Significant Developments in Global Internet Law in 2002
INTRODUCTION

1 CONTENT AND JURISDICTION

- Protection of Minors
- Hate Speech
- Filtering and Technological Measures
- ISP Liability for Illegal Speech
- Liability for the Content of Others
- Jurisdiction over Internet Content Disputes
- Anonymous Speech
- Accessibility

2 PRIVACY AND DATA PROTECTION

- Increased Surveillance Capability
- Data Retention
- Privacy in Electronic Commerce
- Data Protection
- Workplace Privacy
- Encryption

3 INTELLECTUAL PROPERTY

- General Copyright Developments
- Digital Rights Management
- Database Protection and Deep Linking
- Peer-to-Peer Technologies
- Domain Name Disputes
- Metatags and Pay-for-Placement Searches
- Reseller's Use of Trademark
- Internet-based Protests
- Patent Developments

4 ELECTRONIC COMMERCE, CONSUMER PROTECTION AND TAXATION

- Electronic Contracting
- Securities and Banking
- Clickwrap Agreements
- Terms of Internet Service
- Authentication
- Regulation of Unsolicited Commercial Email
- Internet Taxation
- Advisory Tax Opinions
- Other Consumer Protection Developments
- E-Commerce Jurisdiction

5 NETWORK SECURITY

- Disclosure of Security Breaches
- Critical Infrastructure Information Disclosures
- Mandatory Disclosure of Breaches of Personal Information
- Cybercrime Legislation
- Cybercrime Prosecutions
- International Cooperation
TOP TEN DEVELOPMENTS IN GLOBAL INTERNET LAW

1. **Anti-terrorism legislation pits security against personal privacy.** The Homeland Security Act in the United States and new legislation in Europe, South America, Asia and Africa, increased law enforcement surveillance capacity. In Europe and elsewhere, “data retention” proposals raised the potential for massive data files to be held on the Internet and telecommunications movements of all online citizens.

2. **The battle over peer-to-peer technologies and online piracy.** Content owners continued their fight against file-sharing systems that allow users to connect directly without using a centralized server. The music industry won a judgment against Kazaa in Amsterdam, but that verdict was reversed by an appellate court. A suit against the software’s owner in the United States has resulted in a preliminary injunction. In Japan, Finland and England, strong decisions against infringement bolstered the content industries’ efforts.

3. **Internet publishers cope with global jurisdiction over defamation disputes.** In a closely watched case, Dow Jones v. Gutnick, the Australian High Court held that a U.S.-based publication must defend libel litigation in Australia based solely on Internet distribution of an article. Courts in Zimbabwe, Italy and France found jurisdiction over distant Internet publishers as well.

4. **New cybercrime legislation.** As intrusions into essential computer systems continued and viruses and worms targeted businesses and consumers alike, legislatures around the globe tightened penalties for cybercrime. The U.S. Homeland Security Act increased penalties for cyberattacks, and the European Commission and the Council on Europe proposed new penalties for cybercrime.

5. **New data protection measures.** A new European Union data protection directive requires companies to give subscribers notice and an opportunity to opt out before putting a cookie on their computer, and new interpretations of the existing data protection directive continue to evolve to keep pace with the Internet. The U.S. Federal Trade Commission continued enforcement actions based on privacy and consumer protection laws.

6. **The battle for digital rights management.** It was a challenging year for advocates of anti-piracy technologies. In the United States, the Digital Millennium Copyright Act’s anti-circumvention provision was upheld against constitutional challenge but a company being prosecuted under that provision was acquitted by a jury. In Norway, a teenager who cracked the film industry’s code to prevent copying of DVD films was acquitted of hacking. In Australia, chips permitting game consoles to play pirated software were found not to violate Australia’s copyright act.

7. **New tools regulate spam.** In the European Union, a new directive limits the distribution of unsolicited commercial email for direct marketing to customers who have consented to it. New legislation in six states was passed, resulting in more than half of U.S. states requiring labelling of spam and an opt-out opportunity. Following California and Washington court decisions upholding spam regulation statutes against constitutional challenge, enforcement actions were taken by those states’ attorneys general.

8. **The scope of copyright defined.** The U.S. Supreme Court in Eldred v. Ashcroft held that Congress had broad authority to extend the term of copyright. The case focused national and international attention on the balance between copyright and free speech in the digital era.

9. **Council of Europe treaty on hate speech.** After the crafting of an addition to the Cybercrime Treaty on hate speech, European laws criminalizing speech based on ideas that incite unlawful discrimination will be applied to Internet speech in an increasing number of countries -- excluding the United States, which will not sign the treaty.

10. **Mandatory disclosure of security breaches.** A new concept in network security law was created. The Homeland Security Act requires disclosure of breaches to “critical infrastructure,” and new legislation in California requires notification to the state of any breach of a computer system that results in the unauthorized acquisition of personal information.
INTRODUCTION

The year 2002 was a turning point in the development of Internet law. Strong protections for freedom of expression and constitutional due process in jurisdictional disputes continued to develop in the United States. In many other countries, however, courts persisted in applying restrictive local defamation and content-liability laws to distant Internet publishers. Government oversight and increased surveillance, borne of U.S. and global legislative efforts to combat terrorism, continued to provoke debate on the balance between national security and personal privacy. By contrast, privacy rights in the commercial realm posted strong gains in the United States, Europe and Asia, as legislators sought to regulate unsolicited commercial email and misuse of personal data. The battle over intellectual property on the Internet intensified, with the content industries’ novel victory against Napster now seeming straightforward in the face of more complex and elusive peer-to-peer technologies such as Kazaa. And the emerging law of network security continued to expand as more nations enacted cybercrime legislation and prosecuted those who violate the integrity of information systems.

This overview of significant developments in Internet law is designed to be precisely that – an overview. We have selected certain key cases and laws from countries around the globe that, in our practice and experience, best represent the emerging trends in Internet law. There are, of course, thousands of cases, laws and regulations that touch on aspects of the Internet that we could not mention here. If you would like to discuss a matter not addressed in this report, or otherwise would like to inquire about any of the reported cases and laws, please let us know.

This summary was reported by Daniel J. Hirsch, Davendra Kumar, Jeffrey M. Rosenfeld, Tuan N. Samahon, John M. Smith, Lisa Peets and E. Jason Albert and edited by Kurt Wimmer in London, Mark Plotkin in Washington, Bert Wells in New York, and Evan Cox in San Francisco. For more detailed treatment of these and other issues, please see our treatise, Information Technology and Electronic Commerce: Law & Practice, to be released by Aspen Publishers in April 2003.

This report provides general information, not legal advice as to any specific matter, and should not be used as a substitute for appropriate legal advice.
1 CONTENT AND JURISDICTION

Courts in the United States continued to grant Internet content a high degree of constitutional protection, and tests for jurisdiction over content-related disputes became more predictable. Elsewhere, however, developments were more troubling. The 44-member state Council of Europe drafted an additional protocol to its cybercrime treaty that would require nations ratifying it to ban racist and xenophobic speech on the Internet. Moreover, courts in several nations continued the global trend toward exercising jurisdiction over Internet defamation and content disputes involving distant publishers and applying potentially restrictive local laws.

Protection of Minors

• The United States Supreme Court held in Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002), that the Child Pornography Prevention Act violates the First Amendment to the U.S. Constitution. The Act criminalized possession and distribution of any image that "appears to be" or "conveys the impression" of a minor engaging in sexually explicit conduct. The Court rejected the government's argument that the Act's prohibition of virtual child pornography was necessary to prevent pedophiles from using such material to seduce minors, noting that such reasoning could not justify banning speech that was fit for adults. In response, the House passed the 2002 Child Obscenity and Pornography Prevention Act. The bill would apply only to computer-generated images that were indistinguishable from non-virtual child pornography, and would create an affirmative defense if the defendant can show that no actual minors were used in the creation of the images. The Senate failed to pass this legislation, however, and it died with the adjournment of the 107th Congress.

• Somewhat by contrast, in Ashcroft v. ACLU, 535 U.S. 564 (2002), the Supreme Court upheld the Child Online Protection Act's use of local "community standards" to evaluate Internet pornography. The plurality opinion noted that local standards would apply only to the question of whether the material appealed to the prurient interest, while national standards would determine whether the material had serious literary, artistic, political, or scientific value. The latter determination would ensure that appellate courts could narrow the scope of what is deemed to be harmful to minors under the Act.

Hate Speech

• In November 2002, the Council of Europe approved an additional protocol to the 2001 Cybercrime Convention. Parties that ratify the new protocol are required to outlaw racist and xenophobic material, which includes any denials of the Holocaust. The Protocol applies to "any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors."

• In Canada, the Canadian Human Rights Tribunal, in Citron v. Zündel, T460/1596 (Can. H.R. Trib. 2002) applied the Canadian Human Rights Act to a website that published Holocaust denials and other hate speech directed at Jews.

• The Federal Court of Australia ruled in Jones v. Toben, 2002 F.C.A. 1150 (2002), that a website containing material that denied the Holocaust violates the Racial Discrimination Act.
• In Norway v. Tvedt (Asker and Bærum Dist. Ct. 2002), a Norwegian court convicted a man for posting racist material on a website and sentenced him to 75 days imprisonment (although the sentence included time for other crimes as well).

Filtering and Technological Measures

• In American Library Association v. United States, 201 F. Supp. 2d 401 (E.D. Pa. 2002), a federal district court struck down a provision of the Children's Internet Protection Act that conditioned public libraries’ receipt of federal funding on their installation of content-filtering software. The court, relying on evidence that filtering software blocks access to significant amounts of protected speech, found that the Act unconstitutionally conditioned federal funds by inducing public libraries to use filtering software that restricted access to speech protected by the First Amendment. The Supreme Court has accepted the government’s appeal.

• In an effort to implement a technological solution to segregate child-friendly content on the Internet, Congress passed the Dot Kids Implementation and Efficiency Act, which mandates creation of a new second-level .kids domain within the top-level .us domain. The new domain, .kids.us, would contain only content deemed suitable for children of ages 12 and below. The .kids domain would restrict peer-to-peer communications and chat rooms, prohibit hyperlinks to sites outside the kids.us domain, and would be monitored for objectionable content.

ISP Liability for Illegal Speech

• In the U.S., some states sought to control online access to child pornography by targeting Internet service providers (ISPs). Pennsylvania enacted the Internet Child Pornography Act, which requires ISPs to disable access to child pornography within five days of being notified by the Pennsylvania state attorney general’s office. The statute makes clear that the ISP has no duty to monitor its Internet service actively for violations of child pornography laws. In September, a Pennsylvania trial court issued an order pursuant to the Act requiring Worldcom and affiliated ISPs to block a number of sites that were identified as hosting child pornography.

• In adopting an Additional Protocol to the 2001 Cybercrime Convention that would require signatories to ban online racist and xenophobic material, the Council of Europe noted that the provisions of the Protocol apply only to intentional acts. The Council specifically stated that service providers that merely served as conduits for speech would not be liable and that service providers were not required to monitor content.

• The European Parliament voted to favor self-regulation rather than mandatory blocking of Internet content. Although this unanimous vote does not have the effect of law, it indicated that the Parliament would resist efforts to force ISPs to restrict access to websites that were deemed objectionable. The parliament noted protection of minors from harmful Internet content “is primarily the responsibility of their legal guardians.”

Liability for the Content of Others

• Section 230 of the Communications Decency Act grants immunity to “providers of interactive computer services” for content provided by third-party “information content providers.” In Gentry v. eBay, 121 Cal. Rptr. 2d 703 (Cal. Ct. App. 2002),
the court held that Section 230 granted eBay immunity from a lawsuit alleging that it failed to furnish certificates of authenticity for items sold on its auction website. The descriptions of the items were provided by the seller, making eBay immune from liability stemming from allegedly fraudulent descriptions.

- A federal court in Smith v. Intercosmos Media Group d/b/a Directnic.com, No. Civ. A. 02-1964 (E.D. La. Dec. 17, 2002), held that Section 230 granted immunity to an ISP in a defamation suit arising from postings by one of its customers. The court also held that the CDA's immunity applied not only to money damages but also to injunctive relief.

- In a rare case in which a court declined to grant immunity under the CDA, a federal court in Carafano v. Metrosplash.com, Inc., 207 F. Supp. 2d 1055 (C.D. Cal. 2002), held that a "matchmaking" website took too active a role in the creation of its member profiles to qualify for immunity under Section 230 of the CDA. The member profiles on the matchmaking site were created by answering a detailed questionnaire authored by the website. The court concluded that the matchmaking site was partly responsible for the creation and development of the content of the member profiles, and therefore did not qualify for immunity.

- In Germany, the Microsoft Network was found liable for content placed on its server by a third party. In Graf v. Microsoft GmbH, OLGZ Cologne, No. 15 U 221/01, the High Regional Civil Court held that MSN was responsible for the posting of fake nude pictures of tennis star Steffi Graf in its "Celebrities" community. The objectionable content was posted by a user not affiliated with MSN, and MSN specifically stated on its site that it was not responsible for content posted by third parties. Nevertheless, the court held that an objective user would attribute the "Celebrities" community to MSN because it created the forum for publishing such pictures, stipulated the rules for participating in the community, and framed the community website with advertisements for Microsoft products.

- In France, two courts reached opposite conclusions when faced with the question of liability for allegedly defamatory material supplied by a third party. The Lyon Civil Court applied a rule of strict liability to find the editors of a discussion forum liable for defamatory statements made by third parties. In contrast, the Paris Civil Court held that an editor of an Internet discussion forum could not be held liable for statements made by third parties until notified of the presence of illegal content by a judicial authority.

**Jurisdiction over Internet Content Disputes**

- In the United States, Internet jurisdiction law continued to evolve to protect distant publishers. In Young v. New Haven Advocate, No. 01-2340 (4th Cir. June 3, 2002), the court held that allegedly defamatory articles posted on the websites of Connecticut publishers New Haven Advocate and Hartford Courant did not subject the newspapers to personal jurisdiction in Virginia when the articles were not aimed at a Virginia audience. The court held that it could not exercise jurisdiction over the newspapers even though the effect of the alleged defamation was felt by the plaintiff in his home state of Virginia. The court held that the defendant's Internet activity must be expressly targeted at the forum state for jurisdiction to be found.
• The court in Revell v. Lidov, No. 01-10521 (5th Cir. Dec. 31, 2002), reached a similar result in another case involving an allegedly defamatory Internet article. To exercise jurisdiction over an out-of-state defendant, the court found that it must examine “the geographic focus of the article” and not simply the location of the alleged harm. In this case, the plaintiff, a former FBI official, lived in Texas, but the allegedly defamatory article concerned his activities as a government official in Washington, D.C. Like the court in Young, the Revell court focused on whether the forum state was targeted by the defendant.

• Outside the U.S., however, courts have not followed the same approach. In a case closely watched by the world media, the High Court of Australia held in Dow Jones & Co. v. Gutnick, 2002 H.C.A. 56 (2002), that a U.S.-based publisher could be sued in Australia for an allegedly defamatory article that was published on the Internet. Dow Jones was found to be subject to jurisdiction in Victoria following an allegedly defamatory article that was published on Barron’s Online. The court concluded that Australian defamation law focused on the location of the harm rather than the location of the defendant’s activities. Because the plaintiff lived in Victoria, Australia, the court reasoned that his reputation would be harmed in Victoria, making it appropriate for Victorian courts to hear this case. The court noted that Dow Jones knew that the article was about Gutnick, and should have expected to be subject to a lawsuit in the forum in which the defendant resided. The court rejected Dow Jones’ arguments that its decision would make it impossible for publishers to determine what countries’ defamation law to follow, noting also that a plaintiff was likely to seek significant damages only in jurisdictions in which it actually has a reputation.

• Courts in England are well-known for receptivity to defamation suits against foreign publishers. Recognizing the increased risk and expense of being forced to defend a libel action in an English court, Dow Jones took the novel approach of asking a U.S. court to issue a declaratory judgment that it could not be liable in England for an allegedly defamatory article that was posted online. The court in Dow Jones & Co. v. Harrods Ltd., No. 02 Civ. 3979 (VM) (S.D.N.Y. Oct. 11, 2002), concluded that it could not issue an order preventing Dow Jones from being sued in a foreign forum.

• In France, the Paris Criminal Court ruled that it had jurisdiction to hear criminal charges against Yahoo! and a former executive, Timothy Koogle, because its U.S.-based website is accessible to users in France. The charges relate to complaints that the offer to sell Nazi memorabilia on Yahoo!’s auction site contravened French law. The charges were punishable by up to five years in prison and 46,000 euros (about $50,000). In early 2003, the court acquitted the defendants, finding that they did not condone Nazism or place favorable light on Nazi policies by allowing the sale of Nazi-related objects. The court did not alter its view on jurisdiction over the defendants, however.

• In Zimbabwe, Andrew Meldrum, an American journalist residing in Zimbabwe, was prosecuted on charges of “abuse of journalistic privileges by publishing falsehoods” on the basis of stories published in the Guardian in England and posted on its website. Even though the Guardian is unavailable in Zimbabwe, prosecutors asserted that Zimbabwe’s criminal courts have jurisdiction over any content published on the Internet if that content could be accessed in Zimbabwe. On July 15, 2002, Mr. Meldrum was acquitted but served with deportation papers; the judge in the case did not address the Guardian’s argument against jurisdiction.
• In Italy, police closed five websites that were critical of the Catholic Church, despite the fact that the sites were hosted in the United States. The Italian authors of the websites are being prosecuted under Italian laws criminalizing blasphemy and the publication of sacrilegious material. The sites were closed without the involvement of any court because the police investigating the sites accessed the computer by which the defendants uploaded content to the U.S. hosting services that published the sites and replaced the allegedly illegal content with a police crest.

Anonymous Speech

• Courts often have addressed the circumstances in which ISPs must disclose the identity of anonymous posters responsible for allegedly defamatory content (often critical of a plaintiff's business). In 2002, this issue arose in the novel context of peer-to-peer file sharing software.

• The Recording Industry Association of America (RIAA) sought the identity of an anonymous Verizon Internet access subscriber who allegedly traded copyrighted music on the Internet using the peer-to-peer file-sharing software Kazaa. Verizon, however, refused to comply with a subpoena requesting the name, address, and telephone number of the user in question, arguing that because it merely served as a passive conduit for the allegedly infringing material and did not store it on its servers, it should not be responsible for the infringing activities or for monitoring them. The court decided in favor of RIAA, holding that the Digital Millennium Copyright Act's provision allowing copyright holders to subpoena ISPs for information on alleged infringers applies to all ISPs within the meaning of the DMCA, and not just those that stored the allegedly infringing material. In re Verizon Internet Services Inc., No. 02-MS-0323 (D.D.C. Jan. 21, 2003). Verizon has appealed.

Accessibility

• In a case that tested the applicability of the Americans with Disabilities Act to websites, the federal district court in Access Now Inc. v. Southwest Airlines Co., 227 F. Supp. 2d 1312 (S.D. Fla. 2002), held that a website is not a place of public accommodation that must meet the accessibility requirements of the Act. The case involved the Southwest Airlines website, which allegedly did not allow the operation of technological tools used by blind Internet users. The court held that a place of public accommodation as defined by the Act had to be tied to a physical place.

• In Martin v. Metropolitan Atlanta Rapid Transit Authority, 225 F. Supp. 2d 1362 (N.D. Ga. 2002), however, a federal court reached a contrary conclusion, indicating that a website operated by the Metropolitan Atlanta Rapid Transit Authority that failed to work with technology used by blind Internet users likely violated the ADA.
2 PRIVACY AND DATA PROTECTION

Following the terrorist attacks on September 11, 2001, many governments worldwide introduced legislation to enhance law enforcement’s authority to monitor electronic communications. Throughout 2002, these anti-terrorism initiatives continued as nations struggled to balance privacy rights with increased capabilities for law enforcement. Steady growth in global e-commerce also has generated concerns over the commercial collection, use, and disclosure of personal information. Finally, countries continued to develop legal frameworks to guide and restrict the monitoring of employee email and Internet use.

Increased Surveillance Capability

- In the United States, President Bush signed into law the Homeland Security Act, which restructures segments of the federal government into a Homeland Security Department to prevent and respond to terrorism. The Act expands law enforcement authority to monitor electronic communications by (1) allowing ISPs to provide client communications voluntarily to any federal, state or local governmental authority if the ISP believes in good faith that an emergency involving the risk of death or serious injury justifies the release; (2) granting law enforcement officials the authority to install pen registers and trap and trace devices without a court order when confronting an ongoing attack on a protected computer; and (3) establishing protocols for the sharing of critical infrastructure information with the Homeland Security Department.

- Peru enacted a law that permits the interception of telecommunications and Internet traffic upon judicial authorization.

- President Álvaro Uribe Vélez of Columbia declared the country in a "state of internal commotion," and launched an initiative to intercept private electronic communications as an exceptional measure to repel terrorist attacks.

- South Africa enacted detailed legislation that will require telecommunication services and ISPs to render their services intercept-capable by installing equipment to enable government monitoring.

- In India, the Controller declared that any governmental agency may monitor electronic communications under the Information Technology Act of 2000. India also enacted the Prevention of Terrorism Act, which provides law enforcement officials with increased ability to intercept electronic communications; law enforcement officials have since used the Act to ban the use of long-distance telephone and Internet services in certain volatile areas such as Kashmir and Jammu.

- In Japan, the government employed the Communications Interception Law for the first time in May 2002, to track email and cellular phone use in a narcotics investigation.

Data Retention

- The European Union adopted the Electronic Communications Data Protection Directive. The Directive creates a new online data protection framework for issues including “data retention” — the holding by carriers of data that details subscriber use of the Internet and telecommunications systems, including e-mail addresses used, Internet addresses visited, telephone numbers dialled, digital
location information and other traffic data. In a sea change compared to traditional surveillance, carriers will be required to retain data for all subscribers, rather than targeted retention for specific individuals under investigation, to permit law enforcement to mine the retained data after an incident.

- The new Directive, which must be implemented by each EU member state by July 2004, repeals prior law requiring subscriber information to be destroyed. It permits EU member states to require ISPs and telecommunications carriers to retain traffic data. Retention may be required for a "limited" but indeterminate duration for traffic data, which may include websites visited and email addresses employed; retention periods discussed in various member states range from 12 months to five years.

- In late 2002, the Danish presidency of the EU proposed a statement of principles calling for consultation on the harmonization of European data retention and human rights laws. The Danish Presidency also circulated a questionnaire among member states to gain additional information about their data retention requirements at present and their views on possible EU-wide data retention legislation.

- Individual EU member states grappled with data retention proposals. In the United Kingdom, privacy commissioner Elizabeth France issued an opinion holding that inconsistencies between the Regulation of Investigatory Powers Act and the Anti-Terrorism Act of 2001 violate data protection principles and the Human Rights Act. She warned that while the laws enable the retention of data to preserve national security, that data could then be accessed through a warrantless procedure for relatively minor investigations.

- In June, the U.K. Home Office announced a plan to expand the list of organizations that could engage in warrantless surveillance of Internet use, including many regulatory and tax agencies having no connection with anti-terrorism actions, but quickly abandoned this plan following widespread press and public criticism. On August 1, a new data interception law requiring ISPs to acquire the ability to intercept and store electronic communications went into effect in the U.K.

- According to a leaked April 2002 European Council of Justice Ministers report, Ireland’s Minister for Public Enterprise directed licensed telecommunications operators to retain existing traffic data and future traffic data for not less than three years after the date of their generation pursuant to the 1983 Postal and Telecommunications Services Act.

- In Germany, the Bundesrat ratified legislation setting the minimum duration of data retention by ISPs to 12 months.

- France approved the Programming for Internal Security law in August. This act grants law enforcement direct access to the personal data of Internet users retained by telecom operators and ISPs under earlier data retention legislation.

- In Spain, Parliament approved the Law of Information Society Services and Electronic Commerce, which requires network operators to retain traffic data for all of its subscribers for 12 months. Prior to its passage, the Spanish data protection agency expressed its disapproval of this framework on data protection grounds.
• In Switzerland, a new Federal Law on the Surveillance of Mail and Telecommunications requires ISPs to maintain adequate systems to retain traffic data for six months. The law, however, disallows preventive surveillance, and only authorizes interception of communications for a specific list of criminal offenses.

• In Denmark, Parliament ratified an anti-terrorism bill that requires ISPs to retain traffic data for twelve months, and permits law enforcement officials to monitor electronic communications through the use of surveillance software that records keystroke data.

• In Canada, the Department of Justice released a consultation document on lawful government access to retained data in August. The Department prepared the document to gather the input of industry stakeholders in anticipation of Canada's ratification of the Council of Europe's 2001 Convention on Cybercrime. The Canadian government noted the need to amend the criminal code to provide for production and data-preservation orders, as well as the enactment of an offence to criminalize the creation of computer viruses, even before they are deployed.

Privacy in Electronic Commerce

• Although new surveillance laws raised the spectre of eroding personal privacy in 2002, the year was replete with legislative efforts to curb commercial misuse of personal information on the Internet.

• In the U.S. Senate, the Online Personal Privacy Act would have required opt-in consent for sensitive information and opt-out consent for all other information. In the U.S. House of Representatives, the Consumer Privacy Protection Act of 2002 would have required companies to self-certify that they provide opt-out consent and adequate security measures for personal information. Neither bill, however, passed.

• In the absence of a federal law, individual states took legislative measures to protect the privacy of online information. Minnesota enacted a privacy law that requires ISPs to offer their customers either opt-in or opt-out procedures regarding the disclosure of their personal information. California passed a law requiring the encryption of Social Security numbers transmitted over the Internet.

• The U.S. Federal Trade Commission also took enforcement actions. In January, the FTC announced a settlement with Eli Lilly and Co. under which the company would be required to reword its privacy policy and enhance its information security after the company accidentally released personal information collected through its Prozac.com website. Separately, Microsoft agreed to reword its privacy policy for its Passport services and submit to a security audit every two years. The FTC also negotiated a settlement regarding the Etch-A-Sketch and Pop Corn websites, which it accused of violating the Children's Online Privacy Protection Act by conditioning children's access to website activities on disclosure of extraneous personal information without obtaining verifiable parental consent and by failing to describe in a privacy policy how collected information would be used. The FTC also released a study that revealed that a majority of children's websites failed to comply with the law.

• Courts have addressed these issues as well. For example, in In re Pharmatrak, Inc. Privacy Litigation, 220 F. Supp.2d 4 (D.Mass. 2002), the court found that a
website tracking firm’s use of web bugs and cookies to amass personal information about visitors to a pharmaceutical website did not violate the Wiretap Act, the Stored Communications Act, or the Computer Fraud and Abuse Act.

Data Protection

- The European Union adopted a new directive adding specific data protection principles for Internet issues. Under the new Electronic Communications Data Protection Directive, website operators must notify users if they use cookies or similar files and provide them with an opportunity to opt out of receiving them.

- A paper by the Article 29 Working Party, an EU group composed of representatives from national data protection authorities, declared that the installation of cookies on the computers of EU residents constitutes a use of equipment governed by the EU Data Protection Directive. Under this view, the law of the user’s country applies to issues between the European consumer and the website operator, even if the website operator is outside the European Union.

- The European Commission reviewed the compliance of Microsoft’s Passport system, which collects personal data from Internet users, with the Directive. This review culminated in a January 2003 report on online authentication systems (including Passport) issued by the Article 29 Working Party. The report made several recommendations as to how such systems should comply with the Directive. The paper also listed a number of changes Microsoft agreed to make to Passport to enhance user privacy, including providing a prompt box containing key information about Passport’s privacy practices to EU residents and clearly separating creation of a Passport account from provision of personal information.

- Several European countries ratified legislation to bring their data protection laws into compliance with the EU Data Protection Directive. EU members France and Ireland introduced legislation to implement the Directive. Accession countries Bulgaria, Estonia, Latvia, Lithuania and the Slovak Republic likewise implemented data protection legislation, as did the Russian Federation.

- The European Commission announced that the Canadian Personal Information Protection and Electronic Documents Act ensures an adequate level of protection for purposes of the EU Data Protection Directive, thus permitting personal data to be transferred freely between Europe and Canada.

- The influence of European standards for data protection was felt far beyond Europe. In the Asia Pacific region, the Internet Industry Association of Australia announced it would draft a code, as a self-regulatory initiative, to bring itself into compliance with the requirements of the EU Data Protection Directive.

- In Malaysia, the Ministry of Energy, Communications, and Multimedia continued to draft the Personal Data Protection Act, which has been delayed by increasing requests for exemptions. Additionally, Malaysia developed a General Consumer Code of Practice for the Internet, which among other things, provides guidelines for the commercial collection, use, and disclosure of personal information.

- Although Singapore has no overarching data protection law, its National Internet Advisory Committee issued a Model Data Protection Code for the Private Sector in February, which provides voluntary guidelines on the collection and use of personal information.
• Data protection principles became embodied in industry codes in Asia. Hong Kong's Privacy Commissioner, Hong Kong's Consumer Council, and the Office of the Telecommunications Authority released a voluntary code setting forth guidelines for the commercial use of subscriber personal information by telecommunication companies.

• In Japan, as directed by the Internet Provider Responsibility Law, Japanese ISPs issued draft guidelines governing the collection, use, and disclosure of personal information. The guidelines permit the deletion of user information and restrict disclosure of information without explicit user consent.

• South Korea established the Personal Data Dispute Resolution Committee to facilitate settlements between ISPs and users regarding the protection of personal information.

• The Law Commission of South Africa announced it would develop a comprehensive national privacy law over the next two years. The Electronic Communications and Transactions Act was signed into law, and provides limited data protection in e-commerce ventures to fill the gaps left by the lack of a privacy law. Under the Act, an entity that collects information may voluntarily subscribe to certain use and disclosure restrictions, which will then be governed by contract law.

Workplace Privacy

• Workplace privacy continued to be a controversial issue. In Konop v. Hawaiian Airlines Inc., 302 F.3d 868 (9th Cir. 2002), an airline pilot who alleged that his employer obtained unauthorized access to his protected website could state a claim for violation of the Stored Communications Act and the Railway Labor Act, but not the federal Wiretap Act. In United States v. Angevine, 281 F.3d 1130 (10th Cir. 2002), the court found that a university professor lacked a reasonable expectation of privacy in child pornography files he downloaded onto his office computer because the university’s computer use policy explained the university’s right to periodically view files on its computers. In United States v. Bunnell, 201 F.Supp.2d 169 (D.Me. 2002), the court found that a student lacked a reasonable expectation of privacy in child pornography files he had downloaded onto his allotted portion of a shared-usage university computer system.

• In Muick v. Glenayre Electronics, 280 F.3d 741 (7th Cir. 2002) and TBG Insurance Services Corp. v. Superior Court of Los Angeles County 117 Cal.Rptr.2d 155 (2002), the respective courts found that a company computer use policy, which reserved the rights to periodically inspect laptop computers that had been issued to employees, eliminated any reasonable expectation of privacy in files on the computers. In Kelleher v. City of Reading, No. Civ. A 01-3386 (E.D.Pa. May 29, 2002) and Garrity v. John Hancock Mutual Life Insurance Co., No. Civ. A-00-12143 RWZ (D.Mass. May 7, 2002), the respective courts found that employees lacked a reasonable expectation of privacy in workplace e-mail given the presence of policies that qualified the confidentiality of all messages. However, in United States v. Slanina, 283 F.3d 670 (5th Cir. 2002), vacated on other grounds, 313 F.3d 891 (5th Cir. 2002), the court stated that absent a computer use policy to the contrary, a municipal employee has a constitutionally protected privacy interest in materials stored on his office computer.
• In Canada, the data protection commission issued an opinion finding that the monitoring of an employee’s Internet preferences and email use violates the express terms of Canadian data privacy legislation because blanket monitoring of electronic communication fell short of being a proportional response to the perceived threat of personal use of communications systems.

• In Europe, as in Canada, employee rights under data protection legislation have led to an approach that provides more protection for employees and less potential for monitoring by employers. At the EU level, the Article 29 Working Party released the Surveillance of Electronic Communications in the Workplace Report. That report stresses prevention over detection of abuse, and cites the principles of transparency, necessity, fairness, and proportionality in determining whether monitoring of employee email of Internet use is justified.

• The U.K. Information Commissioner issued segments of the Employment Practices Data Protection Code, which outlines practical aspects of employers’ surveillance of Internet and email use and the procedures for storing employees’ personal data.

• In Belgium, a common agreement regulating the electronic surveillance of Internet and email use at the workplace entered into force. The guidelines express a general prohibition against the monitoring of electronic communications.

• In Denmark, the City Court of Kalundborg found that an employer was justified in dismissing an employee for sending private emails while at work despite the absence of a computer-use policy. Similarly, the City Court of Lyngby ruled that the defendant rightly dismissed an employee who had edited and forwarded a racist email message.

• The Hungarian Data Protection Commissioner issued a non-binding opinion finding that employers should distinguish between email accounts used solely by an employee for personal purposes and accounts used for work-related purposes when determining whether surveillance is justified.

• A committee established by the Swedish government to investigate workplace privacy issued a report calling for legislation to protect personal data of employees. Specifically, the report advocated the restriction of employers’ surveillance of employee email and Internet use.

• The European approach toward protecting employee privacy has made headway in Asia as well. The Hong Kong Privacy Commissioner issued a Draft Code of Practice on Monitoring and Personal Data Privacy at Work, which considers the surveillance of employee email, telephone, and Internet use. Under the Draft Code, employers may only monitor employee activity if they possess evidence of criminal activity or other serious malfeasance, and such checks may only be performed for a limited duration and retained employee data must be purged after six months.

• South Korean police arrested three individuals for illegally monitoring employees’ emails. The prosecution marks the first prominent action in what is recognized as a pervasive issue in South Korea.
Encryption

- The use of strong encryption technology has been deregulated to a great degree. However, the U.S. government has continued to enforce restrictions on exporting encryption technologies to certain nations. The Department of Commerce levied a $95,000 fine against Neopoint Inc. for violating federal encryption control laws when it exported 128-bit encryption technology to South Korea, and the Department of Defense rejected Commerce Department proposals to ease encryption export restrictions to certain “friendly countries,” including Australia, Singapore, Mexico, and South Korea.
3 INTELLECTUAL PROPERTY

Governments around the world continued to adapt intellectual property laws to the digital world. As copyright holders continue to struggle with online piracy, confronted with the growing popularity of second generation peer-to-peer networks, several decisions made clear that infringers and those who assist them would still be subject to liability. However, copyright owners did not find much comfort in the decisions relating to the circumvention of technological barriers. This year’s developments in trademark law continue to clarify the relationship between trademark ownership and the right to claim domain names incorporating that mark. Further decisions addressed the right of trademark owners to prevent competitors from using their marks as embedded, invisible metatags in websites. Finally, the U.S. Supreme Court delivered a landmark patent decision at the beginning of 2003, clarifying the relationship between the doctrine of equivalents and patent estoppel.

General Copyright Developments

- In Eldred v. Ashcroft, 123 S. Ct. 769 (2003), a case that focused significant national and international debate on the proper scope of copyright, the United States Supreme Court rejected a challenge to the constitutionality of the Copyright Extension Act of 1998, which extended the term of existing and future copyrights by 20 years. The copyright extension kept copyrighted materials from being released into the public domain, including such classics as Casablanca and Gone with the Wind as well as the version of Mickey Mouse portrayed in Disney’s earliest films. In a 7-2 decision, the Court held that the Constitution “gives Congress wide leeway to prescribe ‘limited times’ for copyright protection and allows Congress to secure the same level and duration of protection for all copyright holders, present and future,” and concluded that in extending the term of copyrights, Congress was acting within its authority.

- Last year, the European Union approved a landmark Directive harmonizing EU-wide rules governing copyright in the digital age and enabling the EU to ratify the 1996 WIPO treaties. That Directive was due to be implemented in each of the 15 member states of the EU by the end of 2002. Only Denmark and Greece met the deadline. Most of the member states have draft legislation in process and continue to work towards implementing the Directive.

- Several EU Member States, including Finland, France, Germany, the Netherlands and Portugal, introduced legislation that would extend so-called “private copy” levies to digital media and equipment used for storing and reproducing copyrighted works. These levies, administered by powerful national collecting societies, are designed to compensate right holders for authorized private copies of their works made by users. In some markets, the levies proposed would extend to PCs and would be relatively significant in amount (one proposal in Germany suggested a levy of $30 on each personal computer). Information technology associations Europe-wide have opposed these levies, concerned that the higher cost of computing equipment could have a negative impact on the growth of e-commerce and Internet usage.

Digital Rights Management

- Several cases suggested that courts (and juries) would not broadly apply laws designed to prevent circumvention of technological barriers protecting copyrighted works.
• In the first major test of the criminal provisions of the Digital Millennium Copyright Act's anti-circumvention measures, a federal court rejected preliminary challenges to the criminal prosecution of a Russian software company and one of its employees for violation of the anti-circumvention provisions of the DMCA, but the jury ultimately acquitted the defendants. United States v. Elcom Ltd., a/k/a ElcomSoft, 203 F. Supp. 2d 1111 (N.D. Cal. 2002). The defendants sold software that allowed users to remove copying restrictions embedded in digital books. In a motion before trial, the defendants challenged the constitutionality of the DMCA. The court held that the statute is constitutional and that it does not create a general exception for circumvention to engage in fair use of copyrighted materials. At trial, however, the jury found that ElcomSoft was not guilty of violating the DMCA. The defense evidently succeeded in convincing the jury that ElcomSoft did not "willfully" break the law, even though senior executives of the software company testified that they were aware of the DMCA. The acquittal was viewed as a major blow for the prospect of criminal enforcement of the DMCA.

• A further challenge to the DMCA was filed but not decided in Edelman v. N2H2, Inc. No. 02-11503-RGS (D. Mass filed July 25, 2002), which challenged the constitutionality of portions of the statute. Edelman sued a company that produces software that is used as an Internet filter, blocking access to certain websites, seeking a declaratory judgment that he has First Amendment and fair use rights to examine the full list of sites contained in N2H2's Internet blocking program and to share his research tools and results with others. Edelman claimed that in order to access the list of sites, he would have to "reverse engineer" the software program and create a software tool to circumvent the measures that prevent users from accessing a readable version of the list. The case is still pending.

• A Norwegian teenager was acquitted by the Oslo City Court in early 2003 of charges related to his hacking of the film industry's technological protection system. The film industry had developed the Content Scrambling System ("CSS") to encrypt and prevent the illegal copying of DVD films. CSS also prevented DVD films from being played on unauthorized equipment. Jon Lech Johansen developed and posted a program called DeCSS on the Internet. The film industry reacted strongly to Johansen's program because DeCSS "unlocked" the films and not only allowed them to be played on unauthorized equipment, but also allowed the films to be copied and distributed digitally. Johansen was charged under a Norwegian law prohibiting illegal access to data, but the Norwegian court dismissed the charges. The court held that one cannot be convicted for gaining access to the data on a legally purchased DVD, and found no proof that Johansen or others had used the program to access illegal pirate copies of films.

• In Australia, a federal court ruled that "mod chips" used to enable Sony's PlayStations to play illegally copied games, did not circumvent technological protection measures in violation of the Australian Copyright Act of 1996. Kabushiki Kaisha Sony Computer Entertainment v. Stevens. The court held that the Sony technology that "mod chips" circumvented did not qualify as a "technological protection measure" under the Act because it was not designed, in the ordinary course of its operation, to prevent or inhibit the infringement of copyright in a work.
Database Protection and Deep Linking

- In the EU, the Database Directive grants copyright protection to database creators for “selecting and arranging” the information contained in the database, even if the creator does not own copyrights in the underlying collected material.

- The Paris Court of Appeals held that under the Database Directive (which France adopted in 1998), databases composed of photographs and biographies in the public domain should be granted intellectual property protection because the creator had selected the contents. The EU legislation also provides protection against “unfair extraction” of material in a database, and specifically prohibits downloading and hyperlinking to extract the underlying information. In contrast to the EU, in the U.S., legislation specifically providing protection to databases has been proposed but never enacted.

- Several cases in Europe demonstrate the impact of the Database Directive on the issue of deep linking. “Deep linking” refers to the practice of linking from one website to another, bypassing the homepage of the site being linked to. In Europe, database rights increasingly have been used to prevent unwanted deep linking. For example, in Mainpost v. Newsclub, a German newspaper sued Newsclub, a search engine, successfully arguing that Newsclub infringed on its database rights by searching through and directly linking to Mainpost's news stories in its database.

- In a similar case in Denmark, Danish Newspapers Publishers’ Association v. Newsbooster.com, the defendant created links to those on-line newspaper stories for its subscribers. The court found for the plaintiff, holding that the website of a newspaper constituted a database, and that Newsbooster’s linking violated the newspaper’s rights under the Danish implementation of the Database Directive. The Dutch Supreme Court reached a similar result in Dutch Assoc. of Real Estate Agents (NVM) v. De Telegraaf finding that the defendant had infringed the plaintiff’s database rights by linking to an online collection of houses for sale.

- In the U.S., the Ninth Circuit decided a case concerning linking (but that did not raise database protection issues). In Kelly v. Arriba, 280 F.3d 934 (9th Cir. 2002), the plaintiff, a professional photographer who displayed his photographs on a website, sued an Internet search engine that displays results in the form of small “thumbnail” pictures. By clicking on a thumbnail, a user of the search engine can view a larger version of the image which is displayed on the search engine website without directing the user to the target website. The court found that the search engine's use of the thumbnails was a fair use and thus did not constitute copyright infringement. As to the framing of full-sized copyrighted images, however, the court found that the site violated the photographer's public display right. The copyright owner has filed a motion for rehearing.

Peer-to-Peer Technologies and Contributory Infringement

- Although copyright infringement litigation ultimately shut down Napster, peer-to-peer piracy gained momentum in 2002. Second-generation file sharing services, such as Kazaa, Morpheus, and Grokster, based on a decentralized structure under which individuals connect directly to one another’s computers without the need for a centralized coordinating server, have made responding to online piracy more complex.
• In 2001, an Amsterdam district court had found that Kazaa’s file sharing software encouraged copyright infringement and ordered Kazaa BV to stop the distribution of its software. In 2002, a Dutch appeals court reversed the lower court’s ruling, holding that Kazaa was not liable for copyright infringement on account of the illegal actions of people using its software. Buma/Stemra v. Kazaa.

• In Japan, in contrast, a Tokyo District Court issued an injunction banning an online music file-sharing service by MMO Japan Ltd., and held that the company was responsible for the copyright violations committed by the users of its service.

• Finally, a Finnish court ruled that MP3 file sharing violated the Finnish Copyright Act. A college student in Finland was sharing MP3 music files through a peer-to-peer network called CuteMX. The court stated that the defendant should have realized that the MP3 files he uploaded would be downloaded by others, and the fact that he received no financial benefit was immaterial.

• In the United States, record companies and movie studios sued Sharman Networks, the company that owns the Kazaa file-sharing software. Sharman is incorporated in the Pacific island nation of Vanuatu and headquartered in Australia, but in early 2003 a California federal judge rejected Sharman’s motion to dismiss the lawsuit based on lack of jurisdiction. Sharman had argued that it was not bound by U.S. laws since it did not have substantial contacts with California. The court disagreed on the basis that the software was downloaded and used by millions of Californians. The court’s decision may mean that the suit against Kazaa will be consolidated with the on-going suit against Streamcast Networks and Grokster, two rival file-swapping companies that use the same underlying technology as Kazaa.

• In In re Aimster Copyright Litigation, No. 01-C-8933 (N.D. Ill. Sept. 4, 2002), an Illinois federal court granted a preliminary injunction, holding that the plaintiff record companies and music publishers had shown a likelihood of success on claims of contributory and vicarious liability, and that Aimster did not qualify for the safe harbor provisions of the Digital Millennium Copyright Act. Using America Online’s Instant Messenger feature, Aimster allowed its subscribers to exchange music files. When Aimster failed to cooperate with its earlier ruling, the court issued a temporary restraining order requiring that Aimster (by then operating as Madster) take down its website and disconnect any computers used in the file-sharing service.

• Search engines and sites linking to music files also have been the subject of litigation. In Arista Records, Inc. v. MP3Board, Inc., No. 00 Civ. 4660 (SHS) (S.D.N.Y. Aug. 29, 2002), several record companies sought summary judgment against MP3Board for contributory and vicarious liability. No music files were located on the MP3Board website; instead, the website had a search engine that searched for and aggregated links to music files elsewhere on the Internet. The record companies alleged that by providing links to infringing copies of musical recordings, MP3Board facilitated infringement. MP3 claimed that its activities were protected by the First Amendment. The court rejected both parties’ motions for summary judgment, and the case is expected to go to trial in 2003.

• In Denmark, the Western High Court held in the Koda litigation that merely linking to a website that contains music files that were uploaded without the consent
of the copyright owner amounts to copyright infringement. Two minors who had homepages linked to sites containing unauthorized music files were found to be liable for copyright infringement under the Danish Act on Intellectual Property.

- In England, a High Court judge issued a summary judgment finding the Easy-Internet Café chain guilty of copyright infringement for allowing customers to download music from the Internet and copy it onto a CD for five pounds. The business unsuccessfully argued that it should not be liable for the infringement of its customers, since it had merely provided the means by which the copies were made.

- In Spain, the Provincial Appellate Court in Barcelona prohibited a website from distributing a record label's music files, holding that websites reproducing and distributing music without paying any royalties are illegal. Ediciones Musicales Horus, S.A. v. www.weblisten.com. The website, without the music label's permission and without payment to the music label, had charged users a fee to download copyrighted music.

- As an alternative or supplement to litigation, many content providers have begun to consider employing technological solutions to combat on-line piracy, including both spoofing and more intrusive denial of service measures. Responding to the concern that some such "self-help" tools may be illegal under current federal and state laws, legislation was introduced by Representative Howard L. Berman giving copyright holders legal immunity when using such technological measures. The response to the proposed legislation was mixed, with some representatives concerned that the technological protection measures the legislation would condone may be too intrusive. Neither the Berman bill nor alternative bills proposed in response were enacted in 2002, but similar legislative proposals are expected to be reintroduced in early 2003.

Domain Name Disputes

- Following the introduction of new top level domain names, including .biz, the Harvard Law School released a study in June which suggested that 75% of .biz websites did not have any substantive content, and at least 5000 .biz domain names were openly offered for sale, in contravention to the .biz registrar's anti-warehousing policy. In the EU, the European Council and Parliament adopted a regulation establishing the conditions for the implementation of the .eu top level domain. The Commission is expected to establish a dispute resolution system for the .eu domain similar to the dispute resolution system governing the .com, .net, and .org domains.

- A series of cases in U.S. courts applied the 1999 Anti-Cybersquatting Consumer Protection Act ("ACPA"). ACPA focuses on the extent to which an accused cybersquatter demonstrates "bad faith" in registering, using, or trafficking in a domain that is a trademark or identical, confusingly similar, or dilutive to a distinctive mark. In Harrods Ltd. v. Sixty Internet Domain Names, 302 F.3d 214 (4th Cir. 2002), the court affirmed a lower court finding that 54 of the names registered by Harrods (Buenos Aires) Ltd., an estranged off-shoot of the plaintiff, were registered in bad faith and ordered that they be transferred to the plaintiff. See also, E&J Gallo Winery v. Spider Webs Ltd., 286 F.3d 270 (5th Cir. 2002). The Harrods decision was significant because the plaintiff sued in rem, naming the domain names rather than the Argentine entity that registered them as a defendant,
Significant Developments in Global Internet Law

thus allowing trademark owners to file suit against cybersquatters without obtaining personal jurisdiction over them. Where no bad faith is shown, as in Interstellar Starship Services, Ltd. v. Epix, Inc., No. 01-35155 (9th Cir. Sept. 20, 2002), courts have not found a violation of ACPA.

• Clarifying what constitutes “bad faith” under WIPO’s Uniform Domain Name Dispute Resolution Policy, a WIPO panel held that merely registering a domain name without posting any content to the site does not constitute bad faith. Ingram Micro, Inc. v. Ingredients Among Modern Microwaves. In concluding that the respondent did not use the domain name in bad faith, the panel noted that there was no content posted to the site, there was no evidence that there had ever been an attempt to attract users to the site for commercial gain, and the registrant had never attempted to sell the domain name to the trademark owner or one of its competitors.

• In a decision limiting the liability of registrars and sites on which domain names are offered for sale, a U.S. court held that neither a domain name registrar nor an Internet auction site were liable for trademark infringement or unfair competition related to the registration or attempted sale of allegedly infringing domain names. Bird v. Parsons, 289 F.3d 865 (6th Cir. 2002).

• In the United Kingdom, the High Court permitted injunctive relief against an individual who threatened repeat cybersquatting in Metalrax v. Vanci. The defendant had registered the domain name “metalrax.co.uk” in 1999, along with 180 other domain names. Metalrax Group plc, a publicly traded company, approached the defendant in 2000 objecting to his use of the domain. The defendant claimed that since he had registered the name first, he had the right to use it, and proceeded to link the domain to a pornographic fetish site (allegedly to embarrass Metalrax into purchasing the domain from him). The Nominet dispute resolution panel suspended delegation of the domain name for three months to encourage the parties to reach an amicable solution, but the defendant made clear that he had no intention to reach an agreement and planned to re-apply for the name as soon as it was released. The High Court determined that the defendant could not possibly re-register the domain name in good faith, and granted an injunction preventing him from re-registering the name.

• Japan, in response to a series of cybersquatting cases, introduced a prohibition on the registration of domain names similar to other companies’ trademarks or business names “for the purposes of generating unlawful profit or causing damage to others.” Further protection for “famous” entities was secured in a decision by Japan’s Supreme Court, which denied a small portable toilet sales company’s claim that it was entitled to use a domain name since it was the first to register for it. Nihonkai Pakuto v. JACCS. The Japanese Supreme Court rejected the argument that the small company had a right to the domain just because it registered the name first on the ground that JACCS, a large credit company, had registered its trade name and the name is widely recognized by the public as associated with the consumer financing company.

• In China, the Beijing Centre of New Asian Domain Name Dispute Resolution Centre handed down its first ruling. The complainant, a Chinese company that sells a famous liquor called “Wuliangye” and had registered the trademark “Wuliangye,” filed a complaint against a Canadian company that had obtained the domain name “wuliangye.com.” The Canadian company did not appear to be using the domain name for a legitimate business purpose and the complainant
offered evidence that the respondent had offered to sell the domain name for an inflated price. Finding that the respondent had acted in bad faith, the panel ordered the domain name transferred to the Chinese company.

**Metatags and Pay-for-Placement Searches**

- In addition to the disputes over domain names, a number of decisions in 2002 addressed the interaction between trademark law and the use of metatags. By embedding a word as a metatag, a website becomes a target of search engines searching for that word. In a case currently before a federal district court in California, the plaintiff, Netbula, Inc., alleged that a competitor infringed its trademark by embedding the Netbula trademark into its web page's keyword metatag sections. In Playboy Enterprises, Inc. v. Welles, 279 F.3d 795 (9th Cir. 2002), the court held that a former Playboy Playmate's use of Playboy trademarks, including the terms “Playboy,” “Playmate of the Month,” “Playmate of the Year,” and the initials “PMOY” could permissibly be used in her site's hidden text as metatags. The court held that the use of the terms on the website and as metatags constituted permissible “nominative use.”

- In France, the Paris Court of Appeal issued a series of decisions consistently holding that using a competitor's trademark as a metatag constitutes an infringement of the trademark. In S.F.O.B. v. Notter GmbH, for example, the court found trademark infringement where the defendant had included in its metatags the registered corporate name of a direct competitor.

- As with the use of trademarks in metatags, the purchase of trademark search terms on a pay-for-placement search engine by the trademark owner's competitors raises the issue of trademark infringement and consumer confusion. In a letter to several leading pay-for-placement search engines, the Federal Trade Commission recommended that the companies provide clearer disclosure to users of their pay-for-placement search engines. The FTC's warning letter followed a complaint by the owner of the trademark “Body Solutions,” who filed suit in a Texas federal court against several search engines for trademark infringement. Body Solutions, which is seeking $440 million in damages, alleged that the search engines sold placement listing for its competitors whose sites are then included in searches for “body solutions.”

- In an English decision addressing the same issue, the High Court held that techniques used to influence search engine results could constitute trademark infringement even if a company's use of another's trademark is invisible to the individual searching on the Internet in Reed Executive PLC and Reed Solutions v. Reed Business Information Ltd.

**Reseller's Use of Trademark**

- Distinct from the issue of cybersquatting is the question of whether or not a reseller of a branded product can reference the brand in its domain name. In Ty Inc. v. Perryman, 306 F.3d 509 (7th Cir. 2002), the court rejected the trademark infringement claim of the manufacturer of Beanie Babies, beanbag stuffed animals, against an individual who sold used Beanie Babies through her website, http://www.bargainbeanies.com. The court emphasized that the defendant was engaged in the legitimate aftermarket sales and noted that “you cannot sell a branded product without using its brand name, that is, its trademark.”
• In contrast, Seiko UK Limited succeeded in its appeal of a dispute resolution proceeding before Nominet, the U.K. Domain Name Registry. Seiko filed a complaint against Designer Time for its registration and use of the domain names “seiko-shop.co.uk” and “spoonwatch.co.uk.” The respondent is an authorized reseller of Seiko and Spoon watches, but the complainant argued that the use of its registered trademarks amounted to trademark infringement. The Nominet Expert agreed with Seiko and ordered the transfer of the two domain names, and this result was affirmed after review by a panel of three Nominet experts. Unlike under the WIPO’s dispute resolution policy, the respondent’s good faith registration of the names was not relevant under the Nominet Dispute Resolution Service policy. While holding that it was not possible to delineate general rules about when a party could make legitimate use of a third party trademark as a domain name, the Nominet experts found that in the present case the use of the domain name would create confusion among consumers and amount to unfair advantage or unfair detriment.

Internet-based Protests

• Two cases in France addressed the use of trademarks in Internet-based protests. In Esso v. Greenpeace, the oil company filed suit before the Paris High Court alleging that the environmental pressure group had “illegally reproduced and imitated” its trademarked brand name and logo in an Internet-based protest campaign. Following precedent established in a 2001 case in which the food giant, Danone, succeeded in having its trademark removed from an Internet site protesting its policies, the French Court ordered Greenpeace to remove Esso’s trademark from its website.

• In Areva v. Greenpeace, however, the Paris High Court denied the plaintiff nuclear firm’s claim against Greenpeace. The plaintiff alleged that its trademarked logo appearing on Greenpeace’s Internet site violated its trademarks. Greenpeace admitted to using the distinctive Areva “A” on its site, but succeeded in convincing the court that its blood-covered version of the “A” was an obvious satire outside of a commercial setting.

Patent Developments

• In British Telecommunications Inc. v. Prodigy Communications Corp., 217 F. Supp. 2d 399 (S.D.N.Y. 2002), a U.S. court ruled that an Internet service provider that gives users access to web pages that incorporate hypertext markup language and hyperlinking does not, as a matter of law, infringe on a patent for an information retrieval system. British Telecom sued Prodigy claiming infringement of a patent filed in 1977 that covers a system to allow users to access text-based information via a telephone network. If the suit had been successful, British Telecom was expected to have sought royalty payments from millions of ISPs and websites for their use of hyperlinks. The case had been closely followed because it established how broadly patents filed prior to the emergence of the Internet would be interpreted to cover Internet-related technology.

• In Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., 535 U.S. 722 (2002), the Supreme Court issued a landmark ruling. Although the facts of the case do not involve the Internet, the case applies to any patent application amended while at the Patent and Trademark Office (PTO). Under the doctrine of equivalents, a patent holder can prove infringement even when the accused infringer had not literally infringed the patent. In 2001, the Federal Circuit had denied the use of
the doctrine in cases where the patent holder had amended its patent application while the application was pending at the PTO. The Supreme Court held that prosecution history estoppel may apply to any claim amendment made to satisfy the Patent Act’s requirements, and not just to amendments made to avoid prior art. However, the Supreme Court held that estoppel does not bar suit against every equivalent to the amended claim element, since a complete bar on the doctrine of equivalents in instances where a patent application has been amended would result in the very literalism that the doctrine of equivalents is designed to overcome.

• In the EU, the European Commission continued to consider adopting legislation harmonizing the rules relating to software patents. Currently, the rules on patentability of software-related innovations are unclear. Although the European Patent Office frequently grants patents for such inventions, some argue that the European Patent Convention suggests that computer programs should not be considered patentable inventions. The legislation, if adopted, would likely harmonize the rules along existing EPO practice.
4 ELECTRONIC COMMERCE, CONSUMER PROTECTION AND TAXATION

The law of electronic commerce, consumer protection and Internet taxation developed at a modest pace in 2002. Existing initiatives to create international legal frameworks remained in the deliberation phase. The European Union adopted a pair of tax regulations affecting online services, and EU member states are gradually implementing EU directives on e-commerce and digital signatures. Legislatures in Europe, Japan and South Korea toughened consumer protection against unsolicited commercial e-mail. In the United States, courts reinforced two emerging trends: "clickwrap" agreements are enforceable, and courts will not exercise personal jurisdiction over an out-of-state website without showing that it is interactive and/or targeted at forum state residents. Several state legislatures enacted bills regulating spam, and state revenue departments issued advisory opinions regarding taxation of online sales and services.

Electronic Contracting

- A pair of proposed international treaties remain works in progress. The UN Commission on International Trade Law (UNCITRAL) has been drafting a convention on electronic contract formation. It may narrow its scope, perhaps by excluding software IP and consumer transactions, in response to U.S. objections that the draft covers too much. The Hague Conference on Private International Law is focusing on a framework for jurisdiction and enforcement of judgments in foreign fora.

- In the U.S., the draft Uniform Computer Information Transactions Act made little headway. A report from a working group of the American Bar Association criticized the UCITA, a proposed model that aims to harmonize states' laws concerning e-commerce. The report found the UCITA difficult to comprehend, too broad, and too uncertain. It also voiced concern that courts could interpret the UCITA as superseding state tort law or unfair business practices regulations.

- In Europe, after a slow start, a majority of EU member states have now implemented the E-Commerce Directive of 2000. Austria, Denmark, Finland, Germany, Luxembourg, Sweden, Spain, and the United Kingdom have now enacted national legislation, while France and Belgium have submitted drafts to the Commission. Like the Digital Signatures Directive of 1999, the E-Commerce Directive is a legal framework for EU harmonization in contract law. It charges member states with specific obligations to facilitate online contracting, e.g., ensuring that customers are sufficiently informed before entering into a contract online, that sellers follow certain procedural steps when accepting orders online, and that service providers carry only limited liability for the information they convey. The Directive adopts a country-of-origin approach to regulation that allows member states some discretion in governing domestic entities.

Securities and Banking

- The Federal Office of the Comptroller of the Currency issued a final rule clarifying that financial institutions may indeed participate in a wide array of e-commerce activities. It contains provisions that concern (a) banks that serve as finders for buyers and sellers, (b) banks that sell access to excess electronic capacity, (c) banks that act as digital certification authorities, and (d) the standards for determining whether banks may engage in new types of electronic activity.
Separately, the Securities and Exchange Commission issued a no-action letter with respect to the following arrangement: a U.S. broker-dealer arranged for its website developer affiliate to offer online services to foreign financial institutions. This letter was the broadest relief to date afforded by the SEC for such an arrangement. It condoned the website developer’s online activities, even though it was not registered with the SEC as a broker-dealer, and did not object to a fee collected by the website developer for each order processed.

In Spain, the Parliament adopted legislation that recognizes a new kind of financial company, “Electronic Money Institutions,” which issue currency in electronic form. These e-money institutions will be subject to regulations that apply to credit institutions plus others added by the government.

In Japan, the securities investigation commission sought its first indictment under a law that bars the dissemination via the Internet of rumors about the value of stocks. The indictment would be aimed at a 23-year-old founder of a stock investment club. After recruiting club members through his website, he emailed them with advice to sell shares of a particular company and then bought that stock at its lowered price. The next day, he reversed his advice, the stock price rose, and he sold his shares at a profit of almost 1 million yen.

**Clickwrap Agreements**

At least four courts in the U.S. upheld the enforceability of so-called “clickwrap” agreements, while a fifth expressed reservations. Typically, these agreements are licenses for software or electronic services, where the licensee-consumer agrees to the licensor's standard terms by clicking on a button signifying assent (labeled, for example, “I agree”) before gaining access to the product.

In i.Lan Systems Inc. v. NetScout Service Level Corp., 183 F. Supp. 2d 328 (D. Mass. 2002), the court ruled that a clickwrap license, which limited the software manufacturer's liability for damages to the consumer's license fee, was an enforceable contract consistent with Article 2 of the Uniform Commercial Code. In Hughes v. McMenamon, 204 F. Supp. 2d 178 (D. Mass. 2002), the same court upheld a forum selection clause in a clickwrap “terms of service” agreement between AOL and a subscriber.

In Moore v. Microsoft Corp., 741 N.Y.S.2d 91 (2002), an appellate state court in New York validated a clickwrap software license by Microsoft, whose terms barred an action for deceptive trade practices. The court noted that the terms were prominently displayed and the user’s click of assent was a precondition to installation.

In Forrest v. Verizon Communications Inc., 805 A.2d 1007 (D.C. 2002), the District of Columbia Court of Appeals upheld a forum selection clause in a clickwrap agreement that was formed on a website for ordering digital subscriber line service, even though the clause was nestled in a long online text that appeared in a small scroll box.

In Comb v. PayPal, Inc., 218 F. Supp. 2d 1165 (N.D. Cal. 2002), the court held that an arbitration provision in a clickwrap agreement was unconscionable. The court found that PayPal did not produce evidence showing that the plaintiffs viewed the user agreement or clicked on the assent button. Moreover, even if plaintiffs had clicked their assent initially, PayPal had since unilaterally amended the agreement five times.
Terms of Internet Service

- In disputes over terms of Internet service, at least two courts sided with ISPs enforcing service terms against subscribers.

- In MonsterHut Inc. v. PaeTec Communications Inc., 294 A.D.2d 945 (N.Y. 2002), a New York appellate court backed the ISP after it dropped a subscriber who spammed in violation of the acceptable use policy.

- In Mathias v. America Online, Inc., No. 79427 (Ohio Ct. App. Feb. 28, 20020, the court ruled that AOL did not breach its terms of service when users were denied access to the system or bumped off during periods of heavy traffic. AOL's terms of service, which warned that service was provided only on an as-available-basis, could be read by users who clicked on a button, and these plaintiffs had done so. The court reasoned that plaintiffs acknowledged these terms by clicking and, moreover, had not shown any damages beyond the inconvenience of delayed or interrupted access.

Authentication

- Following the Federal Electronic Signatures in Global and National Commerce Act of 2000, New York state amended its own Electronic Signatures and Records Act. This year, those amendments took effect and spawned new rules from the NY Office of Technology. The rules empower the office to set forth policy and guidelines on the use of e-signatures and records by government agencies and to assess technologies that satisfy the statute's requirements. They also set forth standards for certification authorities that do business with the government, and they create a public list of revoked certificates.

Regulation of Unsolicited Commercial Email

- To date, almost half of U.S. states have enacted some anti-spam regulation and at least 26 additional bills were introduced in state legislatures in 2002. Nevertheless, the scope of these state laws is relatively narrow. They typically require a label on advertisements and target deceptive spam and spammers who ignore the requests of individual recipients to cease. Truthful, labeled spam that is responsive to "unsubscribe" requests remains permissible. Industry groups, when faced with regulation, prefer a federal solution in order to preempt the emerging patchwork of conflicting state regimes. But Congress has shown little interest in regulating spam, and 2002 proved no different.

- Minnesota, New Jersey, South Dakota, Kansas, Ohio, and Pennsylvania all enacted anti-spam legislation in 2002. A typical example is the Kansas statute, which requires spammers to include accurate labels and "opt-out" instructions in their messages. To help recipients filter incoming messages, the subject line of spam must begin with the label "ADV." (and add "ADLT" if the message promotes sexually explicit material) and not be false or misleading. Within the message, senders must include accurate contact information that enables the recipient to stop future emails. A safe harbor protects Internet service providers who block e-mail that they reasonably believe to be spam. Civil penalties for spamming range up to $10,000 and the statute creates a private right of action. Labeling is not required if sender and recipient have an established business relationship, if the recipient has expressly authorized the spam, or if the sender is a small-volume sender or a charity.
• In Ferguson v. Friendfinders Inc., 115 Cal. Rptr. 2d 258 (Cal. Ct. App. 2002), the court increased the momentum of the anti-spam movement by upholding a California statute that requires unsolicited commercial e-mail to be labeled “ADV:* in the subject line and to instruct recipients how they may stop future emails. The court ruled that the statute did not violate the dormant Commerce Clause of the U.S. Constitution. Last year, the Washington Supreme Court reached the same constitutional conclusion in upholding a similar statute in Washington. See State v. Heckel, 24 P.3d 404 (Wash. 2001).

• In both California and Washington, the state attorneys general have now filed suits against marketers who have allegedly run afoul of those laws. And in EarthLink Inc. v. Smith, No. 1:01-CV-2099 (N.D. Ga. July 9, 2002), a court awarded the ISP almost $25 million against a spammer who flooded EarthLink’s system with a billion emails during one year. The court found that the spammer “engaged in a massive scheme of illegal acts, including credit card and identity theft, password theft, theft of Earthlink’s computer resources and account, fraud, spamming, and spoofing.”

• At the federal level, the FTC announced its first wave of enforcement actions in April. The joint effort with several states and Canada targets Internet “scammers” (those who use deceptive practices on the Internet) and spammers. The initiative included filing actions against four alleged scammers and sending 500 warning letters to alleged spammers. In November, a broader FTC-led coalition announced a larger, four-part program involving sting operations, more than 30 enforcement actions, and an initiative called “Spam Harvest” to investigate which online actions render consumers most prone to attracting spam. The FTC secured a court award of $1.9 million in damages against a company that deceptively redirected Web users to sites with various advertisements.

• In Europe, the EU adopted the Electronic Communications Data Protection Directive, which will now require EU member states to regulate the use of unsolicited commercial e-mail. Under the Directive, the use of e-mail (including SMS and other messages to mobile handsets), automatic calling machines, or fax machines for “direct marketing” is only permissible to reach subscribers who have given “prior consent.” The general rule requiring opt-in consent does not, however, apply to established customer relationships. When an organization obtains e-mail addresses from customers, “in the context of the sale of a product or a service” and in compliance with data protection rules, the organization may use the addresses for the direct marketing of “its own similar products or services,” provided customers have a clear opt-out opportunity at the initial collection stage and in every subsequent message. This will liberalize rules in a few EU states, which have opt-in requirements for all unsolicited commercial email. The Directive also prohibits sending of e-mail “disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease.”

• At least two Asian countries enacted national legislation in 2002 to curb unsolicited commercial e-mail. Japan adopted two new anti-spam laws. Unsolicited and/or commercial e-mail must now be labeled as such, and it must contain the sender’s telephone number and e-mail address. These laws do not purport to regulate spam sent into Japan from abroad.
Significant Developments in Global Internet Law

- South Korea toughened its existing spam regulations (requiring “advertisement” headings and “unsubscribe” instructions) by prohibiting both the random collection of e-mail addresses for commercial use and the sending of adult e-mails to minors. ISPs may now deny service to spammers when necessary to protect the quality of service for other customers.

Internet Taxation

- Delegates to the Streamlined Sales Tax Project, a collective initiative by U.S. states to collect revenue from online sales to U.S. residents, approved such an agreement. No state legislature has given effect to the agreement thus far, but many are considering the measure. Meanwhile, a consortium of 10 major retailers, including Wal-Mart and Target, have agreed to begin collecting taxes for online sales anyway, even for transactions in states where the companies are not physically present.

- In May, finance ministers of the EU approved final rules that impose a value-added tax (VAT) on non-EU companies that sell digitally-delivered products to EU consumers via the Internet or other telecommunications channels. The rules will require non-EU companies to register with the tax authority of one of the member states of the EU. The companies will charge the VAT rate of the consumer's country, but will remit all payments to the tax authority in the country of registration, which in turn will distribute those attributable to sales in other countries to the appropriate tax authority.

- The new rules take effect by July 2003. They will apply to a broad range of digital products: digital delivery of software and computer services generally, as well as cultural, scientific, educational, entertainment, and similar services, plus television and radio broadcasting services. The new rules seek to equalize the VAT burdens placed on sellers based inside and outside the EU. Under the old rules, non-EU sellers enjoyed a competitive advantage because they did not have to levy any VAT, while EU-based sellers of digitally-delivered products had to levy the VAT rate of their country of establishment, even if the customer was outside the EU. However, some competitive disparities remain — while non-EU sellers levy the VAT rate of the country of destination, EU-based sellers still levy the VAT rate of their country of establishment (except for sales outside the EU, where they levy no VAT at all). This means that sellers in low-VAT countries, such as Luxembourg, can sell digitally-delivered goods more cheaply to consumers in high-VAT countries.

Advisory Tax Opinions

- In advance of any online tax legislation, individual states have clarified their positions regarding taxation of e-commerce. The revenue departments of several states issued opinions concluding that, in general, online services were not tangible personal property and thus not taxable. They further distinguished between standardized software (taxable) and custom software (not taxable).

- In New York, for example, website services and consulting were found not to be subject to sales and use tax, and Virginia reached the same conclusion regarding online digital identification services.

- Illinois found taxable the sale of prewritten software programs and updates but not the sale of custom software.
• In Missouri, online financial services and accompanying computer hardware were found to be taxable because the sale of the equipment was the “true object” of the combined transaction.

• In other situations, the customer’s physical location determined tax liability. New York advised that a NY taxpayer, when calculating its state taxable income, must include receipts from a sale of a gift certificate over the Internet if the customer was located in New York when he or she accessed the website. If that location is unknown, then the taxpayer should use the customer’s billing address as the presumptive location. The Department treated Internet gift certificates as intangible personal property.

• In Kansas, a letter ruling stated that an in-state company must collect state and local sales taxes when it ships goods ordered via the Internet to an address within the state.

Other Consumer Protection Developments

• In Oyster Software Inc. v. Forms Processing Inc. No. C-00-0724 JCS (N.D. Cal. Dec. 6, 2001), a court held that a Web robot’s mere use of another’s website was sufficient to sustain a claim for trespass to chattels. The court rejected the argument that such a claim required a showing that the robot’s use caused substantial interference with the target website.

• In State ex rel. Stovall v. Confirmed.com LLC, No. 87,177 (Kan. Jan. 25, 2002), the Kansas Supreme Court found that the prescription and sale of the pharmaceutical Viagra via a website did not violate the state’s consumer law prohibiting unconscionable transactions despite the fact that the defendant-physician was not licensed in the state, the recipient was a minor, and no physical examination occurred.

• In connection with the FTC’s enforcement effort “Operation Top Ten Dot Cons,” five Internet auction sellers will hand over $10,000 for consumer redress, according to a consent decree filed in federal court in California. The sellers allegedly failed consistently to send buyers the products purchased online.

• The District of Columbia Bar Ethics Committee advised that, under DC bar rules, attorneys may solicit prospective clients through Internet chat rooms and listservs. The opinion cautioned that attorneys who engage in this communication should not give specific legal advice (as distinct from general legal information) to avoid forming attorney-client relationships, regardless of any disclaimers they provide.

E-Commerce Jurisdiction

• In Europe, a trend emerged in favor of expanding jurisdiction to reach foreign e-commerce websites. The Brussels Regulation, a measure adopted by the European Council in 2000, took effect in March. It allows residents of EU member states to file suit against foreign website operators in the consumer’s home forum if the operator “directs” its commercial or professional activities at the consumer’s home country. (The scope of Internet activities reached by this term is yet undetermined.) Conversely, businesses filing suit against a consumer must choose a forum in the consumer’s country.
Meanwhile, courts in the U.S. concluded that mere accessibility of a foreign website from within a forum state does not establish jurisdiction. In 2002, a score of federal and state courts issued rulings on personal jurisdiction over out-of-state website operators. With few exceptions, these courts found jurisdiction lacking unless the website was considerably interactive (e.g., enabled users to form agreements online) or it was somehow targeted at residents in the forum state. Claims of jurisdiction over passive websites failed.

Three major cases conformed to this general pattern. In Toys “R” Us Inc. v. Step Two SA, No. 01-3390 (3d Cir. Jan. 27, 2003), the Third Circuit toughened its own Zippo sliding scale test (measuring a website’s level of interactivity) by finding no jurisdiction over a fully interactive website without a showing that the defendant had not intentionally targeted or knowingly conducted business with forum residents. The Ninth Circuit, however, in Northwest Healthcare Alliance Inc. v. Healthgrades.com Inc., No. 01-35648 (9th Cir. Oct. 7, 2002), rejected the Zippo test in favor of the Calder v. Jones effects test and found jurisdiction where a website’s tortuous effects were felt in the state where the plaintiff did business.
5 NETWORK SECURITY

In the wake of both the terrorist attacks on September 11, 2001 and of numerous high-profile virus, worm and hacking attacks in the past year, governments around the world took steps during 2002 to increase network security and more clearly define penalties for security breaches. In the United States, the Homeland Security Act of 2002 created important new penalties for security breaches and requires new disclosures in the event of network security failures. The European Commission has focused on network security issues and a draft framework decision on cybercrime has been released. Parallel measures have been taken in other countries as well, and the pace of these developments is likely to accelerate.

Disclosure of Security Breaches

- In the United States, the Homeland Security Act of 2002 addresses network security issues. The Act amends the Electronic Communications Privacy Act and expands the circumstances under which electronic communication service providers and remote computing services may disclose information to government entities without offending privacy rights of subscribers. A service provider may disclose to government agencies, without risk of liability, the content of electronic communications that it believes in good faith to be related to an emergency involving the risk of death or serious physical injury. Formerly, disclosure required a higher “reasonable belief” standard that the communications were related to an emergency and permitted disclosure only to federal officials. Federal, state, or local government entities that receive voluntary disclosures must report the disclosure to the U.S. Attorney General within ninety days.

- Following a conference with chief information officers, the FBI and U.S. Secret Service, together with private industry, released their Cyberthreat Response and Reporting Guidelines. The Guidelines address computer and network security, such as attacks on information systems or data. Reportable incidents include events with actual organizational impact (e.g. intruder access, malicious code) or where the organization has detected unusual activity (e.g. new traffic pattern, specific IP address as a source of persistent attacks). Routine probes and port scans would fall outside the ambit of reportable incidents.

- Richard Clarke, former Special Advisor to the President for Cybersecurity and Chairman of the President’s Critical Infrastructure Protection Board, released a draft of the National Strategy to Secure Cyberspace for comments. The draft strategy offers recommendations for five “levels” of networked computer audiences: home users, large enterprises, critical sectors, national priorities, and the international community. The draft strategy contains no mandates to government agencies and does not force private industry action through increased regulation. This approach departed from earlier drafts of the strategy that had been leaked to industry and revealed plans for a mandatory cybersecurity fund to which companies would have to contribute, restrictions on government use of 802.11b wireless LAN, and mandatory firewall software for always-on Internet connections.

Critical Infrastructure Information Disclosures

- The Homeland Security Act permits voluntary disclosure of “critical infrastructure information” to the Department of Homeland Security and exempts disclosures, as well as the identity of the person or entity disclosing, from Freedom of Infor-
Significant Developments in Global Internet Law

Critical infrastructure information encompasses information not ordinarily in the public domain concerning actual, potential or threatened interference with critical infrastructure — including the misuse of or unauthorised access to communications and data transmission systems — that is unlawful, harms interstate commerce or threatens public safety. A third party may not use voluntarily shared information submitted in good faith against the disclosing party in any civil action without its written consent.

- The Act provides similar protection for voluntary disclosures to state or local government agencies. If the federal government issues a public security warning based on voluntarily shared critical infrastructure information, it may not release the information source or any proprietary, business-sensitive, or otherwise identifying information about the disclosing entity. Criminal penalties apply to any federal government employee who knowingly discloses voluntarily shared critical infrastructure information.

Mandatory Disclosure of Breaches of Personal Information

- The state of California enacted legislation that will require people and businesses in California to promptly disclose any breach of a network security system that results in the acquisition of unencrypted personal information by an unauthorised person. The legislation is effective July 1, 2003. In the same vein, Senator Hollings has proposed legislation, the Online Personal Privacy Act, that would require ISPs, website operators, and online service providers to disclose to users when a hacker or third party compromises the security, confidentiality, or integrity of their personally identifiable information. Unlike the California enactment, compromised access of encrypted information could trigger the proposed federal legislation’s disclosure requirements.

Cybercrime Legislation

- In the United States, the Homeland Security Act increases maximum penalties for those who knowingly or recklessly cause or attempt to cause death or serious bodily injury through a cyberattack; increases penalties for unlawful access to and interception of electronic communications; criminalizes advertising illegal interception devices by electronic means; and encourages the U.S. Sentencing Commission to increase sentencing ranges for computer-related crimes.

- Europe is stepping up penalties and procedures for cybercrime as well. The European Commission issued a proposed Framework Decision on Cybercrime that would harmonize EU member state criminal laws addressing crimes against information systems. It would establish the offenses of illegal access to (e.g. hacking) and illegal interference (e.g. denial of service and virus attacks) with information systems. The European Parliament adopted its consultation opinion in October. To become final, EU member states must approve the Framework Decision.

- The EU also has adopted the eEurope 2005 Action Plan, which — among other objectives — seeks to establish a secure information infrastructure. To achieve this objective, the Action Plan proposes (1) the creation of a European Network and Information Security Agency; (2) the promotion of a culture of security in the design and implementation of information products; and (3) the establishment of a secure communications environment for the exchange of classified information among governments.
• Computer crime laws have been put into effect elsewhere, largely following the Council of Europe's 2001 Convention on Cybercrime. For example, Thailand approved a draft of its Computer Crime law that criminalizes hacking into computer networks with malicious intent. Offenders may be sentenced to two years imprisonment. The drafting committee modeled the Computer Crime laws on American and European computer crime legislation, including the Convention.

Cybercrime Prosecutions

• The United States prosecuted two notable cyberoffenders in 2002. A federal district court sentenced David Smith, the author of “the Melissa virus,” to 20 months imprisonment, a $5,000 fine, and community service. The Melissa virus caused an estimated $80 million in damages to computers worldwide. In the second prosecution, British national Gary McKinnon was indicted for hacking into 92 U.S. military computer systems, as well as six private companies' networks, in the immediate aftermath of the September 11th terrorist attacks. The United States is seeking his extradition to stand trial.

• Prosecutions for network security breaches are occurring elsewhere as well. Israel sentenced a teen hacker to eighteen months imprisonment for violating the Computer Law of 1995. The Israeli teen had hacked into the computer systems of several sensitive U.S. government agencies, including NASA, the FBI, the U.S. Air Force, and the Department of Defense computers, as well as the Massachusetts Institute of Technology.

• Not all hacking prosecutions ended in convictions, however. The Paris Court of Appeal reversed a lower court decision convicting a journalist of fraudulently accessing a French department store website (Tati v. A.C.). Using only a Netscape browser, an investigative journalist exposed department store Tati's inadequate web security and a lower court convicted him of fraudulently accessing an automated data processing system. On appeal, the court held that an Internet user may not be convicted for merely accessing sections of a web server that are inadequately secured for mass market software. Absent special notice about the confidentiality of site information, insecure portions of a website must be deemed freely accessible by web browsers.

International Cooperation

• The European Commission has drafted a regulation to create an independent European Network and Information Security Agency. The Agency would facilitate the implementation of EU network security measures and verify the interoperability of security functions. It is intended to enhance EU and member states' capacity to respond to security problems by collecting and analyzing data on current and emerging IT incidents. In addition, it will assess evolving network and information security standards. It would coordinate with non-EU countries and international organizations.

• The Organization for Economic Cooperation and Development (OECD) revised its 1992 Guidelines on the Security of Information Systems in July. The new Guidelines for the Security of Information Systems and Networks recommend security measures that are compatible with "democratic values" and urge participants to act in a timely and co-operative manner to prevent, detect and respond to security incidents.
• In October, the Asia-Pacific Economic Cooperation committed to (1) enact a comprehensive cybersecurity and cybercrime regime that is consistent with U.N. General Assembly Resolution 55/63 (2000) on Combating the Criminal Misuse of Information Technologies and the Council of Europe Convention on Cybercrime (2001); (2) identify or establish national cybercrime units and contacts for international assistance; and (3) establish response teams that exchange threat and vulnerability assessments. October 2003 is the targeted date for completion of these goals.

• The Group of 8 (G8) Ministers of Justice and Interior released a Statement on Data Protection Regimes, which recommends ensuring that national laws adequately criminalize abuses of modern technology; providing adequate legal authority to exercise jurisdiction, enforcement and investigatory powers to confront cybercrime; ratifying the Council of Europe's Convention on Cybercrime (2001) and implementing its terms in domestic law; cooperating with private industry in securing computer networks and communication systems; and appropriately balancing privacy and law enforcement's ability to protect public safety.

Cyberwar

PRIMARY OFFICE CONTACTS

Washington
Mark Plotkin
202.662.5656
mplotkin@cov.com

New York
Bert Wells
212.841.1074
bwells@cov.com

San Francisco
Evan Cox
415.591.7073
ecox@cov.com

London
Kurt Wimmer
44.(0)20.7067.2010
kwimmer@cov.com

Brussels
Dave Harfst
32.(0)2.549.5251
dharfst@cov.com
Covington & Burling

Washington
1201 Pennsylvania Avenue NW
Washington, DC 20004-2401
Telephone 202.662.6000
Fax 202.662.6291

New York
1330 Avenue of the Americas
New York, NY 10019
Telephone 212.841.1000
Fax 212.841.1010

San Francisco
One Front Street
San Francisco, CA 94111
Telephone 415.591.6000
Fax 415.591.6091

London
265 Strand
London WC2R 1BH
Telephone 44.(0)20.7067.2000
Fax 44.(0)20.7067.2222

Brussels
Kunstlaan–44 Avenue des Arts
1040 Brussels
Telephone 32.(0)2.549.5230
Fax 32.(0)2.549.5230