ADDITIONAL DEVELOPMENTS—CYBERLAW

ACCESS NOW, INC. V. SOUTHWEST AIRLINES, CO.

227 F. Supp. 2d 1312 (S.D. Fla. 2002)

The court held that Southwest Airlines, Co.'s ("Southwest") website, southwest.com, is not a "place of public accommodation" within the meaning of the American's with Disabilities Act (ADA) and that Access Now, Inc. ("Access Now") did not establish a nexus between Southwest's website and a physical, concrete place of public accommodation.

Access Now is a nonprofit organization that advocates access for disabled persons. Access Now, together with Robert Gumson, a blind individual, filed a complaint alleging that Southwest's website violated the ADA by excluding blind persons, who were unable to access the goods and services offered at the website's virtual ticket counters because of their disability. Southwest does not provide alternate text that works with a screen reader program and voice synthesizer software for the blind. Southwest moved to dismiss the complaint, arguing that southwest.com is not a place of public accommodation and therefore fell outside the scope of Title III of the ADA.

The court examined whether an Internet website is a "place of public accommodation" under the definition of the ADA. Looking to the plain language of the statute, the court noted that the statute specifically identified twelve categories of public places, and the applicable federal regulations defined a "place of public accommodation" as a physical, concrete place. Stating that a court must follow the legislative directive where Congress has specifically enumerated rights and set forth clear standards, the court refused to expand the definition to include a website, which is not a physical, concrete place. It found that the terms refer to physical, concrete structures and do not apply to an Internet website. Accordingly, the court rejected Access Now's argument that southwest.com is a place of "exhibition, display and a sales establishment" and therefore within the scope of Title III of the ADA. The court also stated that the website was not a means for accessing a physical accommodation, unlike the fast finger telephone selection process used in the game show in *Rendon v. Valleycrest Productions, Ltd.*, 294 F.3d 1279 (11th Cir. 2002). Since Access Now failed to demonstrate a nexus between the website and a physical, concrete place, the court granted Southwest's motion to dismiss the complaint.

ALLEN V. COMMISSIONER OF LABOR

100 N.Y.2d 282 (2003)

The New York Court of Appeals held that physical presence determines the state in which an interstate telecommuter would be eligible for unemployment insurance benefits.

Maxine Allen was employed with Reuters America, Inc. ("Reuters"). Initially, she both resided and worked in New York City, where Reuters was based, but she later relocated to Florida. Reuters allowed Allen to "telecommute," or link via the Internet to the New York office, though she was still required to adhere to all of the same policies as an employee who was localized in New York. During this time, Allen traveled to the New York office only once for a period two weeks. Reuters offered her a job in the New York office, but Allen declined. She filed a claim for unemployment insurance benefits in Florida, but her claim was denied on the grounds that Allen had quit her job without good cause. Allen then filed an interstate claim for New York unemployment insurance benefits and received $365 per week. Six months later, the New York Commissioner concluded that Allen's employment was localized in Florida. Furthermore Allen was charged $8,395 (the amount she had received as a result of her false statement that she worked at her employer's New York address). The Unemployment Insurance Appeal Board upheld the findings.

The New York Court of Appeals affirmed the Board's decision. The court reviewed the case de novo and held that the matter was one of pure statutory reading and analysis. The court read the definition of employment to mean that an individual's work will be localized in the place where most of his or her work was done despite any incidental, temporary or transitory work that was done outside of that state. Relying on *In re Mallia*, 299 N.Y. 232 (1949), the court explained that section 511 of the New York Labor Law sets out four tests to define employment: localization, location of base of operations, source of direction or control, and employee's residence. The court held that physical, and not virtual, presence would continue to be used as the indicator of workplace location. New York and most other states have adopted this uniform definition of employment with the goal of creating uniformity among the states and ending uncertainty in the application of state unemployment compensation rules. The court also found that a claimant's false statement of fact, even if unintentional, permitted the recovery of benefits already received due to the false statement.

AMERICA ONLINE, INC. V. NAM TAI ELECTRONICS, INC.

571 S.E. 2d 128 (Va. 2002)

The Supreme Court of Virginia ordered America Online, Inc. ("AOL") to reveal the identity of a subscriber who posted allegedly false and defamatory information about Nam Tai Electronics ("Nam Tai") on a Yahoo! chat board. The order honored a subpoena order stemming from Nam Tai's pending action in California state court for violation of California's unfair business practices law. Despite AOL's motion to quash the subpoena, the Virginia Supreme Court ruled that enforcing the subpoena does not violate principles of comity.

Nam Tai's complaint, filed in Los Angeles County Superior Court, accused fifty-one unknown individuals of posting "false, defamatory, and otherwise unlawful messages" on a message board devoted to discussing Nam Tai's publicly traded stock. Nam Tai sought to discover the identity of the subscriber who used the Yahoo! login name "scovey2" to post messages disparaging the value of the company and its products. Based on information revealed by Yahoo! under a California subpoena *duces tecum*, Nam Tai matched the login "scovey2" to a specific AOL subscriber. Nam Tai next sought and obtained a commission for out-of-state discovery and demanded that AOL reveal scovey2's identity.

In response, AOL filed a motion in the Circuit Court of Loudoun County, Virginia, to quash Nam Tai's subpoena *duces tecum*, based on concerns regarding the "well-established First Amendment right to speak anonymously" and Nam Tai's alleged failure to demonstrate that its California action was legally viable. The Virginia trial court refused to quash the subpoena, and AOL appealed to the Virginia Supreme Court, which applied an abuse of discretion standard to affirm the lower court's action.

The court stated that the important question is whether the substantive law of the foreign jurisdiction is "reasonably comparable to that of Virginia." AOL argued that the *ex parte* nature of the proceedings in California against the John Doe defendants produced a "superficial" judgment that "was not the product of a full-fledged, adversarial consideration of the First Amendment issues at the core of this matter." Nonetheless, the Virginia Supreme Court held that the Virginia trial court had not erred in honoring the California court's order to reveal the unknown subscriber's identity. The court concluded that the California court's commission for out-of-state discovery was entitled to comity because the First Amendment concerns applicable to California law are the same concerns applicable to Virginia law and are for the California courts, not the Virginia courts, to determine.

While the court's reasoning focuses on the doctrine of comity, the denial of AOL's motion to quash the subpoena *duces tecum* raises important policy concerns. As AOL argued, protecting anonymous speech is a well-established value. Although the court admitted that John Doe cases present awkward pleading problems, it found that the *ex parte* nature of the proceeding is not detrimental enough to thwart otherwise legitimate out-of-state discovery.

In future cases, these First Amendment concerns may play a more prominent role at the trial court level of the original action. However, *Nam Tai* illustrates that, barring abuse of discretion, comity probably requires courts to honor such subpoenas until a state changes its own commission for out-of-state discovery.

ARONSON V. BRIGHT-TEETH NOW, LLC

824 A.2d 320 (Pa. Super. Ct. 2003)

MISSOURI V. AMERICAN BLAST FAX, INC.

323 F.3d 649 (8th Cir. 2003)

CALIFORNIA ANTI-SPAM LEGISLATION

A.B. 1769 (2002), A.B. 2944 (2002), S.B. 1560 (2002), S.B. 186 (2003)

Several significant court decisions and legislative developments have taken place regarding the regulation of spam. They stem from the Telephone Consumer Protection Act of 1991 ("TCPA"), 47 U.S.C. § 227 (2000). The TCPA was intended primarily to restrict the use of prerecorded messages in telemarketing and to preclude marketers from sending advertisements to fax machines.

In *Aronson v. Bright-Teeth Now LLC*, the Superior Court of Pennsylvania held that the TCPA does not extend to unsolicited e-mails. Aronson sued a company that sent him unsolicited e-mails and alleged a violation of the TCPA's prohibition on junk faxes. The plaintiff asserted that his personal computer, through the use of a modem and printer, met the statutory definition of "facsimile machine." The appellate court affirmed the dismissal of the claim. It relied on standard principles of statutory construction and distinguished computer from fax machines. Whereas fax machines transcribe messages instantly, computers store messages for users to delete unopened, read the message later, or print the message. Since a personal computer could not be defined as a "fax machine" under the TCPA, the court ruled that the TCPA did not apply and that the trial court properly dismissed the complaint.

The TCPA fared better in *Missouri v. American Blast Fax*. The Eighth Circuit held that the unsolicited fax provisions do not violate the First Amendment. The State of Missouri sued two fax advertisement companies for violating the TCPA's prohibition on junk faxes. The district court dismissed the claim, finding that the junk fax provisions of the TCPA violated the First Amendment guarantee of freedom of speech. Missouri appealed, and the United States intervened.

The Eighth Circuit reversed. The court applied the *Central Hudson* test, which governs the constitutionality of regulations of commercial speech. Under the test, the court asks four questions: whether (1) the commercial speech is unlawful or misleading; (2) the government has a substantial interest in regulating the commercial speech; (3) the regulation directly advances the government interest; and (4) the regulation is narrowly tailored. Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557 (1980). Both parties conceded the lawfulness of the commercial speech in the first prong, which is a threshold question. The court found the TCPA's legislative history and the evidentiary hearings at trial sufficiently showed the government's substantial interest in preventing advertisers from shifting the costs of junk faxes to recipients and placing "interference" upon recipients. The court also concluded that the TCPA directly promoted the government interest, without undue extension. Finally, the court countered the assertion that the relevant provision was overbroad, distinguishing cases that had overturned regulations that sought to protect the public from the content of the speech, to implement policies

unrelated to the speech, or that were so broad as to "constitute nearly a complete ban on the communication of truthful information" about a commercial product.

Since Congress is justified in relying on as little as "simple common sense" in distinguishing between various types of speech, the TCPA's distinction between commercial and noncommercial fax advertising was justified in the view of the court; the distinction is relevant to the TCPA's goal of reducing costs and interference associated with unwanted faxes. Moreover, while the TCPA also distinguishes between unsolicited fax advertisements and live telemarketing calls, this is consistent with the TCPA's goal of protecting the public from bearing the costs of unwanted advertising. Although the TCPA generally permits telemarketing calls unless a consumer has registered his or her objection, calls are prohibited when they result in costs to the recipient. Calls made to pagers or cellular phones fall under this prohibition. The court held that the TCPA's junk fax provision satisfied the constitutional test for regulation of commercial speech and, therefore, withstood First Amendment scrutiny.

The Eighth Circuit's holding immediately led to speculation that the principles relied upon by the court could readily be extended to support the constitutionality of federal legislation regulating e-mail spam. Congress passed such legislation, passing the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act), Pub. L. No. 108-187, 117 Stat. 2699, and the law went into effect on January 1, 2004. This Act requires unsolicited commercial e-mail to be properly labeled and to include opt-out instructions and the sender's physical address, and proscribes deceptive subject lines and false headers. It also authorizes the FTC to establish a national "do not e-mail" register. The Act preempts state laws requiring labels on unsolicited commercial e-mail or prohibiting such messages, but laws merely addressing falsity and deception remain in force.

California recently has passed significant legislation in order to protect consumers. Assembly Bill 2944, 2002 Legis., Reg. Sess. (Cal. 2002), repeals California's relatively weak "opt-out" junk fax law, while making clear that the TCPA's stronger "opt-in" junk fax provisions apply within the state. Assembly Bill 1769, 2002 Legis., Reg. Sess. (Cal. 2002), generally prohibits the transmission of unsolicited advertisements through text-messaging systems used on cellular phones and other mobile devices registered to California residents. California also changed its "do not call" law: starting in April 2003, Californians become eligible to add their phone numbers to the "do not call" list, which telemarketers must buy from the attorney general's office and may be fined for violating. S.B. 1560, 2002 Legis., Reg. Sess. (Cal. 2002). California had passed Senate Bill 186 in early 2003, which would have made it illegal to send unsolicited commercial e-mail from California or to a California e-mail address, but the CAN-SPAM Act pre-empts it and provides weaker protection against spam.

While the TCPA's regulation of junk faxes appears strengthened, it remains to be seen whether the CAN-SPAM Act of 2003 will be efficacious or, if challenged, will withstand First Amendment or other challenges. Although federal e-mail spam regulation was long-anticipated, many have already contended that the CAN-SPAM Act will be of little utility compared to stronger laws, such as S.B. 186, requiring consumers to "opt-in" for such e-mails. Unsolicited commercial advertising will likely to continue to be a source of judicial and legislative developments.

KREMEN V. COHEN

337 F.3d 1024 (9th Cir. 2003)

The Ninth Circuit held that under California law a domain name is a type of intangible property protected by the tort of conversion.

Kremen registered the domain name "sex.com" to Online Classifieds, Inc. ("OCI") with the registrar Network Solutions, Inc. ("NSI"). He did not develop the website. Eighteen months later, NSI received a letter that purported to be from OCI. The letter requested that NSI cancel Kremen's registration and allow Cohen to register the domain name. NSI accepted the letter without question and transferred "sex.com" to Cohen, who created a profitable Internet-based pornography business. When Kremen discovered the transfer, he demanded that NSI correct the false registration, but NSI said it could not do so without a court order. Kremen sued Cohen in federal court for damages and to recover the sex.com registration. The district court found the letter to be a forgery, ordered NSI to transfer sex.com back to Kremen, and awarded Kremen $65 million in damages. Unable to enforce the $65 million judgment against Cohen, who became a fugitive, Kremen sued NSI under contract and tort theories, including the tort of conversion. The district court granted summary judgment to NSI on all of Kremen's claims. Kremen appealed.

Citing the impropriety of a federal court ruling first on an issue of state tort law, the Ninth Circuit certified two questions to the California Supreme Court: (1) whether California conversion law requires an intangible property right to be "merged" with a document and if so, (2) whether the tort protects Internet domain names. Kremen v. Cohen, 325 F.3d 1035 (9th Cir. 2003). The California Supreme Court declined. *Kremen*, 2003 Cal. LEXIS 1342, No. S112591 (Cal. Feb. 25, 2003). The Ninth Circuit then ruled on the issues.

The court affirmed the dismissal of the contract claims. However, it reversed on the tort claims. The Restatement (Second) of Torts § 242 (1965) has a strict merger requirement, but the Ninth Circuit noted that the majority of cases in California do not follow the Restatement. The court stated that if such as requirement exists at all, it is minimal. The intangible property only needs some connection to a document or tangible object. The court found that Kremen's domain name was connected with the Domain Name System (DNS), a record of who owns each domain name, and that the DNS is a document. The court found it immaterial that the DNS stored ownership data in electronic form because California law already protected information stored on floppy discs, audio records, and magnetic tape. Drawing an analogy to shares of stock (protected intangible property), the court found it immaterial that the DNS is a collection of databases that are updated regularly and held that intangible property does not have be merged with a single, static document.

The court also concluded that the district court's policy rationales were insufficient to bar the tort of conversion. The Ninth Circuit stated that further regulation would be desirable if it would prevent a company from handing away someone else's property. In addition, though the tort has a strict liability standard, the court believed that no liability would be worse. Finally, the court stated that the question may be better left to the legislature, but common law applies until the legislature determines otherwise.

EF CULTURAL TRAVEL BV V. ZEFER CORP.

318 F.3d 58 (1st Cir. 2003)

The First Circuit held that the "reasonable expectations" test is inappropriate for determining lack of authorization under the Computer Fraud and Abuse Act ("CFAA"). A software maker, though it was not named in the ordering language of the preliminary injunction against its client, is bound by the injunction. Moreover, the injunction does not violate the defendant's First Amendment rights.

Former employees of EF Cultural Travel BV ("EF") founded Explorica, Inc. and hired Zefer Corporation ("Zefer") to write a computer program (a "scraper tool") that would collect two years of pricing information from EF's website. After downloading the data into a spreadsheet, Explorica then set prices about five percent lower than EF's quotes. When Explorica sued EF in an unrelated action for back wages, EF learned of the scraping tool during discovery. EF then sued Explorica, some of Explorica's employees, and Zefer in federal court. EF alleged violations of the Copyright Act and the CFAA. The district court denied EF's copyright claims. However, the district court applied a provision of the CFAA that prohibits access of a protected computer with the intent to defraud and granted a preliminary injunction against all defendants, who all appealed. The First Circuit upheld the injunction against Explorica, but Zefer's appeal was automatically stayed after it filed for bankruptcy. Zefer reactivated its appeal after the stay was lifted.

The First Circuit affirmed the district court, but narrowed the grounds for the injunction against Zefer. The court rejected EF's arguments that Zefer breached confidentiality agreements, since Zefer and EF had not entered into such an agreement. The court also found that the information used in creating the scraper was publicly available, and it was uncertain whether Zefer knew that this information was improperly obtained by Explorica. Zefer did not contest the fraud element, so the issue before the First Circuit was whether Zefer lacked authorization to use the scraper. The First Circuit agreed with the district court that a lack of authorization may be implicit instead of explicit, but rejected the test that the lower court applied. It reasoned that it is far simpler for companies to explicitly forbid certain uses and accesses than to burden the public with lengthy, imprecise litigation about "reasonable expectations." Therefore, the court concluded that website providers should state what "non-password protected access they purport to forbid."

Nonetheless, the court did not vacate the preliminary injunction against Zefer. Although the district court did not name Zefer in its order, the Eighth Circuit ruled that the injunction precludes anyone with notice, including Zefer, from aiding or acting on behalf of Explorica in violating the decree. Finally, the court noted that the injunction does not forbid the general use of scrapers, but merely restrains Zefer from helping Explorica exploit confidential information. Accordingly, the court held that the injunction does not violate the First Amendment. Thus, it upheld the injunction.

PAVLOVICH V. SUPERIOR COURT

58 P.3d 2 (Cal. 2002)

In *Pavlovich v. Superior Court*, a California-based plaintiff sued a defendant who had never been to California and had never conducted business in California, but who had posted information on an Internet website that reached Californians. The California Supreme Court determined that under the particular facts of the case, the trial court could not properly exercise personal jurisdiction over the defendant.

The DVD Copy Control Association, Inc. ("DVD CCA") is a Delaware-based non-profit trade association with its principal place of business in California. Created in December 1998 by the DVD industry, DVD CCA controls and administers licensing of Content Scrambling System ("CSS") technology, a system that encrypts and protects copyrighted motion pictures on DVDs. DVD CCA began administering the licenses in December 1999. Soon thereafter, it acquired the licensing rights to the CSS technology and became the sole licensing entity for this technology in the DVD video format. Defendant Mathew Pavlovich ("Pavlovich") is the president of Media Driver, LLC, a technology consulting company in Texas. Pavlovich is a resident of Texas, and lived in Indiana prior to moving to Texas. In addition, he does not work in California and has not solicited any business in California.

While in Indiana, Pavlovich was the founder of a project to improve video and DVD support for the GNU/Linux operating system. To achieve this goal, the project sought to defeat the CSS technology and thus enable the playback of DVDs on GNU/Linux-based computers. Pavlovich posted the source code of DeCSS, which allows users to decrypt data contained on DVDs, on the project website around October 1999. Pavlovich knew that DeCSS that it was derived from CSS algorithms and that reverse engineering the algorithms was probably illegal.

In late 1999, DVD CCA filed a complaint in California against Pavlovich and other defendants for misappropriation of trade secrets. The complaint alleged that Pavlovich, by posting the DECSS program, had repeatedly published DVD CCA's trade secrets and copyrighted material on the Internet. Pavlovich protested that the California courts lacked jurisdiction over him. After the state trial and appellate courts ruled against him, Pavlovich appealed to the California Supreme Court.

The court stated that the test for determining specific jurisdiction over a nonresident defendant had three prongs: (1) whether "the defendant has purposefully availed himself or herself of forum benefits"; (2) whether the suit is related to or arises out of the defendant's contact with the forum; and (3) whether "the assertion of personal jurisdiction would comport with fair play and substantial justice." The court focused on the first prong, and found that posting information on a passive website on the Internet was not, in itself, "purposeful availment" sufficient to subject Pavlovich to jurisdiction in California. Instead, DVD CCA was required to show that Pavlovich "*expressly aimed* [his] tortious conduct at the forum." Mere knowledge of possible harm, by itself, was insufficient to establish purposeful availment under the effects test. To hold otherwise, the court stated, "would effectively subject all intentional tortfeasors whose conduct may harm industries in California to jurisdiction in California."

The court concluded that the evidence in the record failed to show that Pavlovich expressly aimed his tortious conduct at California or that his conduct intentionally targeted California.

SEARCH KING, INC. V. GOOGLE TECHNOLOGY, INC.

No. CIV-02-1457-M, 2003 WL 21464568 (W.D. Okla. May 27, 2003)

The district court held that website rankings were protected free speech and were lawful; therefore, plaintiff's claim for tortious interference with contractual relations was without merit.

Google, Inc. ("Google"), a popular online search engine, uses its proprietary "PageRank" algorithm to return results in response to user-supplied Internet search queries. This algorithm depends on various factors, including the number of links to a site, to rank sites with scores indicating their relevance to the search terms. Search King, Inc. was an online seller of advertising space, who sought out highly-ranked websites for their clients' advertisements. Search King compensated the websites with a portion of the fee—based in part on the PageRank of the website—charged to its clients. When the PageRank scores of Search King and its affiliates dropped, Search King claimed that it suffered financially and sued Google for tortious interference with contractual relations. Search King's request for a preliminary injunction was denied, and the court examined Google's motion to dismiss the suit.

The issue before the court was whether Google's devaluation of Search King's PageRank results was malicious and wrongful. Google argued that PageRanks are opinions protected by the First Amendment. Search King argued that the PageRank algorithm was patented and professed by its creator to be "objectively verifiable." Therefore, PageRanks were not ideas or expressions protected by free speech, and Google's interference was unlawful. The court rejected Search King's argument, finding that although the process in PageRank's algorithm is objective, it produced results that are fundamentally subjective in nature, since each search engine's method of determining rankings is "unique." Finding no way to prove Google's PageRank "false," the court concluded that Google's PageRank results are subjective opinions entitled to full constitutional protection. Protected speech cannot be tortious interference with contractual relations, thus the court ruled that Search King had failed to state a claim upon which relief could be granted and dismissed the suit.

USA PATRIOT ACT UPDATE

Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 8 U.S.C., 18 U.S.C., 42 U.S.C., and 50 U.S.C.)

Legal and legislative efforts to define more precisely the constitutional scope of the government's authority to conduct Internet and electronic surveillances under the USA PATRIOT Act ("Patriot Act") are continuing.

On the legal front, the Foreign Intelligence Surveillance Court of Review ruled in November 2002 that the Department of Justice ("DOJ") has broad discretion to use wiretaps and other surveillance measures to track suspected terrorists and spies. *In re* Sealed Case No. 02-001, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002) (per curiam). The decision overturned an earlier ruling by the secret Foreign Intelligence Surveillance Court, which held that there must be a well-defined wall separating domestic police agencies from spy agencies. The Court of Review stated the Patriot Act's expansion of the wiretap guidelines made any such wall obsolete and unnecessary. In overturning the lower court, the Court of Review found "no definitive jurisprudential answer" to the question of constitutionality, but it upheld the amendments to the guidelines because the authorized surveillances "certainly come close" to meeting minimal constitutional standards regarding searches and seizures and therefore are reasonable.

Separately, a federal judge judge in California declared unconstitutional a portion of the Patriot Act that prohibits giving expert advice or assistance to groups designated as international terrorist organizations. The judge found that ban impermissibly vague, in violation of the First and Fifth Amendments. Humanitarian Law Project v. Ashcroft, CV 03-6107 ABC (MCx), 2004 U.S. Dist. LEXIS 926 (C.D. Cal. Jan. 23, 2004).

In Congress, Sen. Larry Craig (R-Idaho) in October 2003 introduced the Security and Freedom Ensured Act ("SAFE"), H.R. 3352, 108th Cong. (2003), to amend the Patriot Act by placing limits on current police practices relating to surveillance and search warrants. SAFE would, among other things, roll back "sneak-and-peek" searches that allow searches without having to notify the target, establish expiration dates on nationwide search warrants, and prohibit law enforcement agents from obtaining library records without a reason supported by specific facts. In response, Attorney General Ashcroft warned that President Bush would veto any legislation that curtails the Patriot Act. President Bush urged Congress in his annual State of the Union address to renew key provisions of the Patriot Act, such as warrantless Internet surveillances, which are due to expire in December 2005.

Also in Congress, a divided House Judiciary Committee killed a bill, which would have barred the surveillance of people or groups engaged in legal activities if law enforcement lacks "particularized suspicion" to justify the surveillance.

The DOJ, responding to questions by the House Judiciary Committee, released an extensive report in late 2002 detailing how it has used the Patriot Act to conduct Internet and electronic surveillance. Letter from Daniel J. Bryant, Assistant Attorney General, Office of Legislative Affairs, U.S. Department of Justice, to F. James Sensenbrenner, Jr., Chairman, Committee on the Judiciary, U.S. House of Representatives (Jul. 26, 2002), *available at* http://www.house.gov/judiciary/patriotresponses01702.pdf. The report stated that the DOJ had made relatively limited use of its new powers, sharing intelligence information from criminal grand juries with other agencies on forty occasions in thirty-eight jurisdictions nationwide, and sharing information from regular criminal wiretaps twice. Some of the information in the report was deemed classified, and has not been

made available to the public. This classified information included answers to questions concerning the number of times that the DOJ has used its new powers to obtain roving surveillance orders. The American Civil Liberties Union last year sued the DOJ under the Freedom of Information Act seeking disclosure of information related to this classified information. The court held that the information could be withheld on national security grounds. ACLU v. U.S. Dep't of Justice, 265 F. Supp. 2d 20 (D.D.C. 2003).

President Bush also took steps last year to address threats to the nation's technological infrastructure by releasing a policy statement. The White House, National Strategy to Secure Cyberspace (2003), *at* http://www.whitehouse.gov/pcipb/cyverspace_strategy.pdf. The statement calls for the government to cooperate with private industry to create an emergency response system to cyber attacks, to establish a threat and vulnerability reduction program, to improve security training and awareness, to protect the government's own systems and to work internationally to address security issues. As part of this plan and the Homeland Security Act of 2002, the Department of Homeland Security created the National Cyber Security Division, which operates under the Department's Information Analysis and Infrastructure Protection Directorate.