From PLI's Course Handbook
Communications Law 2003
G0-00UI

5

CYBERLIABILITY 2003: SELECT DEVELOPMENTS

Jeffrey P. Cunard
Jennifer B. Coplan
Debevoise & Plimpton

Cyberliability 2003: Select Developments

Jeffrey P. Cunard
Jennifer B. Coplan*

1. Online Contracting.

Specht v. Netscape Communications Corp., 306 F.3d 17 (2nd Cir. 2002).

The Second Circuit affirmed the district court's denial of Netscape's motion to enforce an arbitration clause contained in an online license agreement. Consumers downloaded software from Netscape's website by clicking on a "download" button. The link to the software license was located below the button and was visible only if the consumers scrolled down to the next screen. The district court had noted that users could download and use the software without taking any action that "plainly manifests assent." 150 F. Supp. 2d 585 (S.D.N.Y. 2001).

The Second Circuit concluded that merely clicking on a download button does not communicate assent to contractual terms if the offer does not make clear that assent is the consequence of clicking the button. The court found that "a reasonably prudent offeree in plaintiffs' position" would not have necessarily known about the license agreement, and that Netscape

---

* Jeffrey P. Cunard is a partner in the Washington, D.C. office, and Jennifer B. Coplan is counsel in the New York office, of Debevoise & Plimpton.

did not provide reasonable notice of the license terms. Accordingly, "plaintiffs' bare act of downloading the software did not unambiguously manifest assent to the arbitration provision contained in the license terms."

Ticketmaster Corp. v. Tickets.com, Inc., No. CV99-7654-HLH (VBKX), 2003 WL 21406289 (C.D. Cal. 2003).

A California district court denied Tickets.com's motion for summary judgment on a contract claim brought by Ticketmaster alleging that Tickets.com used information from Ticketmaster's website in violation of Ticketmaster's conditions of use. Ticketmaster placed a warning in a prominent place on the home page of its website stating that proceeding beyond the home page binds the user to the conditions of use, which included a prohibition on using the information from Ticketmaster's website for commercial purposes.

The district court held that "a contract can be formed by proceeding into the interior web pages after knowledge (or ... presumptive knowledge) of the conditions accepted when doing so." The court distinguished the facts from those present earlier in the case, noting that at the time of the motion for preliminary injunction, the notice was placed at the bottom of the home page, where a user would have to scroll down to read it; since that time, the notice was moved to a "prominent" location and evidence was presented that Tickets.com was familiar with the terms, including a letter from Ticketmaster quoting the relevant conditions. The court also distinguished *Ticketmaster* from *Specht* (discussed above) in that the terms of use in *Specht,* by contrast, were not plainly visible or known to the defendants.

DeJohn v. The .TV Corp. Int'l, 245 F. Supp. 2d 913 (C.D. Ill. 2003).

The district court held that a valid contract was formed when a user clicked on a box indicating that he had agreed to Register.com's clickwrap service agreement, even if he did not actually read the terms of the agreement. The text of the agreement was provided through a hyperlink located directly above the box. Noting that the user had an opportunity to review the terms of the agreement, the court concluded that the fact that he claimed not to have read it was "irrelevant because absent fraud ... failure to read a contract is not a get out of jail free card."

2. Defamation; ISP Immunity Under CDA Section 230.

Carafano v. Metrosplash.com, Inc., 339 F.3d 1119 (9th Cir. 2003).

In Metrosplash, the Ninth Circuit addressed the question of whether Matchmaker.com, a commercial Internet dating service, was immune from liability, based on Section 230 of the Communications Decency Act (47 U.S.C. § 230), where a third party had submitted a false profile of the actress Christianne Carafano.

In 2002, a district court found that Matchmaker had taken an active role in developing the information posted on its online service (because users were limited to posting information solicited through Matchmaker's questionnaire). It found that Matchmaker itself was the "information content provider" and, therefore, ineligible for Section 230

protection. 207 F. Supp. 2d 1055 (C.D. Cal. 2002). The Ninth Circuit disagreed, concluding that the fact that the service provider had provided the questionnaire did not make it an information content provider with respect to information chosen and posted by a user in response to that questionnaire. The court reasoned that under Section 230(c), "so long as a third party willingly provides the essential published content, the interactive service provider receives full immunity regardless of any specific editing or selection process." Although the Matchmaker questionnaire facilitated the user's expression of information, the "selection of the content was left exclusively to the user" and so it was the user, not Matchmaker, who was responsible for the "underlying misinformation." The court concluded that so long as a third party provides the published content, "the interactive service provider receives full immunity regardless of the specific editing or selection process."

Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003).

Robert Smith, on suspicion that he had seen stolen art in the home of someone for whom he was working, sent an email expressing his suspicions to a website concerning stolen artwork. Ton Cremers, the operator of the website, published Smith's email, with minor editorial changes, on the website and later posted it on a listserv operated by the same organization. After the posting, Smith emailed a subscriber to the listserv explaining that he had no idea that his email would be posted to the listserv or put on the web. A district court denied two motions filed by Cremers, resulting in an appeal to the Ninth Circuit.

The Ninth Circuit confirmed that Section 230 immunizes interactive service providers acting as both publishers and distributors. It concluded that Cremers, as a user or provider of an interactive computer service, was potentially entitled to Section 230 immunity. It held that Cremers, as operator of the Network website and listserv, could not be considered the "content provider" of the email for purposes of Section 230. The court reasoned that Smith composed the email entirely on his own, and that neither Cremers' minor alterations nor his selection of the letter for publication on the listserv (while rejecting other emails) rose to the level of "creation" or "development."

The court then considered whether Smith can be said to have "provided" his email in the sense intended by Section 230(c) (i.e., as an "information content provider"). The court concluded that if Cremers should have reasonably concluded that the email was not sent to him for posting on the listserv, then Cremers could not avail himself of Section 230 immunity because the posted information was not "provided" by another "information content provider." The court remanded the case to the district court to make such determination.

Firth v. State of New York, 761 N.Y.S.2d 361 (2003).

After a public employee's defamation suit based on publication on a state government website of an allegedly defamatory report was dismissed, the employee sued based on republication of the report when it was moved by the state to a new directory on the website. A New York appellate court affirmed the lower court's denial of the state's summary judgment motion, holding that plaintiff's allegations were sufficient to state a cause of action for republication

to a new audience since the subsequent publication was intended to and actually did reach a new audience. The court reasoned that the moving of the report was akin to the repackaging of a book from hard cover to paperback.

3. Spam.

Gillman v. Sprint Communications Co., 2002 WL 31497311 (Utah Dist. Ct. 2003).

The Utah District Court held that Utah's anti-spam law, Unsolicited Commercial and Sexually Explicit Email Act, Utah Code Ann. §§ 13-36-101 et seq. , does not prohibit businesses from sending unwanted email to consumers with whom they have a "preexisting legal relationship." The Utah statute proscribes the sending of "unsolicited" commercial emails if they do not comply with the Act's requirements. A commercial email is "unsolicited" if it is received "without the recipient's express permission, except where the sender has a preexisting business or personal relationship with the sender." §13-36-102(8)(a).

A Utah resident agreed to receive promotional emails in connection with his registration on a website. The website operator sold its email addresses to Traffix, Inc., which had contracted with Sprint to send, through a subsidiary, emails promoting Sprint's long distance telephone service. The plaintiff requested that Traffix remove his name from the distribution list. Nevertheless, he thereafter received a promotional email for Sprint service. The plaintiff sued Sprint for violation of the Utah statute.

The court held that because the plaintiff had a preexisting business relationship with Traffix's

subsidiary, the Sprint email he received was not "unsolicited." The court acknowledged that such interpretation – that a preexisting relationship continues ad infinitum – would potentially leave all consumers that had, at one time, a business relationship with an commercial email provider unable to avail themselves of the Act, even if they subsequently terminated the business relationship. Conceding that such reading of the Act may be contrary to legislative intent, the court invited the Utah legislature to clarify the statutory language.

People of New York v. Monsterhut, Inc., 12 ILR (P&F) 897 (NY Sup. Ct., 2003).

The New York Attorney General brought an action against Monsterhut, an Internet marketing company, alleging that the company fraudulently represented to its consumers that its email lists were obtained based on permission based protocols and that consumers "opted-in" to receive the email. Monsterhut had purchased its email lists from third parties who claimed that their lists comprised users who had consented to receive advertisements. The court held that the record before it did not support Monsterhut's assertion that the use of such purchased lists constituted "opt-in" as that term is used in the email marketing industry.

Intel Corp. v. Hamidi, 71 P.3d 296; 1 Cal Rptr. 3d 32 (2003).

The California Supreme Court held that, under California law, the tort of trespass to chattels does not

encompass an electronic communication that neither damages the recipient computer system nor impairs its functioning. The decision overturned two lower court decisions upholding the right of Intel to block Hamidi, a former employee, from sending thousands of unsolicited emails to Intel employees. The court distinguished the facts before it from the cases in which Internet service providers have sued senders of spam on a trespass to chattels theory. The court reasoned that in the latter cases the trespass to chattels claims were based upon evidence that the vast quantities of email sent by spammers overburdened the ISPs' computers. In those cases, the court stated, electronic contact constituted trespass because they "involved some actual or threatened interference" with the functioning of the computers. Intel had not claimed that Hamidi's emails had any functional effect on its computer systems and, therefore, that Intel suffered any cognizable injury to its property.

Mainstream Marketing Services, Inc. v. FTC, 2003 WL 22213517 (D. Colo. Sept. 25, 2003); *In FTC v. Mainstream Marketing Services Inc.*, 2003 WL 22293798 (10th Cir. Oct. 7, 2003).

Recent decisions addressing the constitutionality of the FTC's amended Telemarketing Sales Rules (Rules), which create a "do-not-call" registry, have potential implications for legislative proposals that would create a "do-not-spam" list. In late September 2003, a federal district court in Colorado enjoined the enforcement of the Rules (which were to have gone into effect on October 1) on First Amendment grounds. The court held that the Rules constitute a content-based restriction on commercial speech that does not pass intermediate scrutiny.

The court applied the three-part "intermediate scrutiny" test for assessing the constitutionality of restrictions on commercial speech set forth in *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557 (1980): whether the (1) government asserts a substantial interest; (2) restriction on commercial speech directly and materially advances the interest; and (3) regulation is narrowly tailored. The court first concluded that the do-not-call registry was the type of regulation that affected protected commercial speech. It then recognized that the government has a substantial interest in protecting consumers from deceptive and abusive telemarketing practices and protecting privacy. Nevertheless, it found that the Rules do not advance that interest to a material degree (thereby failing the second prong of the test) because they exclude calls from charitable organizations without a logical basis for the disparate treatment.

In early October, 2003, the 10th Circuit issued a stay of the district court's ruling, pending final resolution of the appeal on the merits. The 10th Circuit concluded that the FTC is likely to succeed on its argument that the distinction between commercial and non-commercial phone solicitations satisfies the *Central Hudson* analysis. The court of appeals agreed with the district court that the government had a substantial interest in preventing abusive and coercive sales practices and protecting privacy, but disagreed with the district court's conclusion that the Rules do not materially advance that interest.

The court of appeals found persuasive the argument that commercial telemarketing carries a greater risk of privacy invasion and abusive sales practices. The court of appeals also concluded that the "opt-in" nature of the do-not-call list weighs in favor of a

finding that the Rule satisfies the "reasonable fit" test used to determine the final two *Central Hudson* factors. The court of appeals set an expedited schedule for briefing and oral argument.

Legislation.

The following states have enacted legislation restricting unsolicited commercial email:

Alaska*, Arizona*, Arkansas*, California, Colorado, Connecticut, Delaware, Idaho, Illinois, Indiana*, Iowa, Kansas, Louisiana, Maine*, Maryland, Michigan*, Minnesota, Missouri, Nevada, New Mexico*, North Carolina, North Dakota*, Ohio, Oklahoma, Oregon*, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas*, Utah, Virginia*, Washington, West Virginia, Wisconsin and Wyoming*.

*Legislation enacted since September 2002.

California: Calif. Bus. and Prof. Code §§ 17529 and 17538.45.

In September 2003, California amended its spam legislation to make it illegal to send unsolicited commercial email from California or to a California email address, unless the recipient has asked for information about products or services offered by the sender, or had a previous business relationship with the sender. The sender must include a means for the recipient to opt out of receiving future commercial email, even if a recipient and sender had a previous business relationship. In amending its legislation, California joined Delaware in becoming the only two states to adopt an "opt-in" rule for email advertising.

The California statute allows an individual, email service provider, or the state Attorney General, to sue someone who initiates or advertises in an unsolicited commercial email for actual damages, plus statutory damages of $1,000 per message up to $1 million total per incident. Whether the statute will pass constitutional muster under a Commerce Clause analysis has yet to be tested.

Federal Legislative Proposals.

Federal legislation, if enacted into law, might preempt inconsistent state laws and could usefully establish nation-wide norms for regulating spam. As of October 2003, several anti-spam bills have been considered in the 108th Congress. Some legislative proposals call for a nationwide "do-not-email" list creating a registry of email addresses of individuals who wish not to receive unsolicited commercial email.

4. Search Engines.

Kelly v. Arriba Soft Corp., 336 F.3d 811 (9th Cir. 2003).

The Ninth Circuit issued a new decision after withdrawing its decision in *Kelly v. Arriba Soft Corp.*, 280 F.3d 934 (9th Cir. 2002).

A photographer sued Arriba for copyright infringement. Arriba operates a search engine that allowed users to search for images corresponding to search terms. Results were displayed as small, low-resolution "thumbnail" images, including those of the photographer's pictures. When a user clicked on the thumbnail image, a full-sized version of the image would be displayed (from the source website) in a

frame on Arriba's website. The Ninth Circuit found that Arriba's display of the "thumbnail" images was a fair use because the use was transformative – they were used for accessing information on the Internet, and not for the artistic expression they conveyed. Moreover, the "thumbnail" images were small, had low resolution, and lost clarity when enlarged. The court of appeals further noted that there was no market harm to the photographer's sales and licensing of his photographs because the "thumbnail" images would not be a substitute for the full-sized images, and also because the search engine did not sell or license images, and directed traffic to the photographer's website.

The Ninth Circuit remanded to the district court the issue of whether Arriba's display of full-sized images of the copyrighted photographs would be infringing, holding that the district court had impermissibly broadened the scope of the parties' motions, which did not seek summary judgment as to copyright infringement for the full-size images. (In its prior (withdrawn) decision, the Ninth Circuit had reversed the district court's determination that display of the full-sized images was a fair use.)

5. Peer-to-peer.

In re Aimster, 334 F.3d 643 (7th Cir. 2003).

Content owners successfully sued the owners and operators of the Aimster system (renamed Madster), which had been used to exchange music and other digital files over instant messaging services such as AOL Instant Messenger, as well as over the Internet generally. In upholding the district court's grant of a preliminary injunction, the Seventh Circuit, in an extensive opinion by Judge Posner, held that the

content owners were likely to succeed on their contributory infringement claim. The court, however, disagreed with the Ninth Circuit's suggestion in *Napster* "that actual knowledge of specific infringing uses is a sufficient condition for deeming a facilitator a contributory infringer."

The court applied a modified version of the *Sony Corp. v. Universal City Studios* device-based test that allows a service provider to avoid liability if it first demonstrates actual -- not simply possible — non-infringing uses of the service. Once a service provider establishes real, substantial non-infringing uses, the Seventh Circuit suggests that courts use a cost-benefit analysis to examine how much of a burden it would be for the service provider to eliminate or reduce infringing uses. If there are substantial noninfringing uses, then, unless the burden would be "disproportionately costly," the Seventh Circuit suggests the provider should be liable if it has constructive or actual knowledge of infringement.

Under this analysis, the Seventh Circuit held that Aimster was properly enjoined. The court found that Aimster had failed to demonstrate any actual non-infringing uses and, even assuming those non-infringing uses existed, Aimster had not proven that it would be disproportionately costly for it to police its system. The court rejected Aimster's argument that because the file transfers were encrypted, the service failed to satisfy the "knowledge" prong of the contributory liability test. The court noted: "Willful blindness is knowledge, in copyright law (where indeed it may be enough that the defendant should have known of the direct infringement), as it is in the law generally. . . . Aimster blinded itself in the hope that by doing so it might [avoid liability]."

Metro-*Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp. 2d 1029 (C.D. Cal. 2003).

Recording companies and motion picture studios sued the distributors of the Kazaa and Gnutella-based software used in connection with distributed peer-to-peer networks. A California district court distinguished the services at issue in *Napster* and *Aimster* (discussed above) from the software at issue in the case before it and declined to hold defendants liable for contributory or vicarious infringement.

As to contributory infringement, the court reasoned that the defendants distributed *products*, but did not provide services akin to Napster or Aimster. The court noted that the software was capable of noninfringing uses, but did not inquire as to the substantiality or commercial significance of those uses.

The court acknowledged that the defendants might have known that their software was used "illegally" by consumers. It held, however, that defendants did not have "actual knowledge of specific infringement ... at a time when . . . [d]efendant[s] materially contribute[d] to the alleged infringement, and [could] therefore do something about it."

As to the claims for vicarious copyright infringement, the court found that the defendants satisfied the "financial benefit" test. Unlike Napster, however, the defendants did not provide an "integrated service" that they could monitor and police. As such, they did not have ability to supervise and control the infringing conduct and, therefore, they would not be found vicariously liable.

The decision is on expedited appeal to the Ninth Circuit.

In re Verizon Internet Servs., Inc., Subpoena Enforcement Matter, 240 F. Supp. 2d 24 (D.D.C. 2003).

A district court granted the Recording Industry Association of America's (RIAA) motion to enforce its subpoena served on Verizon under Section 512(h) of the Digital Millennium Copyright Act (DMCA) in July 2002. Under Section 512(h), a copyright owner may request a clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer if certain conditions are met. The court rejected Verizon's argument that Section 512(h) applies only to service providers that store infringing materials on their own systems and not to service providers, such as Verizon, which merely transmit the infringing materials over its network.

In re Verizon Internet Servs., Inc., Subpoena Enforcement Matter, 257 F. Supp. 2d 244 (D.D.C. 2003).

In another case involving a subpoena under Section 512(h), a district court denied Verizon's motion to quash an RIAA subpoena served on Verizon. The court rejected Verizon's argument that § 512(h) violates Article III of the Constitution because it authorizes federal courts to issue subpoenas in the absence of a pending case or controversy. The court ruled that the issuance of a Section 512(h) subpoena is a non-judicial "ministerial task," requiring no

exercise of the clerk's discretion, and therefore does not implicate Article III judicial power.

The court also rejected Verizon's claim that Section 512(h) violates the First Amendment rights of Internet users to preserve their anonymity. The court held that the DMCA does not regulate protected expression or otherwise permit prior restraint of protected speech. The court further found that the DMCA provides sufficient procedures protecting the First Amendment rights of Internet users (such as a requiring a sworn declaration by the copyright owner stipulating the purpose for which the subpoena is sought). Finally, though the court acknowledged that the Section 512(h) subpoena may have a "marginal impact" on the expressive or anonymity rights of Internet users, it found that such impact is "outweighed by the extent of copyright infringement over the Internet through peer-to-peer file sharing."

The decision is on appeal to the D.C. Circuit.

6. Pop-up Advertising.

U-Haul Int'l, Inc. v. WhenU.com, Inc.,
No. 02-1469-A, 2003 U.S. Dist. LEXIS 15710
(E.D. Va. 2003).

WhenU.com is a vendor of software that displays targeted pop-up advertisements on various websites to users that have downloaded the software. The software scans the user's Internet activity for commonly used search phrases, visited websites and keyword algorithms. A Virginia district court held that the software vendor is not liable for trademark or copyright infringement based on the appearance of the pop-up ads.

With respect to the copyright claims, the display right was not infringed because the pop-up advertisements lie on top of the web site, in a separate window, with the computer user, not the program, controlling the display on the desktop. Nor was the derivative work right infringed: the program did not alter the web site in any way and the pop-up advertisements were a "distinct" and "transitory" occurrence.

As to the trademark claim, the court held that U-Haul had failed to establish that WhenU.com had used the plaintiff's marks in commerce because defendant did not guarantee to any advertiser that its ad will be shown when a consumer visits a particular website; did not display plaintiff's mark to consumers and did not interact with plaintiff's website to hinder or impede user access to the site.

7. DMCA.

Model Legislation/State Legislation

The Motion Picture Association of America ("MPAA"), with communication service providers, including cable operators and programmers, has drafted model communications security legislation, referred to by some commentators and critics as a "Super-DMCA." The purpose of the legislation is to provide comprehensive legal protection for all broadband and Internet-based services against unauthorized access, receipt, transmission and decryption. These interests have been lobbying state legislatures to adopt these or similar measures.

The model legislation proposes criminal and civil liability for knowingly, and with an intent to defraud, engaging in activities that include the following:

- Development, distribution, promotion, possession or use of any "communication device" in connection with the theft, receipt, decryption or transmission of a communication service without the express authorization or consent of the service provider.

- Concealment of the origin or destination of a communication from any communication service provider or modification of a communication device in connection with the above referenced prohibited activities.

- Development, distribution, promotion, possession or use of any "unlawful access device," defined as a device or technology that is primarily designed, developed and used to circumvent any effective device or technology instituted to protect a communication service or transmission from unauthorized access.

- Preparation, distribution, promotion, possession or use of plans or instructions for the creation of an unlawful access device or communication device for any prohibited purposes.

- Preparation, distribution, promotion, possession or use of material with the knowledge that a third party or purchaser intends to use the material to create a communication device or an unlawful access device for a prohibited purpose.

Several states have enacted legislation based on or including elements of this model, including Pennsylvania in 2000, Delaware and Maryland in

2001, Illinois, Michigan and Virginia in 2002, and Arkansas and Florida in 2003. Several other states are currently considering similar legislation.

Supporters of the legislation argue that these protections are necessary to protect e-commerce and ensure that content owners will continue to provide programming and other products in digital format. Detractors argue that the legislation is overbroad and vague, would chill technological innovation and the sale of legitimate devices, and would restrict fair use.

Lexmark Intern., Inc. v. Static Control Components, Inc., 253 F. Supp. 2d 943 (E.D. Ky. 2003).

Lexmark, the computer printer manufacturer, sued Static Control Components ("SCC"), a manufacturer of replacement printer toner cartridges, for violating the anti-circumvention provisions of the DMCA. Lexmark's products contain copyrighted toner loading programs, which use an authentication sequence to prevent the use of unauthorized toner cartridges in its printers. SCC's products circumvented the Lexmark sequence, allowing unauthorized toner cartridges to be used in Lexmark's printers.

In granting a preliminary injunction, the district court found that Lexmark had demonstrated a likelihood of success on its claims that SCC's products violated the DMCA's anti-circumvention provisions by allowing unauthorized access to Lexmark's toner loading and printer engine programs. The court noted that Lexmark's products were protected by the DMCA, as the statute does not require that the protected copyrighted work have an independent market value, only that the work – in this case software – was entitled to protection under the Copyright Act.

The court concluded that SCC's products were prohibited by the plain language of the DMCA because their primary purpose was to circumvent Lexmark's access controls. The products did not qualify for the reverse-engineering exception contained in 17 U.S.C. § 1201(f) because SCC's identical copying of Lexmark's program 1) did not provide access to independently created computer programs, and 2) constituted copyright infringement.

SCC has appealed the preliminary injunction and filed a countersuit against Lexmark alleging a violation of the federal antitrust laws. The Copyright Office issued a Notice of Inquiry with respect to whether there should be an exemption from section 1201(a)(1) for access to computer programs embedded in computer printers, toner cartridges and the like. *See* 68 Fed. Reg. 6678 (Feb. 10, 2003).

Chamberlain Group, Inc. v. Skylink Technologies, Inc., No. 02-C-6376, 2003 WL 22038638 (N.D. Ill. Aug. 29, 2003).

Chamberlain, an electronic garage door opener ("GDO") manufacturer, sued Skylink, a competitor that distributed a universal remote control that could be used to operate certain Chamberlain GDOs. The Chamberlain GDOs utilized a system to prevent unauthorized devices from operating the GDOs, and included computer programs in the transmitters and receivers. Chamberlain alleged that Skylink's universal remote circumvented the protections included in the GDOs and allowed unauthorized access to the copyrighted computer programs.

In August of 2003, the district court denied Chamberlain's motion for summary judgment on its claims that Skylink's product violated the anti-

circumvention provision of Section 1201 of the DMCA. The court concluded that even though the Skylink GDO has multiple, presumably legitimate purposes, because a single setting operated the Chamberlain GDO, the existence of the other purposes was not sufficient to deny summary judgment.

In addition, the court found that there were genuine issues of material fact as to whether the computer program was copyrightable and whether the owners of Chamberlain GDOs had been authorized to use the Skylink universal remote to operate the GDOs. In particular, the court noted that under Chamberlain's interpretation of the DMCA, a homeowner who lost the Chamberlain remote and managed to circumvent the GDO's access control measures to open his garage would be in violation of the DMCA; the court thought that this result would be at odds with the history of universal remote garage door openers, which had created a legitimate expectation by consumers that they could open their garage doors even if they lost the original transmitter.

8. California Law Relating to Personal Information, CAL. CIV. CODE §§ 1798.82, 1798.84 (2002).

Effective as of July 2003, California law requires an entity that conducts business in California and owns or licenses computerized data that includes personal information to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California (not just customers) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." The law defines "personal information" as an individual's

name *in combination with* his or her social security number, driver's license number, California Identification Card number, or other specified financial information. A "breach" is defined to mean unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of that personal information.

Disclosure of the breach must be made "in the most expedient time possible and without unreasonable delay." Notice may be provided by actual written or electronic notice, substitute notice (e.g., through a website or media), in cases where the cost or administrative burden would be excessive, or through a company's own notification procedures as part of an information security policy.

9. Obscenity and Indecency.

United States v. American Library Association, 123 S. Ct. 2297 (2003).

The Supreme Court held that the Children's Internet Protection Act (CIPA), 20 U.S.C. § 7001, § 9134 and § 254(h), enacted by Congress in 2000, was not unconstitutional. CIPA requires that public schools and libraries install Internet filtering software in order to be eligible for universal service discounts and federal funding for telecommunications services, computers, Internet service, and other technology. A three-judge district court held that CIPA was unconstitutional because libraries cannot technologically implement filtering software without blocking constitutionally protected speech, and enjoined the FCC from withholding funds from public libraries that declined to install the blocking technology. 201 F. Supp. 2d 401 (E.D. Pa. 2002).

The Court, in reversing, was clearly influenced by its views that Congress could condition receipt of federal funding on compliance with its policy objectives. It held that CIPA's funding incentives did not facially violate the First Amendment. For the plurality, Chief Justice Rehnquist held that a public library ought not be regarded as a public forum because libraries, traditionally, exercise discretion in selecting the content available to their patron. Nor is Internet access in a public library but, merely, a "technological extension of the book stack." Accordingly, it would be improper to apply a strict scrutiny analysis to CIPA.

Applying rational basis scrutiny, the Court emphasized that libraries have discretion over their collections and found that CIPA's requirements were rationally related to the state's interest in protecting minors. The Court rejected purportedly less restrictive alternatives as unworkable. It conceded, however, that filtering software "overblocked," by screening out material that would not harm minors. It concluded that CIPA alleviated these concerns by allowing library patrons to request to have the filtering software disabled.

In two separate concurrences, Justices Kennedy and Breyer emphasized that CIPA might not survive an as-applied challenge by an adult who could show that her use of the Internet had been burdened (i.e., because, in fact, it is not easy to ask a librarian to unblock a filter). Justice Breyer would have applied a "heightened" but not strict "scrutiny" test."

Justice Stevens dissented, arguing that CIPA violated the First Amendment by inhibiting the ability of

authors to reach the widest possible audience. In a separate dissent, Justice Souter, joined by Justice Ginsburg, noted that CIPA only says that librarians "may" unblock a website on a patron's request, not that they "must"; they would have concluded that CIPA was an unconstitutional condition imposed on libraries. Justice Souter concluded that this language was not adequate to address the problem of "overblocking."

American Civil Liberties Union v. Ashcroft, 322 F.3d 240 (3d Cir. 2003).

In the next phase of judicial consideration of the Child Online Protection Act (COPA), the Third Circuit unanimously upheld the injunction against enforcement of the Act. The Supreme Court had vacated the Third Circuit's decision affirming the district court's grant of an injunction and remanded the case in May 2002. 535 U.S. 564 (2002).

On remand, the court of appeals determined that COPA could not survive a strict scrutiny analysis because it affected a wide range of speech, subjecting to liability all publishers who communicate for "commercial purposes," whether for-profit or not. It also concluded that the "community standards" test was overly restrictive, as applied to the Internet, a global medium. The court also held that plaintiffs were likely to be able to prove that the statute was overbroad.

The Third Circuit also concluded that COPA did not use the "least restrictive means" to protect minors, as both blocking and filtering were technological alternatives. The court of appeals also held that the statute's use of the term "minor" was impermissibly

vague, because it embraced all children under the age seventeen, without regard to whether the banned material might appeal to their prurient interests or be suitable for them or not. The court also held that the affirmative defenses themselves would chill protected speech and burden Web publishers.

The United States petitioned for certiorari on August 11, 2003.

American Booksellers Foundation for Free Expression v. Dean, 342 F.3d 96 (2d Cir. 2003).

The Second Circuit affirmed the district court's issuance of a permanent injunction against enforcement of a Vermont statute that prohibited distribution to minors of sexually explicit material "harmful to minors." The statute violated both the First Amendment and dormant Commerce Clause, the court of appeals held, because it prohibited material placed on a website or sent to an internet discussion group. The court of appeals stated that the statute is not narrowly tailored, as the state's goals could be achieved through alternative means, such as filtering technologies, and through "luring" statutes. Moreover, as a sender might not know whether a minor was present in those online venues, expression constitutionally protected for adults would be impermissibly chilled.

Finally, the Second Circuit analyzed the Commerce Clause implications of the statute. Like other courts of appeals reviewing other similar state statutes, the Second Circuit concluded that because the Vermont law had extraterritorial effects, it presented a per se violation of the dormant Commerce Clause.