of maintaining the library as a place of civilized enquiry by widely different sorts of people. Selectivity is thus necessary and complex, and these two characteristics explain why review of a library’s selection decisions must be limited: the decisions are made all the time, and only in extreme cases could one expect particular choices to reveal impermissible reasons (reasons even the plurality would consider to be illegitimate), like excluding books because their authors are Democrats or their critiques of organized Christianity are unsympathetic. See *Board of Ed., Island Trees Union Free School Dist. No. 26 v. Pico*, 457 U. S. 853, 870-871 (1982) (plurality opinion). Review for rational basis is probably the most that any court could conduct, owing to the myriad particular selections that might be attacked by someone, and the difficulty of untangling the play of factors behind a particular decision.

At every significant point, however, the Internet blocking here defies comparison to the process of acquisition. Whereas traditional scarcity of money and space require a library to make choices about what to acquire, and the choice to be made is whether or not to spend the money to acquire something, blocking is the subject of a choice made after the money for Internet access has been spent or committed. Since it makes no difference to the cost of Internet access whether an adult calls up material harmful for children or the Articles of Confederation, blocking (on facts like these) is not necessitated by scarcity of either money or space. In the instance of the Internet, what the library acquires is electronic access, and the choice to block is a choice to limit access that has already been acquired. Thus, deciding against buying a book means there is no book (unless a loan can be obtained), but blocking the Internet is merely blocking access purchased in its entirety and subject to unblocking if the librarian agrees. The proper analogy therefore is not to passing up a book that might have been bought; it is either to buying a book and then keeping it from adults lacking an acceptable “purpose,” or to buying an encyclopedia and then cutting out pages with anything thought to be unsuitable for all adults.

The plurality claims to find support for its conclusions in the “traditional missio[n]” of the public library. The plurality thus argues, in effect, that the traditional responsibility of public libraries has called for

denying adult access to certain books, or bowdlerizing the content of what the libraries let adults see. But, in fact, the plurality's conception of a public library's mission has been rejected by the libraries themselves. And no library that chose to block adult access in the way mandated by the Act could claim that the history of public library practice in this country furnished an implicit gloss on First Amendment standards, allowing for blocking out anything unsuitable for adults. \* \* \*

To these two reasons to treat blocking differently from a decision declining to buy a book, a third must be added. Quite simply, we can smell a rat when a library blocks material already in its control, just as we do when a library removes books from its shelves for reasons having nothing to do with wear and tear, obsolescence, or lack of demand. Content-based blocking and removal tell us something that mere absence from the shelves does not.

I have already spoken about two features of acquisition decisions that make them poor candidates for effective judicial review. The first is their complexity, the number of legitimate considerations that may go into them, not all pointing one way, providing cover for any illegitimate reason that managed to sneak in. A librarian should consider likely demand, scholarly or esthetic quality, alternative purchases, relative cost, and so on. The second reason the judiciary must be shy about reviewing acquisition decisions is the sheer volume of them, and thus the number that might draw fire. Courts cannot review the administration of every library with a constituent disgruntled that the library fails to buy exactly what he wants to read.

After a library has acquired material in the first place, however, the variety of possible reasons that might legitimately support an initial rejection are no longer in play. Removal of books or selective blocking by controversial subject matter is not a function of limited resources and less likely than a selection decision to reflect an assessment of esthetic or scholarly merit. Removal (and blocking) decisions being so often obviously correlated with content, they tend to show up for just what they are, and because such decisions tend to be few, courts can examine them without facing a deluge. The difference between choices to keep out and choices to throw out is thus enormous, a perception that underlay the good sense of the plurality's conclusion in *Board of Ed., Island Trees Union Free School Dist. No. 26 v. Pico*, 457 U. S. 853 (1982), that removing classics from a school library in response to pressure from parents and school board members violates the Speech Clause.

### III

There is no good reason, then, to treat blocking of adult enquiry as anything different from the censorship it presumptively is. For this reason, I would hold in accordance with conventional strict scrutiny that a library's practice of blocking would violate an adult patron's First and Fourteenth Amendment right to be free of Internet censorship, when unjustified (as here) by any legitimate interest in screening children from harmful

material. On that ground, the Act’s blocking requirement in its current breadth calls for unconstitutional action by a library recipient, and is itself unconstitutional.

### *Notes and Questions*

1. To what extent does the division in the Court turn on whether a library’s use of filtering software is analogous to “selecting” books for acquisition, or “removing” or “cutting out pages from” books? Which analogy do you find more apt? Why does Justice Souter believe that removal decisions should be more strictly scrutinized than acquisition decisions?

2. No member of the Court defends the district court’s public forum analysis. Would you? How?

3. The plurality opinion and the concurrences place great weight on the fact that a librarian can, for any patron, “unblock” an erroneously blocked site. Even if this were true, does it adequately dispose of all First Amendment issues? Recall the concerns expressed by Professor Lessig that, depending on how filtering software operates, users may not know what sites are blocked. Suppose, for example, that a library’s filtering software operated to exclude from search results any sites meeting the software’s blocking criteria. Should a different result obtain? In a case raising a facial challenge, or only an as-applied challenge?

4. The plurality opinion and the concurrences also focus on the fact that librarians can disable filtering software altogether. The statute allows a patron to request disabling “to enable access for bona fide research or other lawful purposes.” On the justices’ understanding of the statute, must a library patron actually articulate what his or her bona fide research project or other lawful purpose is? By what criteria should librarians measure what constitutes “bona fide research” or a “lawful purpose”? If you were advising a public library that received funds under the federal programs at issue, what policy on disabling access would you encourage the library to adopt?

5. Suppose that adult patrons of particular libraries have difficulty getting the libraries to disable filtering software, and bring as-applied challenges to the statute. What framework should courts use in evaluating such challenges?

6. A majority of the Court, even Justice Souter, would find the statute constitutional if it affected only the First Amendment interests of children. At the same time, the plurality, the concurrences, and Justice Souter seem to recognize that the e-rate statute is at least ambiguous as to whether a library can disable filtering software upon a minor’s request. As to minors, then, the e-rate statute seems to lack one of the safety valves on which a majority of the Court heavily relies. How would you analyze the effect of the statute on minors’ First Amendment rights?

7. Suppose that a local library that does *not* receive federal funds wishes to implement filtering software. How would you advise the library to write its policy?

## Chapter Six

---

---

### PROBLEMS OF SPEAKERS AND CONDUITS

---

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

##### 1. Liability for Defamatory Content

Page 513:

Add a new note, as follows:

8. Should discussion group moderators similarly be immune from defamation liability for messages written by other people and posted to the groups? Should it matter whether or not the moderators manually decide which messages to allow through? What if the moderators are very selective? At that point, should they become liable for the defamatory message, or is that simply resurrecting the distinction between CompuServe and Prodigy that section 230 rejected? At least one court of appeals has granted discussion group leaders broad immunity under section 230. *See Batzel v. Smith*, \_\_\_ F.3d \_\_\_, 2003 WL 21453358 (9th Cir. 2003).

##### 2. Copyright Liability

Pages 524-25:

At the end of note 3, add a new paragraph as follows:

Note that, in this scenario, not only will the subscriber whose material was wrongly taken down not have a cause of action against the ISP; there might not even be a cause of action against the copyright holder who

incorrectly claimed infringement. For example, *Rossi v. Motion Picture Association of America* (MPAA) involved a section 512 notice-and-take-down request issued by the MPAA that resulted in Rossi's site being taken down despite the absence of infringing material. The court dismissed Rossi's subsequent suit against the MPAA, ruling that a copyright holder does not need to conduct an investigation in order to make a good faith take-down request. See *Rossi v. Motion Picture Ass'n of America*, No. Civ. 0200239 (Apr. 29, 2003).

**Page 534:**

**Add a second paragraph to note 1 as follows:**

The Seventh Circuit recently has rejected the *Napster* court's conclusion that actual knowledge of infringing use is sufficient, in and of itself, for contributory infringement. See *In re Aimster Copyright Litigation*, \_\_\_ F.3d \_\_\_, 2003 WL 21488143 (7th Cir. 2003). According to the *Aimster* court, it was surely apparent that VCRs were being used for infringing as well as noninfringing purposes at the time of the *Sony* litigation, and yet the Supreme Court "was unwilling to allow copyright holders to prevent infringement effectuated by means of a new technology at the price of possibly denying noninfringing consumers the benefit of the technology." *Id.* at \_\_\_, 2003 WL at \*5. Nevertheless, the Seventh Circuit ruled that, because *Aimster* had failed to show that its file-sharing service had ever been used for *any* noninfringing purposes, a preliminary injunction based on a theory of contributory copyright liability was still justified.

## Chapter Seven

---

---

### PROBLEMS OF INDIVIDUAL AUTONOMY AND COMMERCIAL CONTROL

---

#### SECTION B. CONTROL OF PERSONAL INFORMATION

##### 2. The Legal Framework

##### b. Online Profiling and the Collection and Use of Personal Data

Pages 588-94:

In place of *In re Pharmatrak, Inc. Privacy Litigation* and accompanying notes and questions, insert:

#### **In re DoubleClick Inc. Privacy Litigation**

United States District Court for the Southern District of New York, 2001  
154 F. Supp. 2d 497

BUCHWALD, District Judge.

Plaintiffs bring this class action on behalf of themselves and all others similarly situated against defendant DoubleClick, Inc. (“defendant” or “DoubleClick”) seeking injunctive and monetary relief for injuries they have suffered as a result of DoubleClick’s purported illegal conduct. Specifically, plaintiffs bring three claims under federal laws: (1) 18 U.S.C. § 2701, *et seq.*; (2) 18 U.S.C. § 2510, *et seq.*; (3) 18 U.S.C. § 1030, *et seq.* \* \* \* . Now pending is DoubleClick’s [motion to dismiss].

## DOUBLECLICK'S TECHNOLOGY AND SERVICES

DoubleClick provides the Internet's largest advertising service. Commercial Web sites often rent out online advertising "space" to other Web sites. In the simplest type of arrangement, the host Web site (e.g., Lycos.com) rents space on its webpages to another Web site (e.g., TheGlobe.com) to place a "hotlink" banner advertisement ("banner advertisement"). When a user on the host Web site "clicks" on the banner advertisement, he is automatically connected to the advertiser's designated Web site.

DoubleClick acts as an intermediary between host Web sites and Web sites seeking to place banner advertisements. It promises client Web sites that it will place their banner advertisements in front of viewers who match their demographic target. For example, DoubleClick might try to place banner advertisements for a Web site that sells golf clubs in front of high-income people who follow golf and have a track record of making expensive online purchases. DoubleClick creates value for its customers in large part by building detailed profiles of Internet users and using them to target clients' advertisements.

DoubleClick compiles user profiles utilizing its proprietary technologies and analyses in cooperation with its affiliated Web sites. DoubleClick is affiliated with over 11,000 Web sites for which and on which it provides targeted banner advertisements. \* \* \* When users visit any of these DoubleClick-affiliated Web sites, a "cookie" is placed on their hard drives. Cookies are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner. However, Plaintiffs allege that DoubleClick's cookies collect "information that Web users, including plaintiffs and the Class, consider to be personal and private, such as names, e-mail addresses, home and business addresses, telephone numbers, searches performed on the Internet, Web pages or sites visited on the Internet and other communications and information that users would not ordinarily expect advertisers to be able to collect." \* \* \*

A. *Targeting Banner Advertisements*

DoubleClick's advertising targeting process involves three participants and four steps. The three participants are: (1) the user; (2) the DoubleClick-affiliated Web site; (3) the DoubleClick server. For the purposes of this discussion, we assume that a DoubleClick cookie already sits on the user's computer with the identification number "# 0001."

In Step One, a user seeks to access a DoubleClick-affiliated Web site such as Lycos.com. The user's browser sends a communication to Lycos.com (technically, to Lycos.com's server) saying, in essence, "Send me your homepage." \* \* \*

In Step Two, Lycos.com receives the request, processes it, and returns a communication to the user saying "Here is the Web page you requested." The communication has two parts. The first part is a copy of the Lycos.com

homepage, essentially the collection of article summaries, pictures and hotlinks a user sees on his screen when Lycos.com appears. The only objects missing are the banner advertisements; in their places lie blank spaces. The second part of the communication is an IP-address link to the DoubleClick server. This link instructs the user's computer to send a communication automatically to DoubleClick's server.

In Step Three, as per the IP-address instruction, the user's computer sends a communication to the DoubleClick server saying "I am cookie # 0001, send me banner advertisements to fill the blank spaces in the Lycos.com Web page." This communication contains information including the cookie identification number, the name of the DoubleClick-affiliated Web site the user requested, and the user's browser type.

Finally, in Step Four, the DoubleClick server identifies the user's profile by the cookie identification number and runs a complex set of algorithms based, in part, on the user's profile, to determine which advertisements it will present to the user. It then sends a communication to the user with banner advertisements saying "Here are the targeted banner advertisements for the Lycos.com homepage." Meanwhile, it also updates the user's profile with the information from the request.

DoubleClick's targeted advertising process is invisible to the user. His experience consists simply of requesting the Lycos.com homepage and, several moments later, receiving it complete with banner advertisements.

#### B. *Cookie Information Collection*

DoubleClick's cookies only collect information from one step of the above process: Step One. The cookies capture certain parts of the communications that users send to DoubleClick-affiliated Web sites. They collect this information in three ways: (1) "GET" submissions, (2) "POST" submissions, and (3) "GIF" submissions.

GET information is submitted as part of a Web site's address or "URL," in what is known as a "query string." For example, a request for a hypothetical online record store's selection of Bon Jovi albums might read: *http://recordstore.hypothetical.com/search?terms=bonjovi*. The URL query string begins with the "?" character meaning the cookie would record that the user requested information about Bon Jovi.

Users submit POST information when they fill in multiple blank fields on a webpage. For example, if a user signed up for an online discussion group, he might have to fill in fields with his name, address, email address, phone number and discussion group alias. The cookie would capture this submitted POST information.

Finally, DoubleClick places GIF tags on its affiliated Web sites. GIF tags are the size of a single pixel and are invisible to users. Unseen, they record the users' movements throughout the affiliated Web site, enabling DoubleClick to learn what information the user sought and viewed.

Although the information collected by DoubleClick's cookies is allegedly voluminous and detailed, it is important to note three clearly

defined parameters. First, DoubleClick's cookies *only* collect information concerning users' activities *on DoubleClick-affiliated Web sites*. Thus, if a user visits an unaffiliated Web site, the DoubleClick cookie captures no information. Second, plaintiff does not allege that DoubleClick ever attempted to collect *any* information other than the GET, POST, and GIF information submitted by users. DoubleClick is never alleged to have accessed files, programs or other information on users' hard drives. Third, DoubleClick will not collect information from any user who takes simple steps to prevent DoubleClick's tracking. As plaintiffs' counsel demonstrated at oral argument, users can easily and at no cost prevent DoubleClick from collecting information from them. They may do this in two ways: (1) visiting the DoubleClick Web site and requesting an "opt-out" cookie; and (2) configuring their browsers to block any cookies from being deposited. \* \* \*

Once DoubleClick collects information from the cookies on users' hard drives, it aggregates and compiles the information to build demographic profiles of users. Plaintiffs allege that DoubleClick has more than 100 million user profiles in its database. Exploiting its proprietary Dynamic Advertising Reporting & Targeting ("DART") technology, DoubleClick and its licensees target banner advertisements using these demographic profiles. \* \* \*

#### CLAIM I. TITLE II OF THE ECPA

Title II ("Title II") of the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2701 et seq. ("§ 2701"), aims to prevent hackers from obtaining, altering or destroying certain stored electronic communications. It creates both criminal sanctions and a civil right of action against persons who gain unauthorized access to communications facilities and thereby access electronic communications stored incident to their transmission. Title II specifically defines the relevant prohibited conduct as follows:

"(a) Offense. Except as provided in subsection (c) of this section whoever (1) intentionally accesses without authorization a facility through which an electronic [communication] service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains . . . access to a wire or electronic communication while it is in electronic storage in such system shall be punished. . . ."

Plaintiffs contend that DoubleClick's placement of cookies on plaintiffs' hard drives constitutes unauthorized access and, as a result, DoubleClick's collection of information from the cookies violates Title II. However, Title II contains an exception to its general prohibition.

"(c) Exceptions.—Subsection (a) of this section does not apply with respect to conduct authorized . . . (2) by a user of that [electronic communication] service with respect to a communication of or intended for that user;"

DoubleClick argues that its conduct falls under this exception. It contends that the DoubleClick-affiliated Web sites are "users" of the Internet and

that all of plaintiffs' communications accessed by DoubleClick's cookies have been "of or intended for" these Web sites. Therefore, it asserts, the Web sites' authorization excepts DoubleClick's access from § 2701(a)'s general prohibition. \* \* \*

Assuming that the communications are considered to be in "electronic storage," it appears that plaintiffs have adequately pled that DoubleClick's conduct constitutes an offense under § 2701(a), absent the exception under § 2701(c)(2). Therefore, the issue is whether DoubleClick's conduct falls under § 2701(c)(2)'s exception. This issue has three parts: (1) what is the relevant electronic communications service?; (2) were DoubleClick-affiliated Web sites "users" of this service?; and (3) did the DoubleClick-affiliated Web sites give DoubleClick sufficient authorization to access plaintiffs' stored communications "intended for" those Web sites?

A. *"Internet Access" is the relevant electronic communications service.*

Obviously, in a broad sense, the "Internet" is the relevant communications service. However, for the purposes of this motion, it is important that we define Internet service with somewhat greater care and precision. Plaintiff, at turns, argues that the electronic communications service is "Internet access" and "the ISP [Internet Service Provider]." The difference is important. An ISP is *an entity* that provides access to the Internet; examples include America Online, UUNET and Juno. Access to the Internet is *the service* an ISP provides. Therefore, the "service which provides to users thereof the ability to send or receive wire or electronic communications" is "Internet access."

B. *Web Sites are "users" under the ECPA.*

The ECPA defines a "user" as "any person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use." 18 U.S.C. § 2510(13). On first reading, the DoubleClick-affiliated Web sites appear to be users—they are (1) "entities" that (2) use Internet access and (3) are authorized to use Internet access by the ISPs to which they subscribe. However, plaintiffs make two arguments that Web sites nevertheless are not users. Both are unpersuasive.

First, plaintiffs argue that "[t]he most natural reading of 'user' is the person who has signed up for Internet access, which means the individual plaintiffs and Class members—not the Web servers." \* \* \* [This argument] rests on the erroneous assumption that only human users "sign[] up for Internet access," not Web sites or servers. \* \* \* [A]ll people and entities that utilize Internet access subscribe to ISPs or are ISPs. Although the vast majority of people who sign up for Internet access from consumer-focused ISPs such as America Online and Juno are individuals, every Web site, company, university, and government agency that utilizes Internet access also subscribes to an ISP or is one. These larger entities generally purchase "Internet access" in bulk from ISPs, often with value-added services and technologically advanced hardware. Nevertheless, they purchase the same underlying Internet access as individual users. Therefore, plaintiffs fail to

distinguish class members from Web sites and servers based on whether they subscribe to an ISP for Internet access.

Second, plaintiffs argue that “[t]he individual plaintiff (‘user’) owns the personal computer (‘facility’), while the Web sites she visits do not. [And that] [u]nder basic property and privacy notions, therefore, only she can authorize access to her own messages stored on that facility.” Again, plaintiffs seem to ignore the statute’s plain language. The general rule under § 2701(a) embodies plaintiffs’ position that only those authorized to use a “facility” may consent to its access. Nevertheless, Congress explicitly chose to make § 2701(a)’s general rule subject to § 2701(c)(2)’s exception for access authorized by authors and intended recipients of electronic communications. Thus, plaintiffs’ argument is essentially that this Court should ignore § 2701(c)(2) because Congress failed to take adequate account of “basic property and privacy notions.” However, it is not this Court’s role to revisit Congress’ legislative judgments. \* \* \*

C. *All of the communications DoubleClick has accessed through its cookies have been authorized or have fallen outside of Title II’s scope.*

Because plaintiffs only allege that DoubleClick accessed communications from plaintiffs to DoubleClick-affiliated Web sites, the issue becomes whether the Web sites gave DoubleClick adequate authorization under § 2701(c)(2) to access those communications. This issue, in turn, has two parts: (1) have the DoubleClick-affiliated Web sites authorized DoubleClick to access plaintiffs’ communications to them?; and (2) is that authorization sufficient under § 2701(c)(2)?

1. *The DoubleClick-affiliated Web sites have consented to DoubleClick’s interception of plaintiffs’ communications.*

\* \* \* Examining DoubleClick’s technological and commercial relationships with its affiliated Web sites, we find it implausible to infer that the Web sites have not authorized DoubleClick’s access. In a practical sense, the very reason clients hire DoubleClick is to target advertisements based on users’ demographic profiles. DoubleClick has trumpeted this fact in its advertising, patents and Securities and Exchange filings. True, officers of certain Web sites might not understand precisely how DoubleClick collects demographic information through cookies and records plaintiffs’ travels across the Web. However, that knowledge is irrelevant to the authorization at issue—Title II in no way outlaws collecting personally identifiable information or placing cookies, qua such. All that the Web sites must authorize is that DoubleClick access plaintiffs’ communications to them. [As described earlier,] the DoubleClick-affiliated Web sites actively notify DoubleClick each time a plaintiff sends them an electronic communication (whether through a page request, search, or GIF tag). The data in these notifications (such as the name of the Web site requested) often play an important role in determining which advertisements are presented to users. Plaintiffs have offered no explanation as to how, in anything other than a purely theoretical sense, the DoubleClick-affiliated

Web sites could have played such a central role in the information collection and not have authorized DoubleClick's access. \* \* \*

2. *DoubleClick is authorized to access plaintiffs' GET, POST and GIF submissions to the DoubleClick-affiliated Web sites.*

Plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all "intended for" those Web sites. In the case of the GET and POST submissions, users voluntarily type in information they wish to submit to the Web sites, information such as queries, commercial orders, and personal information. GIF information is generated and collected when users use their computer "mouse" or other instruments to navigate through Web pages and access information. Although the users' requests for data come through clicks, not keystrokes, they nonetheless are voluntary and purposeful. Therefore, because plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all "intended for" those Web sites, the Web sites' authorization is sufficient to except DoubleClick's access under § 2701(c)(2).

3. *To the extent that the DoubleClick cookies' identification numbers are electronic communications, (1) they fall outside of Title II's scope, and (2) DoubleClick's access to them is otherwise authorized.*

Plaintiffs argue that even if DoubleClick's access to plaintiffs' GET, POST and GIF submissions is properly authorized under § 2701(c)(2), the cookie identification numbers that accompany these submissions are not because they are never sent to, or through, the Web sites. However, this argument too is unavailing.

- (a) *The Cookies' identification numbers are not in "electronic storage" and therefore are outside Title II's scope.*

Putting aside the issue of whether the cookie identification numbers are electronic communications at all, DoubleClick does not need anyone's authority to access them. The cookies' long-term residence on plaintiffs' hard drives places them outside of § 2510(17)'s definition of "electronic storage" and, hence, Title II's protection. Section 2510(17) defines "electronic storage" as:

- (A) any *temporary, intermediate storage* of a wire or electronic communication incidental to the electronic transmission thereof; and
  - (B) any storage of such communication *by an electronic communication service* for the purpose of backup protection of such communication."
- (emphasis added)

Clearly, the cookies' residence on plaintiffs' computers does not fall into § 2510(17)(B) because plaintiffs are not "electronic communication service" providers.

Section 2510(17)(A)'s language and legislative history make evident that "electronic storage" is not meant to include DoubleClick's cookies either. Rather, it appears that the section is specifically targeted at communications temporarily stored by electronic communications services

incident to their transmission—for example, when an email service stores a message until the addressee downloads it. The statute’s language explicitly refers to “temporary, intermediate” storage. Webster’s Dictionary defines “temporary” as “lasting for a limited time,” and “intermediate” as “being or occurring at the middle place . . . .” *Webster’s Third New International Dictionary* 2353, 1180 (1993). In other words, Title II only protects electronic communications stored “for a limited time” in the “middle” of a transmission, i.e. when an electronic communication service temporarily stores a communication while waiting to deliver it. \* \* \*

Turning to the facts of this case, it is clear that DoubleClick’s cookies fall outside § 2510(17)’s definition of electronic storage and, hence, § 2701’s scope. \* \* \*

(b) *If the DoubleClick cookies’ identification numbers are considered stored electronic communications, they are “of or intended for” DoubleClick and DoubleClick’s acquisition of them does not violate Title II.*

Even if we were to assume that cookies and their identification numbers were “electronic communication[s] . . . in electronic storage,” DoubleClick’s access is still authorized. Section 2701(c)(2) excepts from Title II’s prohibition access, authorized by a “user,” to communications (1) “of” (2) “or intended for” that user. In every practical sense, the cookies’ identification numbers are internal DoubleClick communications—both “of” and “intended for” DoubleClick. DoubleClick creates the cookies, assigns them identification numbers, and places them on plaintiffs’ hard drives. The cookies and their identification numbers are vital to DoubleClick and meaningless to anyone else. \* \* \* [B]ecause the identification numbers are “of or intended for” DoubleClick, it does not violate Title II for DoubleClick to obtain them from plaintiffs’ electronic storage.

#### CLAIM II. WIRETAP ACT

Plaintiffs’ second claim is that DoubleClick violated the Federal Wiretap Act (“Wiretap Act”), 18 U.S.C. § 2510, et seq. The Wiretap Act provides for criminal punishment and a private right of action against:

“any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept wire, oral, or electronic communication [except as provided in the statute].” 18 U.S.C. § 2511.

For the purposes of this motion, DoubleClick concedes that its conduct, as pled, violates this prohibition. However, DoubleClick claims that its actions fall under an explicit statutory exception:

“It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception *unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the*

*Constitution or laws of the United States or any State.*” 18 U.S.C. § 2511(2)(d) (“§ 2511(2)(d)”) (emphasis added).

DoubleClick argues once again that the DoubleClick-affiliated Web sites have consented to its interceptions and, accordingly, that its conduct is exempted from the Wiretap Act’s general prohibition as it was from the Title II’s. Plaintiffs deny that the Web sites have consented and argue that even if the Web sites do consent, the exception does not apply because DoubleClick’s purpose is to commit “criminal or tortious act[s].”

As a preliminary matter, we find that the DoubleClick-affiliated Web sites are “parties to the communication[s]” from plaintiffs and have given sufficient consent to DoubleClick to intercept them. In reviewing the case law and legislative histories of Title II and the Wiretap Act, we can find no difference in their definitions of “user” (Title II) and “parties to the communication” (Wiretap Act) or “authorize” (Title II) and “consent” (Wiretap Act) that would make our analysis of the Web sites’ consent under Title II inapplicable to the Wiretap Act. Therefore, the issue before us is: assuming that DoubleClick committed every act alleged in the Amended Complaint, could this evince a “criminal or tortious” purpose on DoubleClick’s part?

In light of the DoubleClick-affiliated Web sites’ consent, plaintiffs must allege “either (1) that the primary motivation, or (2) that a determinative factor in the actor’s [DoubleClick’s] motivation for intercepting the conversation was to commit a criminal [or] tortious . . . act.” *United States v. Dale*, 991 F.2d 819, 841-42 (D.C. Cir. 1993). \* \* \*

Plaintiffs attempt to meet § 2511(2)(d)’s “purpose” requirement by arguing that their six non-Wiretap Act claims against DoubleClick “plead conduct that has underlying it a tortious purpose and/or that translates into tortious acts.” In other words, by virtue of its tortious acts, DoubleClick must have had a tortious purpose. \* \* \* In the instant case, plaintiffs clearly allege that DoubleClick has committed a number of torts. However, nowhere have they alleged that DoubleClick’s “primary motivation” or a “determining factor” in its actions has been to injure plaintiffs tortiously. \* \* \* [W]e find that plaintiffs have failed to allege that DoubleClick has intercepted plaintiffs’ communications for a “criminal or tortious” purpose.

### COUNT III. COMPUTER FRAUD AND ABUSE ACT

Plaintiffs’ final federal claim is under the Computer Fraud and Abuse Act (“CFAA”), [which prohibits one from] “intentionally access[ing] a computer without authorization, or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer if the conduct involved an interstate or foreign communication . . .” 18 U.S.C. § 1030(c)(2). The CFAA \* \* \* provides a civil right of action for victims under 18 U.S.C. § 1030(g) (“§ 1030(g)”):

“(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain

compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in section (e)(8)(A) are limited to economic damages . . .”

However, section 18 U.S.C. § 1030(e)(8) (“§ 1030(e)(8)”) limits the “damage” civilly recoverable to the following instances:

“(e)(8) the term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information that—(A) causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals; [B. Impairs medical care; C. Causes physical injury; D. Threatens public health or safety].” (emphasis added).

For the purposes of this motion, DoubleClick does not contest that plaintiffs’ computers were “protected” under the CFAA or that its access was unauthorized. Instead, it claims that § 1030(e)(8) creates a \$5,000 damages threshold for each individual class member and that plaintiffs have failed to plead these damages adequately. Plaintiffs argue that “loss” under § 1030(g) is distinct from “damage” and, accordingly, is not subject to § 1030(e)(8)’s damage threshold. In the alternative, if § 1030(e)(8)’s damage threshold is found applicable to plaintiffs’ claims, plaintiffs argue that they easily meet the threshold by “aggregating” losses for the entire class over “any 1-year period.” \* \* \*

[We conclude that] all injuries under § 1030(g) are subject to § 1030(e)(8)’s \$5,000 threshold, whether termed “damage” or “loss.” [In addition, we] find that damages and losses under § 1030(e)(8)(A) may only be aggregated across victims and over time for a single act. \* \* \* The relevant clause states that “the term ‘damage’ means any impairment to the integrity or availability of data, a program, a system, or information that—(A) causes loss aggregating at least \$5,000 in value during any 1-year period to one or more individuals.” The fact that § 1030(e)(8)(A) is phrased in the singular (“any *impairment* to the integrity or availability of data, *a program, a system, or information* that—(a) causes loss”), rather than the plural (e.g., any *impairments* to the integrity or availability of data, *programs, systems, or information* that—(a) cause loss . . . ), indicates that § 1030(e)(8)(A) should only apply to single acts. \* \* \*

[P]laintiffs fail to plead facts that could meet the damages threshold. Plaintiffs essentially plead two bases of “damage or loss”: (1) their cost in remedying their computers and data in the wake of DoubleClick’s access, and (2) the economic value of their attention (to DoubleClick’s advertisements) and demographic information. Clearly, any economic losses plaintiffs bore in securing or remedying their systems in the wake of DoubleClick’s alleged CFAA violations would count towards § 1030(e)(8)(A)’s damage threshold. However, as counsel demonstrated at oral argument, users may easily and at no cost prevent DoubleClick from collecting information by simply selecting options on their browsers or downloading an “opt-out” cookie from DoubleClick’s Web site. Similarly, they have not pled that DoubleClick caused any damage whatsoever to

plaintiffs' computers, systems or data that could require economic remedy. Thus, these remedial economic losses are insignificant if, indeed, they exist at all.

Plaintiffs also contend that they have suffered economic damages consisting of the value of: (1) the opportunity to present plaintiffs with advertising; and (2) the demographic information DoubleClick has collected. \* \* \* Even assuming that the economic value of plaintiffs' attention and demographic information could be counted towards the monetary threshold—a dubious assumption—it would still be insufficient. We do not commonly believe that the economic value of our attention is unjustly taken from us when we choose to watch a television show or read a newspaper with advertisements and we are unaware of any statute or caselaw that holds it is. We see no reason why Web site advertising should be treated any differently. \* \* \* Nevertheless, to the extent that some value could be placed on these losses, we find that the plaintiffs have failed to allege facts that could support the inference that the damages and losses plaintiffs incurred from DoubleClick's access to any *particular* computer, over one year's time, could meet § 1030(e)(8)(A)'s damage threshold.

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

1. Re-read 18 U.S.C. § 2701(a). What is it designed to prohibit? The court states that it “appears that the plaintiffs have adequately pled that DoubleClick's conduct constitutes an offense under § 2701(a).” Do you agree? What is the “facility through which an electronic communication service is provided” that DoubleClick has accessed without authorization? What “electronic communication” did DoubleClick obtain from “electronic storage”?

2. Under the court's reading of the consent exceptions in § 2701(c) and § 2511(2)(d), the consent of the web site that engaged DoubleClick's services is sufficient to preclude liability. Should the law instead require the consent of the user of the web site? Why or why not?

3. Consider the substantive predicate for liability under the second cause of action the court discusses, 18 U.S.C. § 2511. As the court notes, DoubleClick concedes that its conduct, as pled, violates this provision. If you were DoubleClick's lawyer, would you have made this concession? What communications did DoubleClick intercept, and what “device” did DoubleClick use to intercept them?

4. The court rejects the plaintiffs' claim under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, based on a lack of cognizable damage. What about the substantive predicate for liability under section 1030, which DoubleClick again concedes was met for purposes of its motion to dismiss? Did DoubleClick access the plaintiffs' computers without authorization, or exceed authorized access? What information was obtained from the computers? We examine the CFAA in more detail in Section C.

5. *DoubleClick* is one of several cases addressing challenges under the federal wiretap statute (Title III), the stored communications access provisions of ECPA, and the CFAA to the use of cookies. See *Chance v. Avenue A*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001) (rejecting challenge to advertiser's use of

cookies); *In re Intuit Privacy Litigation*, 138 F. Supp. 2d 1272 (C.D. Cal. 2001) (rejecting Title III and CFAA claims against web site operator that placed cookies, but denying motion to dismiss ECPA claim); *In re Pharmatrak, Inc. Privacy Litigation*, 220 F. Supp. 2d 4 (D. Mass. 2002) (rejecting Title III, ECPA, and CFAA claims against company that planted cookies to track data on behalf of pharmaceutical company clients), *rev'd*, 329 F.3d 9 (1st Cir. 2003) (reversing grant of summary judgment on Title III claim).

For our purposes, what is interesting is that courts have largely accepted the framework that plaintiffs' lawyers have created for bringing claims under Title III, the stored communications access provisions of ECPA, and the CFAA. The point of contention in the cases is typically whether one party *consented* to the use of cookies to track data, thus triggering the statutory exceptions—not whether the federal statutes cover this sort of conduct in the first place. Since the adoption of the statutes well pre-dated the use of cookies, we can legitimately ask whether courts should interpret the statutes to cover the conduct in question, and whether the statutes are adequate to address privacy concerns raised by the use of cookies. Consider the following case.

### **In re Pharmatrak, Inc. Privacy Litigation**

United States Court of Appeals for the First Circuit, 2003  
329 F.3d 9

LYNCH, Circuit Judge.

This case raises important questions about the scope of privacy protection afforded internet users under [the federal Wiretap Act, as amended by Title I of] the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2511, 2520 (2000).

In sum, pharmaceutical companies invited users to visit their websites to learn about their drugs and to obtain rebates. An enterprising company, Pharmatrak, sold a service, called "NETcompare," to these pharmaceutical companies. That service accessed information about the internet users and collected certain information meant to permit the pharmaceutical companies to do intra-industry comparisons of website traffic and usage. Most of the pharmaceutical companies were emphatic that they did not want personal or identifying data about their web site users to be collected. In connection with their contracting to use NETcompare, they sought and received assurances from Pharmatrak that such data collection would not occur. As it turned out, some such personal and identifying data was found, using easily customized search programs, on Pharmatrak's computers. Plaintiffs, on behalf of the purported class of internet users whose data Pharmatrak collected, sued both Pharmatrak and the pharmaceutical companies asserting, *inter alia*, that they intercepted electronic communications without consent, in violation of [18 U.S.C. § 2511].

The district court entered summary judgment for defendants on the basis that Pharmatrak's activities fell within an exception to the statute where one party consents to an interception. The court found the client

pharmaceutical companies had consented by contracting with Pharmatrak and so this protected Pharmatrak. \* \* \* We hold that the district court incorrectly interpreted the “consent” exception to the [statute]; we also hold that Pharmatrak “intercepted” the communication under the statute. We reverse and remand for further proceedings. \* \* \*

#### I.

Pharmatrak provided its NETcompare service to pharmaceutical companies including American Home Products, Pharmacia, SmithKline Beecham, Pfizer, and Novartis from approximately June 1998 to November 2000. The pharmaceutical clients terminated their contracts with Pharmatrak shortly after this lawsuit was filed in August 2000. As a result, Pharmatrak was forced to cease its operations by December 1, 2000.

NETcompare was marketed as a tool that would allow a company to compare traffic on and usage of different parts of its website with the same information from its competitors’ websites. The key advantage of NETcompare over off-the-shelf software was its capacity to allow each client to compare its performance with that of other clients from the same industry.

NETcompare was designed to record the webpages a user viewed at clients’ websites; how long the user spent on each webpage; the visitor’s path through the site (including her points of entry and exit); the visitor’s IP address; and, for later versions, the webpage the user viewed immediately before arriving at the client’s site (i.e., the “referrer URL”). This information-gathering was not visible to users of the pharmaceutical clients’ websites. According to [Pharmatrak executives], NETcompare was not designed to collect any personal information whatsoever.

NETcompare operated as follows. A pharmaceutical client installed NETcompare by adding five to ten lines of HTML code to each webpage it wished to track and configuring the pages to interface with Pharmatrak’s technology. When a user visited the website of a Pharmatrak client, Pharmatrak’s HTML code instructed the user’s computer to contact Pharmatrak’s web server and retrieve from it a tiny, invisible graphic image known as a “clear GIF” (or a “web bug”). The purpose of the clear GIF was to cause the user’s computer to communicate directly with Pharmatrak’s web server. When the user’s computer requested the clear GIF, Pharmatrak’s web servers responded by either placing or accessing a “persistent cookie” on the user’s computer. On a user’s first visit to a webpage monitored by NETcompare, Pharmatrak’s servers would plant a cookie on the user’s computer. If the user had already visited a NETcompare webpage, then Pharmatrak’s servers would access the information on the existing cookie.

A cookie is a piece of information sent by a web server to a web browser that the browser software is expected to save and to send back whenever the browser makes additional requests of the server (such as when the user visits additional webpages at the same or related sites). A persistent cookie is one that does not expire at the end of an online session.

Cookies are widely used on the internet by reputable websites to promote convenience and customization. Cookies often store user preferences, login and registration information, or information related to an online “shopping cart.” Cookies may also contain unique identifiers that allow a website to differentiate among users.

Each Pharmatrak cookie contained a unique alphanumeric identifier that allowed Pharmatrak to track a user as she navigated through a client’s site and to identify a repeat user each time she visited clients’ sites. If a person visited *www.pfizer.com* in June 2000 and *www.pharmacia.com* in July 2000, for example, then the persistent cookie on her computer would indicate to Pharmatrak that the same computer had been used to visit both sites. As NETcompare tracked a user through a website, it used JavaScript and a JavaApplet to record information such as the URLs the user visited. This data was recorded on the access logs of Pharmatrak’s web servers.

Pharmatrak sent monthly reports to its clients juxtaposing the data collected by NETcompare about all pharmaceutical clients. These reports covered topics such as the most heavily used parts of a particular site; which site was receiving the most hits in particular areas such as investor or media relations; and the most important links to a site. The monthly reports did not contain any personally identifiable information about users. \* \* \*

While it was marketing NETcompare to prospective pharmaceutical clients, Pharmatrak repeatedly told them that NETcompare did not collect personally identifiable information. It said its technology could not collect personal information, and specifically provided that the information it gathered could not be *used* to identify particular users by name. In their affidavits and depositions, executives of Pharmatrak clients consistently said that they believed NETcompare did not collect personal information, and that they did not learn otherwise until the onset of litigation, at which point they promptly terminated the service. Some, if not all, pharmaceutical clients explicitly conditioned their purchase of NETcompare on Pharmatrak’s guarantees that it would not collect users’ personal information. \* \* \*

Pharmatrak nevertheless collected some personal information on a small number of users. Pharmatrak distributed approximately 18.7 million persistent cookies through NETcompare. The number of unique cookies provides a rough estimate of the number of users Pharmatrak monitored. Plaintiffs’ expert was able to develop individual profiles for just 232 users.

The following personal information was found on Pharmatrak servers: names, addresses, telephone numbers, email addresses, dates of birth, genders, insurance statuses, education levels, occupations, medical conditions, medications, and reasons for visiting the particular website. Pharmatrak also occasionally recorded the subject, sender, and date of the web-based email message a user was reading immediately prior to visiting the website of a Pharmatrak client. Most of the individual profiles assembled by plaintiffs’ expert contain some but not all of this information.

The personal information in 197 of the 232 user profiles was recorded due to an interaction between NETcompare and computer code written by one pharmaceutical client, Pharmacia, for one of its webpages. Starting on or before August 18, 2000 and ending sometime between December 2, 2000 and February 6, 2001, the client Pharmacia used the “get” method to transmit information from a rebate form on its Detrol website; the webpage was subsequently modified to use the “post” method of transmission. [The use of the get method] was the source of the personal information collected by Pharmatrak from users of the Detrol website.

Web servers use two methods to transmit information entered into online forms: the get method and the post method. The get method is generally used for short forms such as the “Search” box at Yahoo! and other online search engines. The post method is normally used for longer forms and forms soliciting private information. When a server uses the get method, the information entered into the online form becomes appended to the next URL. For example, if a user enters “respiratory problems” into the query box at a search engine, and the search engine transmits this information using the get method, then the words “respiratory” and “problems” will be appended to the query string at the end of the URL of the webpage showing the search results. By contrast, if a website transmits information via the post method, then that information does not appear in the URL. Since NETcompare was designed to record the full URLs of the webpages a user viewed immediately before and during a visit to a client’s site, Pharmatrak recorded personal information transmitted using the get method.

There is no evidence Pharmatrak instructed its clients not to use the get method. The detailed installation instructions Pharmatrak provided to pharmaceutical clients ignore entirely the issue of the different transmission methods.

In addition to the problem at the Detrol website, there was also another instance in which a pharmaceutical client used the get method to transmit personal information entered into an online form. The other personal information on Pharmatrak’s servers was recorded as a result of software errors. These errors were a bug in a popular email program (reported in May 2001 and subsequently fixed) and an aberrant web browser.

## II.

On June 28, 2001, plaintiffs filed an amended consolidated class action complaint against Pharmatrak; its parent company, Glocal Communications, Ltd.; and five pharmaceutical companies: American Home Products Corp., Glaxo Wellcome, Inc., Pfizer, Inc., Pharmacia Corp., and SmithKline Beecham Corp. Plaintiffs alleged nine counts including violation of [the federal Wiretap Act, as amended by] Title I of the ECPA, 18 U.S.C. § 2510 *et seq.* \* \* \*. Pharmatrak, Glocal, and a number of the pharmaceutical defendants moved for summary judgment \* \* \*. [T]he district court issued a memorandum and order on August 13, 2002 \* \* \* [granting in relevant

part] defendants' summary judgment motions. The court held that the claim against Pharmatrak under Title I of the ECPA was precluded because "the Pharmaceutical Defendants consented to the placement of code for Pharmatrak's NETcompare service on their websites."

### III.

\* \* \* ECPA amended the Federal Wiretap Act by extending to data and electronic transmissions the same protection already afforded to oral and wire communications. \* \* \* The post-ECPA Wiretap Act provides a private right of action against one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a); *see* 18 U.S.C. § 2520 (providing a private right of action). The Wiretap Act defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4). Thus, plaintiffs must show five elements to make their claim \* \* \* : that a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device. This showing is subject to certain statutory exceptions, such as consent.

In its trial and appellate court briefs, Pharmatrak sought summary judgment on only one element of § 2511(1)(a), interception, as well as on the statutory consent exception. \* \* \*

#### C. *Consent Exception*

There is a pertinent statutory exception to § 2511(1)(a) "where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act . . ." 18 U.S.C. § 2511(2)(d). \* \* \* Plaintiffs do not allege that Pharmatrak acted with a criminal or tortious purpose. Therefore, the question under the exception is limited to whether the pharmaceutical defendants gave consent to the interception. \* \* \*

The district court adopted Pharmatrak's argument that the only relevant inquiry is whether the pharmaceutical companies consented to use Pharmatrak's NETcompare service, regardless of how the service eventually operated. In doing so, the district court did not apply this circuit's general standards for consent under the Wiretap Act and the ECPA set forth in *Griggs-Ryan v. Smith*, 904 F.2d 112 (1st Cir. 1990). It also misread two district court opinions on which it purported to rely: *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001), and *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

This court addressed the issue of consent under the Wiretap Act in *Griggs-Ryan*. A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications. "Thus, 'a reviewing court must inquire into the *dimensions of the consent* and then ascertain whether the interception

exceeded those boundaries.” *Gilday v. Dubois*, 124 F.3d 277, 297 (1st Cir. 1997) (quoting *Griggs-Ryan*, 904 F.2d at 119). Consent may be explicit or implied, but it must be actual consent rather than constructive consent. Pharmatrak argues that it had implied consent from the pharmaceutical companies. \* \* \*

The district court made an error of law, urged on it by Pharmatrak, as to what constitutes consent. It did not apply the standards of this circuit. Moreover, *DoubleClick* and *Avenue A* do not set up a rule, contrary to the district court’s reading of them, that a consent to interception can be inferred from the mere purchase of a service, regardless of circumstances. If these cases did so hold, they would be contrary to the rule of this circuit established in *Griggs-Ryan*. *DoubleClick* and *Avenue A*, rather, were concerned with situations in which the defendant companies’ clients purchased their services for the precise purpose of creating individual user profiles in order to target those users for particular advertisements. See *Avenue A*, 165 F. Supp. 2d at 1156, 1161; *DoubleClick*, 154 F. Supp. 2d at 502, 510-11. This very purpose was announced by *DoubleClick* and *Avenue A* publicly, as well as being self-evident. See *Avenue A*, 165 F. Supp. 2d at 1161; *DoubleClick*, 154 F. Supp. 2d at 502, 510-11. These decisions found it would be unreasonable to infer that the clients had *not* consented merely because they might not understand precisely how the user demographics were collected. See *Avenue A*, 165 F. Supp. 2d at 1161-62; *DoubleClick*, 154 F. Supp. 2d at 510-11. The facts in our case are the mirror image of those in *DoubleClick* and *Avenue A*: the pharmaceutical clients insisted there be no collection of personal data and the circumstances permit no reasonable inference that they did consent. \* \* \*

The interpretation urged by Pharmatrak would, we think, lead to results inconsistent with the statutory intent. It would undercut efforts by one party to a contract to require that the privacy interests of those who electronically communicate with it be protected by the other party to the contract. It also would lead to irrational results. Suppose Pharmatrak, for example, had intentionally designed its software, contrary to its representations and its clients’ expectations, to redirect all possible personal information to Pharmatrak servers, which collected and mined the data. Under the district court’s approach, Pharmatrak would nevertheless be insulated against liability under the [Wiretap Act] on the theory that the pharmaceutical companies had “consented” by simply buying Pharmatrak’s product. Or suppose an internet service provider received a parent’s consent solely to monitor a child’s internet usage for attempts to access sexually explicit sites—but the ISP installed code that monitored, recorded and cataloged all internet usage by parent and child alike. Under the theory we have rejected, the ISP would not be liable under the [Wiretap Act].

Nor did the users consent. On the undisputed facts, it is clear that the internet user did not consent to Pharmatrak’s accessing his or her communication with the pharmaceutical companies. The pharmaceutical companies’ websites gave no indication that use meant consent to collection

of personal information by a third party. Rather, Pharmatrak's involvement was meant to be invisible to the user, and it was. Deficient notice will almost always defeat a claim of implied consent. Pharmatrak makes a frivolous argument that the internet users visiting client Pharmacia's webpage for rebates on Detrol thereby consented to Pharmatrak's intercepting their personal information. On that theory, every online communication would provide consent to interception by a third party.

*D. Interception Requirement*

The parties briefed to the district court the question of whether Pharmatrak had "intercepted" electronic communications. If this question could be resolved in Pharmatrak's favor, that would provide a ground for affirmance of the summary judgment. It cannot be answered in favor of Pharmatrak.

The [Wiretap Act] prohibits only "interceptions" of electronic communications. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." *Id.* § 2510(4).

Before enactment of the ECPA, some courts had narrowed the Wiretap Act's definition of interception to include only acquisitions of a communication contemporaneous with transmission. *See, e.g., Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 460-61 (5th Cir. 1994) (applying pre-ECPA interpretation to post-ECPA case). There was a resulting debate about whether the [post-ECPA Wiretap Act] should be similarly restricted. \* \* \* The facts here do not require us to enter the debate over the existence of a real-time requirement. The acquisition by Pharmatrak was contemporaneous with the transmission by the internet users to the pharmaceutical companies. \* \* \* [U]sers communicated simultaneously with the pharmaceutical client's web server and with Pharmatrak's web server. After the user's personal information was transmitted using the get method, both the pharmaceutical client's server and Pharmatrak's server contributed content for the succeeding webpage; \* \* \* Pharmatrak's content (the clear GIF that enabled the interception) sometimes arrived before the content delivered by the pharmaceutical clients. Even those courts that narrowly read "interception" would find that Pharmatrak's acquisition was an interception. \* \* \*

Pharmatrak argues that there was no interception because "there were always two separate communications: one between the Web user and the Pharmaceutical Client, and the other between the Web user and Pharmatrak." This argument fails for two reasons. First, as a matter of law, even the circuits adopting a narrow reading of the Wiretap Act merely require that the acquisition occur at the same time as the transmission; they do not require that the acquisition somehow constitute the same communication as the transmission. Second, Pharmatrak acquired the same URL query string (sometimes containing personal information)

exchanged as part of the communication between the pharmaceutical client and the user. Separate, but simultaneous and identical, communications satisfy even the strictest real-time requirement.

E. *Intent Requirement*

At oral argument this court questioned the parties about whether the “intent” requirement under § 2511(a)(1) had been met. We remand this issue because it was not squarely addressed by both parties before the district court.

**Notes and Questions**

1. What distinguishes this case from *DoubleClick*? Recall that in *DoubleClick*, the court noted that web site operators “might not understand precisely how” DoubleClick collects and tracks information, but that “all that the Web sites must authorize is that DoubleClick access plaintiffs’ communications to them.” Does the *Pharmatrak* court adequately deal with this language?

2. Unlike in *DoubleClick*, the court here explicitly holds that Pharmatrak “intercepted” electronic communications. What communications did Pharmatrak intercept? What “device” did Pharmatrak use to intercept them?

3. *Pharmatrak* involved issues regarding the collection of information, not its subsequent use and disclosure. To what extent does the law regulate the use and disclosure of personal data? Consider the following case.

## SECTION C. CONTROLLING ACCESS TO DATA

Pages 601-10:

In place of *Ticketmaster Corporation v. Tickets.com, Inc.*, *Kelly v. Arriba Soft Corp.*, and accompanying notes and questions, insert:

### **Ticketmaster Corporation v. Tickets.com, Inc.**

United States District Court for the Central District of California, 2003  
2003 U.S. Dist. LEXIS 6483

HUPP, J.

Both [Ticketmaster Corporation (“TM”)] and [Tickets.com, Inc. (“TX”)] are in the business of selling tickets to all kinds of “events” (sports, concerts, plays, etc.) to the public. They are in heavy competition with one another, but operate in distinctive ways. TM is the largest company in the industry. It sells tickets by the four methods of ticket selling—venue box office, retail outlets, by telephone, and over the internet. \* \* \* TX at the time of the events considered in this motion was primarily (but not exclusively) an internet seller. Both TM and TX maintain a web page reachable by anyone with an internet connection. Each of their web pages

has many subsidiary (or interior) web pages which describe one event each and provide such basic information as to location, date, time, description of the event, and ticket prices. \* \* \*

TM principally does business by exclusive contracts with the event providers or their producers, and its web pages only list the events for which TM is the exclusive ticket seller. TX also sells tickets to a number of events \* \* \* . At [relevant times, however,] its web pages attempted to list all events for which tickets were available whether or not TX sold the tickets. \* \* \* When TX could not sell the tickets, it listed ticket brokers who sold at premium prices. \* \* \* Until early 2000, in situations where TM was the only source of tickets, TX provided a “deep link” by which the customer would be transferred to the interior web page of TM’s web site, where the customer could purchase the ticket from TM. This process of “deep linking” is the subject of TM’s complaint in this action, of which there [are] now left the contract, copyright, and trespass theories. [TX moves for summary judgment on all three theories.]

Starting in 1998 and continuing to July 2001, when it stopped the practice, TX employed an electronic program called a “spider” or “crawler” to review the internal web pages (available to the public) of TM. The “spider” “crawled” through the internal web pages to TM and electronically extracted the electronic information from which the web page is shown on the user’s computer. The spider temporarily loaded this electronic information into the Random Access Memory (“RAM”) of TX’s computers for a period of from 10-15 seconds. TX then extracted the factual information (event, date, time, tickets prices, and URL) and discarded the rest (which consisted of TM identification, logos, ads, and other information which TX did not intend to use; much of this discarded material was protected by copyright). The factual information was then organized in the TX format to be displayed on the TX internal web page. The TX internal web page carried no TM identification and had only the factual information about the event on it \* \* \* plus any information or advertisement added by TX. From March 1998 to early 2000, the TX user was provided the deep linking option \* \* \* to go directly from the TX web site to the relevant TM interior web page. This option stopped (or was stopped by TM) in early 2000. For an unknown period afterward, the TX customer was given the option of linking to the TM home page, from which the customer could work his way to the interior web page in which he was interested. \* \* \*

The contract aspect of the case derives from a notice placed on the home page of the TM web site which states that anyone going beyond that point into the interior web pages of the web site accepts certain conditions, which include, relevant to this case, that all information obtained from the website is for the personal use of the user and may not be used for commercial purposes. \* \* \* [T]here has been developed evidence that TX was fully familiar with the conditions TM claimed to impose on users, including a letter from TM to TX which quoted the conditions (and a reply by TX stating that it did not accept the conditions). Thus, there is sufficient evidence to defeat summary judgment on the contract theory if knowledge

of the asserted conditions of use was had by TX, who nevertheless continued to send its spider into the TM interior web pages, and if it is legally concluded that doing so can lead to a binding contract. \* \* \* As a result, the TX motion for summary judgment on the contract issue is denied.

The trespass to chattels issue requires adapting the ancient common law action to the modern age. \* \* \* [Lower court] cases discussing the chattel theory \* \* \* tend to support the proposition that mere invasion or use of a portion of the web site by a spider is a trespass (leading at least to nominal damages), and that there need not be an independent showing of direct harm either to the chattel (unlikely in the case of a spider) or tangible interference with the use of the computer being invaded. However, scholars and practitioners alike have criticized the extension of the trespass to chattels doctrine to the internet context, noting that this doctrinal expansion threatens basic internet functions (i.e., search engines) and exposes the flaws inherent in applying doctrines based in real and tangible property to cyberspace. Pending appellate guidance, this court comes down on the side of requiring some tangible interference with the use or operation of the computer being invaded by the spider. [The] Restatement (Second) of Torts § 219 requires a showing that “the chattel is impaired as to its condition, quality, or value.” Therefore, unless there is actual dispossession of the chattel for a substantial time (not present here), the elements of the tort have not been made out. Since the spider does not cause physical injury to the chattel, there must be some evidence that the \* \* \* utility of the computer (or computer network) being “spiderized” is adversely affected by the use of the spider. No such evidence is presented here. This court respectfully disagrees with other district courts’ finding that mere use of a spider to enter a publically available web site to gather information, without more, is sufficient to fulfill the harm requirement for trespass to chattels.

TM complains that the information obtained by the use of the spider was valuable (and even that it was sold by TX), and that it spent time and money attempting to frustrate the spider, but neither of these items shows damage to the computers or their operation. One must keep in mind that we are talking about the common law tort of trespass, not damage from breach of contract or copyright infringement. The tort claim may not succeed without proof of tort-type damage. Plaintiff TM has the burden to show such damage. None is shown here. The motion for summary judgment is granted to eliminate the claim for trespass to chattels. \* \* \*

The copyright issues are more difficult. They divide into three issues. The first is whether the momentary resting in the TX computers of [information copied from TM’s computers] constitutes actionable copyright infringement. The second is whether the URLs, which were copied and used by TX, contain copyrightable material. The third is whether TX’s deep linking caused the unauthorized public display of TM event pages.

In examining these questions, we must keep in mind a prime theorem of copyright law—facts, as such, are not subject to copyright protection. What is subject to copyright protection is the manner or mode of expression of those facts. Thus, addresses and telephone numbers contained in a directory do not have copyright protection, *Feist Publications v. Rural Tel. Serv. Co.*, 499 U.S. 340 (1991), despite the fact that time, money, and effort went into compiling the information. Similarly, in this case, the existence of the event, its date and time, and its ticket prices, are not subject to copyright. Anyone is free to print (or show on the internet) such information. Thus, if TX had sat down a secretary at the computer screen with instructions manually to go through TM’s web sites and pick out and write down purely factual information about the events, and then feed it into the TX web pages (using the TX distinctive format only), no one could complain. The objection is that the same thing was done with an electronic program. \* \* \* [TX’s] spider picks up the electronic [signals] and loads them momentarily (for 10 to 15 seconds) into the RAM of the TX computers, where a program [extracts] the factual data (not protected) [and places it] into the TX format for its web pages \* \* \*. Thus, the actual copying (if it can be called that) is momentary while the non-protected material, all open to the public, is extracted.

Is this momentary resting of the electronic symbols from which a TM web page could be (but is not) constructed fair use where the purpose is to obtain nonprotected facts? The court thinks the answer is “yes”. There is not much law in point. However, there are two Ninth Circuit cases which shed light on the problem. They are *Sony Computer Entm’t, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000), and *Sega Enters. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992). In each of these cases, the alleged infringer attempted to get at non-protected source code by reverse engineering of the plaintiff’s copyrighted software. In doing so, the necessary method was to copy the software and work backwards to derive the unprotected source code. The copied software was then destroyed. In each case, this was held to be fair use since it was necessary to temporarily copy the software to obtain the non-protected material. There may be a difference with this case, however; at least TM claims so. It asserts in its points and authorities that taking the temporary copy in this case was not the only way to obtain the unprotected information, and that TX was able to, and in actuality did, purchase such information from certain third-parties. Both Sony and Sega stated that the fair use was justified because reverse engineering (including taking a temporary copy) was the only way the unprotected information could be obtained. Although this court recognizes that the holdings of Sony and Sega were limited to the specific context of “disassembling” copyrighted object code in order to access unprotected elements contained in the source code, this court believes that the “fair use” doctrine can be applied to the current facts.

\* \* \* In determining whether a challenged use of copyrighted material is fair, a court must keep in mind the public policy underlying the Copyright Act: to secure a fair return for an author’s creative labor and to stimulate

artistic creativity for the general good. This court sees no public policy that would be served by restricting TX from using spiders to temporarily download TM's event pages in order to acquire the unprotected, publicly available factual event information. The rest of the event page information (which consisted of TM identification, logos, ads, and other information) was discarded and not used by TX and is not exposed to the public by TX. In temporarily downloading TM's event pages to its RAM through the use of spiders, TX was not exploiting TM's creative labors in any way: its spiders gathered copyrightable and non-copyrightable information alike but then immediately discarded the copyrighted material. It is unlikely that the spiders could have been programmed to take only the factual information from the TM web pages without initially downloading the entire page.

Consideration of the fair use factors listed in 17 USC § 106 supports this result. First, TX operates its site for commercial purposes, and this fact tends to weigh against a finding of fair use. *Campbell v. Acuff-Rose Music*, 510 U.S. 569, 585 (1994). TX's use of the data gathered from TM's event pages was only slightly transformative. As for the second factor, the nature of the copyrighted work, the copying that occurred when spiders download the event page, access the source code for each page, and extract the factual data embedded in the code, is analogous to the process of copying that the *Sony* court condoned \* \* \*. Third, because TX's final product—the TX web site—did not contain any infringing material, the “amount and substantiality of the portion used” is of little weight. The fourth factor (the effect on the market value of the copyrighted work) is, of course nil, and weighs towards finding fair use. TM's arguments and evidence regarding loss of advertising revenue \* \* \* are not persuasive.

The second copyright problem is whether the URLs (Uniform Resource Locator) are subject to copyright protection. The URLs are copied by TX and, while TX was deep hyper-linking to TM interior web pages, were used by TX to allow the deep-linking (by providing the electronic address of the particular relevant TM interior web page). \* \* \* TM contends that, although the URLs are strictly functional, they are entitled to copyright protection because there are several ways to write the URL, and, thus, original authorship is used. The court disagrees. A URL is simply an address, open to the public, like the street address of a building, which, if known, can enable the user to reach the building. There is nothing sufficiently original to make the URL a copyrightable item, especially the way it is used. There appear to be no cases holding the URLs to be subject to copyright. On principle, they should not be.

The third copyright problem is whether TX's deep linking caused the unauthorized public display of TM event pages in violation of TM's exclusive rights of reproduction and display under 17 U.S.C. § 106. The Ninth Circuit in *Kelly v. Arriba Soft Corp.*, 280 F.3d 934 (9th Cir. 2002), recognized that inline linking and framing of full-sized images of plaintiff's copyrighted photographs within the defendant's web site violated the plaintiff's public display rights. In that case, defendant's web site contained links to plaintiff's photographs (which were on plaintiff's publicly available

website). Users were able to view plaintiff's photographs within the context of defendant's site: Plaintiff's images were "framed" by the defendant's window, and were thus surrounded by defendant web page's text and advertising. \* \* \* TM alleges that when a user was deep-linked from the TX site to a TM event page, a smaller window was opened. The smaller window was described as containing a page from the TM web site which was "framed" by the larger window. At the time of the preliminary injunction motion, TX stated that whether "framing" occurs or not depends on the settings on the user's computer, over which TX has no control. Thus, framing occurred on some occasions but not on others. However, TX says that it "did not try to disguise a sale by use of frames occurring on the Tickets.com website." TX further states that when users were linked to TM web pages, the TM event pages were clearly identified as belonging to TM.

[E]ven if the TM interior web site page was "framed" within the TX web page, this case is distinguishable from *Kelly*. In *Kelly*, the defendant's site would display a variety of "thumbnail" images as a result of the user's search. By clicking on the desired thumbnail image, a user could view the "Images Attributes" page, which displayed the original full-size image, a description of its dimensions, a link to the originating web site, and defendant's banner and advertising. The full-size image was not technically located on defendant's web site, but was taken directly from the originating web site. However, only the image itself, and not any other part of the originating web site, was displayed on the "Images Attributes" page. The Ninth Circuit determined that by importing plaintiff's images into its own web page, and by showing them in the context of its own site, defendant infringed upon plaintiff's exclusive public display right.

In this case, a user on the TX site was taken directly to the originating TM site, containing all the elements of that particular TM event page. Each TM event page clearly identified itself as belonging to TM. Moreover, the link on the TX site to the TM event page contained the following notice: "Buy this ticket from another online ticketing company. Click here to buy tickets. These tickets are sold by another ticketing company. Although we can't sell them to you, the link above will take you directly to the other company's web site where you can purchase them." Even if the TM site may have been displayed as a smaller window that was literally "framed" by the larger TX window, it is not clear that, as matter of law, the linking to TX event pages would constitute a showing or public display in violation of 17 U.S.C. § 106(5). Accordingly, summary judgment is granted on the copyright claims of TM and it is eliminated from this action.

**Kelly v. Arriba Soft Corp.**

United States Court of Appeals for the Ninth Circuit, 2003

\_\_\_ F.3d \_\_\_, 2003 WL 21518002

T.G. NELSON, Circuit Judge.

This case involves the application of copyright law to the vast world of the internet and internet search engines. The plaintiff, Leslie Kelly, is a professional photographer who has copyrighted many of his images of the American West. Some of these images are located on Kelly's web site or other web sites with which Kelly has a license agreement. The defendant, Arriba Soft Corp., operates an internet search engine that displays its results in the form of small pictures rather than the more usual form of text. Arriba obtained its database of pictures by copying images from other web sites. By clicking on one of these small pictures, called "thumbnails," the user can then view a large version of that same picture within the context of the Arriba web page.

When Kelly discovered that his photographs were part of Arriba's search engine database, he brought a claim against Arriba for copyright infringement. The district court found that Kelly had established a prima facie case of copyright infringement based on Arriba's unauthorized reproduction and display of Kelly's works, but that this reproduction and display constituted a non-infringing "fair use" under Section 107 of the Copyright Act. Kelly appeals that decision, and we affirm in part and reverse in part. The creation and use of the thumbnails in the search engine is a fair use. However, the district court should not have decided whether the display of the larger image is a violation of Kelly's exclusive right to publicly display his works. Thus, we remand for further proceedings consistent with this opinion.

## I.

The search engine at issue in this case is unconventional in that it displays the results of a user's query as "thumbnail" images. When a user wants to search the internet for information on a certain topic, he or she types a search term into a search engine, which then produces a list of web sites that contain information relating to the search term. Normally, the list of results is in text format. The Arriba search engine, however, produces its list of results as small pictures.

To provide this service, Arriba developed a computer program that "crawls" the web looking for images to index. This crawler downloads full-sized copies of the images onto Arriba's server. The program then uses these copies to generate smaller, lower-resolution thumbnails of the images. Once the thumbnails are created, the program deletes the full-sized originals from the server. Although a user could copy these thumbnails to his computer or disk, he cannot increase the resolution of the thumbnail; any enlargement would result in a loss of clarity of the image.

The second component of the Arriba program occurs when the user double-clicks on the thumbnail. From January 1999 to June 1999, clicking on the thumbnail produced the “Images Attributes” page. This page used in-line linking to display the original full-sized image, surrounded by text describing the size of the image, a link to the original web site, the Arriba banner, and Arriba advertising. In-line linking allows one to import a graphic from a source website and incorporate it in one’s own website, creating the appearance that the in-lined graphic is a seamless part of the second web page. The in-line link instructs the user’s browser to retrieve the linked-to image from the source website and display it on the user’s screen, but does so without leaving the linking document. Thus, the linking party can incorporate the linked image into its own content. As a result, although the image in Arriba’s Images Attributes page came directly from the originating web site and was not copied onto Arriba’s server, the user would not realize that the image actually resided on another web site.

From July 1999 until sometime after August 2000, the results page contained thumbnails accompanied by two links: “Source” and “Details.” The “Details” link produced a screen similar to the Images Attributes page but with a thumbnail rather than the full-sized image. Alternatively, by clicking on the “Source” link or the thumbnail from the results page, the site produced two new windows on top of the Arriba page. The window in the forefront contained solely the full-sized image. This window partially obscured another window, which displayed a reduced-size version of the image’s originating web page. Part of the Arriba web page was visible underneath both of these new windows.

In January 1999, Arriba’s crawler visited web sites that contained Kelly’s photographs. The crawler copied thirty-five of Kelly’s images to the Arriba database. Kelly had never given permission to Arriba to copy his images and objected when he found out that Arriba was using them. Arriba deleted the thumbnails of images that came from Kelly’s own web sites and placed those sites on a list of sites that it would not crawl in the future. Several months later, Arriba received Kelly’s complaint of copyright infringement, which identified other images of his that came from third-party web sites. Arriba subsequently deleted those thumbnails and placed those third-party sites on a list of sites that it would not crawl in the future.

The district court granted summary judgment in favor of Arriba. Kelly’s motion for partial summary judgment asserted that Arriba’s use of the thumbnail images violated his display, reproduction, and distribution rights. Arriba cross-moved for summary judgment. For the purposes of the motion, Arriba conceded that Kelly established a *prima facie* case of infringement. However, it limited its concession to the violation of the display and reproduction rights *as to the thumbnail images*. Arriba then argued that its use of the thumbnail images was a fair use.

The district court did not limit its decision to the thumbnail images alone. The court granted summary judgment to Arriba, finding that its use

of both the thumbnail images and the full-size images was fair. In doing so, the court broadened the scope of Kelly's original motion to include a claim for infringement of the full-size images. The court also broadened the scope of Arriba's concession to cover the prima facie case for both the thumbnail images and the full-size images. The court determined that two of the fair use factors weighed heavily in Arriba's favor. Specifically, the court found that the character and purpose of Arriba's use was significantly transformative and the use did not harm the market for or value of Kelly's works. Kelly now appeals this decision.

## II.

\* \* \* The district court's decision in this case involves two distinct actions by Arriba that warrant analysis. The first action consists of the reproduction of Kelly's images to create the thumbnails and the use of those thumbnails in Arriba's search engine. The second action involves the display of Kelly's larger images when the user clicks on the thumbnails. We conclude that, as to the first action, the district court correctly found that Arriba's use was fair. However, as to the second action, we conclude that the district court should not have reached the issue because neither party moved for summary judgment as to the full-size images and Arriba's response to Kelly's summary judgment motion did not concede the prima facie case for infringement as to those images.

### A.

An owner of a copyright has the exclusive right to reproduce, distribute, and publicly display copies of the work. To establish a claim of copyright infringement by reproduction, the plaintiff must show ownership of the copyright and copying by the defendant. As to the thumbnails, Arriba conceded that Kelly established a prima facie case of infringement of Kelly's reproduction rights.

A claim of copyright infringement is subject to certain statutory exceptions, including the fair use exception. This exception "permits courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster." *Dr. Seuss Enters., L.P. v. Penguin Books USA, Inc.*, 109 F.3d 1394, 1399 (9th Cir. 1997) (internal quotation marks omitted). The statute sets out four factors to consider in determining whether the use in a particular case is a fair use. We must balance these factors in light of the objectives of copyright law, rather than view them as definitive or determinative tests. We now turn to the four fair use factors.

#### 1. *Purpose and character of the use.*

\* \* \* There is no dispute that Arriba operates its web site for commercial purposes and that Kelly's images were part of Arriba's search engine database. As the district court found, while such use of Kelly's images was commercial, it was more incidental and less exploitative in nature than more traditional types of commercial use. Arriba was neither using Kelly's images to directly promote its web site nor trying to profit by

selling Kelly's images. Instead, Kelly's images were among thousands of images in Arriba's search engine database. Because the use of Kelly's images was not highly exploitative, the commercial nature of the use weighs only slightly against a finding of fair use.

The second part of the inquiry as to this factor involves the transformative nature of the use. We must determine if Arriba's use of the images merely superseded the object of the originals or instead added a further purpose or different character. We find that Arriba's use of Kelly's images for its thumbnails was transformative.

Although Arriba made exact replications of Kelly's images, the thumbnails were much smaller, lower-resolution images that served an entirely different function than Kelly's original images. Kelly's images are artistic works intended to inform and to engage the viewer in an aesthetic experience. His images are used to portray scenes from the American West in an aesthetic manner. Arriba's use of Kelly's images in the thumbnails is unrelated to any aesthetic purpose. Arriba's search engine functions as a tool to help index and improve access to images on the internet and their related web sites. In fact, users are unlikely to enlarge the thumbnails and use them for artistic purposes because the thumbnails are of much lower-resolution than the originals; any enlargement results in a significant loss of clarity of the image, making them inappropriate as display material. \* \* \*

2. *Nature of the copyrighted work.*

"Works that are creative in nature are closer to the core of intended copyright protection than are more fact-based works." *A & M Records v. Napster*, 239 F.3d 1004, 1016 (9th Cir. 2001). Photographs that are meant to be viewed by the public for informative and aesthetic purposes, such as Kelly's, are generally creative in nature. The fact that a work is published or unpublished also is a critical element of its nature. Published works are more likely to qualify as fair use because the first appearance of the artist's expression has already occurred. Kelly's images appeared on the internet before Arriba used them in its search image. When considering both of these elements, we find that this factor weighs only slightly in favor of Kelly.

3. *Amount and substantiality of portion used.*

"While wholesale copying does not preclude fair use per se, copying an entire work militates against a finding of fair use." *Worldwide Church of God v. Philadelphia Church of God*, 227 F.3d 1110, 1118 (9th Cir. 2000) (internal quotation marks omitted). However, the extent of permissible copying varies with the purpose and character of the use. If the secondary user only copies as much as is necessary for his or her intended use, then this factor will not weigh against him or her.

This factor neither weighs for nor against either party because, although Arriba did copy each of Kelly's images as a whole, it was reasonable to do so in light of Arriba's use of the images. It was necessary

for Arriba to copy the entire image to allow users to recognize the image and decide whether to pursue more information about the image or the originating web site. If Arriba only copied part of the image, it would be more difficult to identify it, thereby reducing the usefulness of the visual search engine.

4. *Effect of the use upon the potential market for or value of the copyrighted work.*

\* \* \* Arriba's use of Kelly's images in its thumbnails does not harm the market for Kelly's images or the value of his images. By showing the thumbnails on its results page when users entered terms related to Kelly's images, the search engine would guide users to Kelly's web site rather than away from it. \* \* \* Arriba's use of Kelly's images also would not harm Kelly's ability to sell or license his full-sized images. \* \* \*

Having considered the four fair use factors and found that two weigh in favor of Arriba, one is neutral, and one weighs slightly in favor of Kelly, we conclude that Arriba's use of Kelly's images as thumbnails in its search engine is a fair use.

B.

As mentioned above, the district court granted summary judgment to Arriba as to the full-size images as well. However, because the court broadened the scope of both the parties' motions for partial summary judgment and Arriba's concession on the prima facie case, we must reverse this portion of the court's opinion.

With limited exceptions that do not apply here, a district court may not grant summary judgment on a claim when the party has not requested it. The parties did not move for summary judgment as to copyright infringement of the full-size images. Further, Arriba had no opportunity to contest the prima facie case for infringement as to the full-size images. Accordingly, we reverse this portion of the district court's opinion and remand for further proceedings.

CONCLUSION

We hold that Arriba's reproduction of Kelly's images for use as thumbnails in Arriba's search engine is a fair use under the Copyright Act. However, we hold that the district court should not have reached whether Arriba's display of Kelly's full-sized images is a fair use because the parties never moved for summary judgment on this claim and Arriba never conceded the prima facie case as to the full-size images. The district court's opinion is affirmed as to the thumbnails and reversed as to the display of the full-sized images.

**Notes and Questions**

1. Recall the approaches to trespass to chattels in *eBay v. Bidder's Edge* and *Intel Corporation v. Hamidi* in Chapter Two. Does the *Ticketmaster* court's treatment of the issue differ, and if so, how? Which approach do you find more

persuasive? Why shouldn't Ticketmaster's efforts to frustrate Tickets.com's activities count as harm for purposes of the trespass to chattels claim?

2. Should the law grant Ticketmaster a more robust right to control its computer system, so that Ticketmaster could exclude any use that it finds detrimental? Why or why not?

3. Should Tickets.com's use of Ticketmaster's site, with awareness of the Ticketmaster's acceptable use policy, create a binding contract? For further discussion of these issues, see Section D, *infra*.

4. In *Kelly*, the Ninth Circuit avoids resolving whether Arriba Soft's "in-line linking" to or "framing" of Kelly's full-size images violates Kelly's copyright. How should the district court resolve this issue on remand? In a now-withdrawn opinion, the Ninth Circuit initially concluded that Arriba Soft's actions with respect to Kelly's full-size images violated Kelly's exclusive right to display his copyrighted works publicly: "Arriba actively participated in displaying Kelly's images by trolling the web, finding Kelly's images, and then having its program inline link and frame those images within its own web site. \* \* \* Arriba acted as more than a passive conduit of the images by establishing a direct link to the copyrighted images." 280 F.3d 934, 947 (9th Cir. 2002), *withdrawn*, 2003 WL 21518002 (9th Cir. July 7, 2003). What distinguishes Arriba Soft's activities from the activities of ordinary search engines? Suppose that Arriba Soft merely searched for and linked to Kelly's images, rather than framing them. Could Kelly object to that conduct, and on what legal theory?

5. The district court in *Ticketmaster* distinguishes the Ninth Circuit's treatment in the original *Kelly* opinion of Arriba Soft's framing of the full-size images in part on the ground that Arriba Soft "import[ed]" Kelly's image, while a Tickets.com user "was taken directly to the originating TM site." In both cases, however, the alleged infringer's site simply instructed the user's browser to communicate with the copyright holder's site and display portions of it. Suppose that Arriba Soft had not just framed Kelly's images, but had framed an entire page on which Kelly's image appeared. Should that change the court's approach to the case? How might you argue that Tickets.com's conduct is more harmful than Arriba Soft's conduct?