Significant Developments in Global Internet Law in 2003

COVINGTON

CONTENTS

TOP TEN DEVELOPMENTS IN GLOBAL INTERNET LAW

1. **The Battle Over Peer-to-Peer File Sharing**. Courts split in infringement cases, but a combination of some 1,000 subpoenas, more than 500 lawsuits and the emergence of popular websites for legal downloading of music led to a dramatic decline in the popularity of file-sharing.

2. **Crackdowns on Spam**. Legislation regulating spam finally passed the U.S. Congress, EU regulations began to be implemented, and new laws against spam were passed in Asia. Yet, the flow of unsolicited commercial email exploded to some 15 billion messages per day, prompting calls for cross-border cooperation.

3. **Beginnings of a Backlash Against Anti-Terrorism Surveillance**. In the U.S., two anti-terrorism proposals provoked public opposition. In Europe, laws requiring ISPs to retain massive amounts of customer usage data led to controversy but moved ahead.

4. **Struggles for Free Speech**. Some 20 countries signed a Council of Europe protocol seeking to ban racist speech on the Internet. In the U.S., the Supreme Court upheld a federal law requiring libraries to install mandatory Internet filtering software and agreed to review a lower court's decision striking down a federal law against providing content that is harmful to minors.

5. **New Protections for Personal Information**. In Europe, the e-Privacy Directive went into effect. Enforcement actions against companies accused of failing to secure customers' personal information became widespread in the U.S., Europe and Asia.

6. **Increasing Stability in Electronic Commerce**. Electronic signature laws were implemented around the world, and the scope of treaties and U.S. model legislation was narrowed. A U.S. national moratorium on Internet taxation expired, and the EU enacted online VAT legislation.

7. **Uncertainties in Jurisdiction and Choice of Law**. In Europe, the EU proposed a new rule that could undermine the beneficial "country of origin" approach, while U.S. courts began focusing on a more favorable framework for jurisdiction.

8. **Invigorated International IP Enforcement**. The EU began harmonizing penalties against infringement, and 43 countries now have signed the WIPO Copyright Treaty.

9. **Uncertainty Over Open Source**. SCO alleged that IBM's distribution of Linux software violation SCO's intellectual property rights and threatened legal action against Linux users, casting a shadow over the open-source operating system.

10. **DMCA Anti-Circumvention Disputes**. Courts split on whether the Digital Millennium Copyright Act's anti-circumvention provisions applied in diverse industries, and critics continued to charge that the DMCA unfairly favors copyright owners.

INTRODUCTION

The year 2003 was a year of contrasts in the development of global Internet law. Privacy concerns continued to be balanced against increased anti-terrorism surveillance capabilities, but the beginnings of a backlash against intrusive measures could be felt. The most high-profile dispute of the digital age—copyright infringement of digital music—resulted in landmark court decisions, hundreds of lawsuits and, just as importantly, the emergence of popular commercial alternatives. Strong protections for free speech continued, but doubts were raised about the breadth of immunity for online service providers, and, in Europe, some 20 countries signed a treaty seeking to ban racist speech on the Internet. New electronic marketing regulations were adopted in Europe and the United States, but the flow of spam became a torrent. The EU considered jurisdictional rules that would undermine its country-of-origin approach, even as courts in various U.S. states began to focus on new legal constructs that are favorable for distant Internet defendants. Global electronic commerce rules continued to become more stable and Internet purchases soared, even as the Internet tax moratorium expired in the U.S.

After only one month's experience in 2004, we can already see trends for the year ahead. Electronic commerce continues to thrive and become mainstream, moving from an enterprise that lawmakers seek to foster to one they seek to regulate. Efforts to stanch the flow of spam will continue and accelerate, as the effectiveness of just-enacted legislation already is questioned. Battles for free speech on the Internet will focus again on the U.S. Supreme Court, which has agreed to review the one significant case that struck down an Internet law on First Amendment grounds in 2003, and the Council of Europe, which moves ahead with its cybercrime and right-of-reply initiatives. Finally, the market for downloading music promises to stabilize in 2004 with the emergence of popular, legal, commercial sites.

This report is designed to be a high-level overview. We have selected key cases and laws from countries around the world that, in our practice and experience, best represent the emerging trends in Internet law. There are thousands of cases, laws and regulations that touch on the Internet that we could not mention here. If you have an interest in an area that is not addressed in this report or have any questions about the reported cases and laws, please feel free to let us know.

This report was edited by Kurt Wimmer and Mark Plotkin in Washington, Bert Wells in New York, Evan Cox in San Francisco, Lisa Peets and Dan Cooper in London and Jason Albert in Brussels. It was reported by Jeff Rosenfeld, Tim Jucovy, Amy Toro, Brian Smith, Erica Price and Heather Nevin. For more detailed treatment of these and related issues, please see our treatise, E-Commerce Law & Practice (Aspen Publishers).

PRIVACY AND SECURITY

Following the terrorist attacks on September 11, 2001, many governments worldwide introduced legislation to enhance law enforcement's authority to monitor electronic communications. These initiatives continued throughout 2003. Additionally, in response to the growing recognition of the breadth of Internet-related crimes, efforts continued on national and international levels to adopt legislation targeting such activities and to prosecute offenders. Steady growth in global e-commerce also has generated concerns over the commercial collection, processing, and transfer of personal information. Finally, countries continued to develop legal frameworks to guide and restrict the monitoring of employee email and Internet use.

Increased Anti-Terrorism Surveillance

- In the United States, a public backlash against increasing surveillance resulted in the modification of two government surveillance programs. First, the Terrorism Information Awareness project (TIA) intended to identify terrorist activity through the creation of a "revolutionary technology" for a "virtual, centralized, grand database," populated by financial, medical, communication, and travel records from other government and commercial databases. Throughout 2003, several legislative proposals emerged to prevent the construction of the TIA database. Finally, on September 30, Congress voted to block funding for the TIA database in its fiscal 2004 Defense Department appropriations bill.

- Similarly, the Computer Assisted Passenger Pre-Screening System (CAPPS II) proposes to assign passengers a score based on data gathered from government and commercial databases. In response to public concern, appropriations legislation for the Department of Homeland Security prohibited the implementation of the system, other than on an experimental basis, until the General Accounting Office reports on the operation and oversight of the program. Additionally, in an October 16 letter to the Pentagon, the Senate Governmental Affairs Committee sought details regarding Jet Blue Airways' disclosure of personal data on more than a million of its passengers to a Defense Department contractor. The U.S. government has continued to implement CAPPS II during the probationary period, and in January 2004 indicated that it may soon compel airlines to hand over passenger data.

- In 2002, the Canadian Custom and Revenue Agency (CCRA) released plans to establish an airline passenger database, which would retain, for six years, the Advance Passenger Information/Passenger Name Record information for every airline passenger entering Canada. In response to public criticism, the CCRA amended the program to require the deletion of certain information unrelated to security purposes and to require a warrant in some circumstances.

- In February 2003, the French Parliament adopted the Internal Safety Law, which authorizes law enforcement officials' immediate access to the communications data of telecommunications operators and ISPs.

- On June 4, 2003, the Danish Parliament enacted an anti-terrorism bill that, among other things, expands the capability for law enforcement officials to monitor Internet activity.

- Japan's national computerized identification system became operational in August 2003. The online database contains every citizen's name, address, date of birth, and gender, and seeks to streamline person-to-government administrative procedures, such as changing an individual's mailing address. Three local governments have refused to employ the system. The Singapore Ministry of Finance released an online identification system to facilitate electronic government access. The U.K. and Canada also have proposed implementing compulsory national identity card schemes using cards with unique biometric identifiers.

- The Chinese government's monitoring of Internet activity led to the arrest and imprisonment of several individuals in 2003 who had posted online content critical of the government. In June 2003, the Chinese Government began to license Internet café chains. Privacy advocates claim that the licensing scheme serves, in part, as a subterfuge to monitor Internet use.

Retention of Internet Traffic and Location Data

- Under the terms of the European Union's Directive on Privacy and Electronic Communications (2002/58/EC), Member States may enact laws mandating the retention of traffic and location data for all communications taking place on the Internet or other electronic communications media where "necessary, appropriate, and proportionate" in a democratic society. Member countries were required to implement the Directive by October 31,2003, although a number failed to meet that deadline.

- In January 2003, the EC Article 29 Working Party issued a report on the storage of traffic data for billing purposes. The Working Party stated that a reasonable interpretation of the Directives on data protection calls for the routine storage of traffic data for billing purposes for a maximum of three to six months. Individual EU Member States grappled with data retention proposals in 2003.

- In 2003, the United Kingdom enacted the Regulation of Investigatory Powers (Communications Data) Order 2003, which extends the list of central and local government authorities granted access to citizens' Internet traffic data under the Regulation of Investigatory Powers Act 2000. The U.K. also passed the Retention of Communications Data (Code of Practice) Order 2003 pursuant to powers arising under the Anti-Terrorism, Crime and Security Act 2001. This Order approves a voluntary "Code of Practice" for telecommunications providers that would allow them to retain certain forms of traffic data for up to 12 months. Government officials cautioned that if providers fail to adhere to the voluntary scheme, a mandatory system may be imposed.

- Several nations adopted measures that affirmatively require the retention of traffic data by ISPs. Finland, Lithuania, the Netherlands, Poland, and Switzerland all enacted legislation that require ISPs to retain Internet traffic data for a specific duration for law enforcement purposes. Additionally, legislation in Finland, Lithuania, Poland and Switzerland requires the retention of certain user-posted data, email content and traffic data.

- In Belgium, a royal decree provided guidance on the practical and technical measures that ISPs must adopt to assist law enforcement officials. In Denmark, the government sought to draft an administrative order regarding ISP data retention. And the Irish Data Protection Commissioner stated in February 2003 that data retention measures are appropriate but "must be proportionate and have regard to the human right to privacy."

Cybercrime

- Several international organizations dealt with cybercrime in 2003. The Organization for Economic Cooperation and Development (OECD) released guidelines to help law enforcement agencies combat Internet-related fraud. In July 2003, the members of Asia-Pacific Economic Cooperation (APEC) agreed to strengthen legislation prohibiting computer- and Internet-related crime. The Council of Europe Cybercrime Convention gained momentum as Estonia and Hungary ratified the Convention, Denmark and Lithuania signed it, and Armenia, Belgium, Estonia, Finland, France, Germany, Greece, Luxembourg, Malta, the Netherlands, and Sweden signed the Additional Protocol to the Convention. U.S. President Bush, in November 2003, urged the Senate to ratify the Convention.

- The EU has made progress toward adoption of its Framework Decision on Cybercrime. The proposed legislation requires Member States to harmonize the criminal rules applicable to illegal interference with and illegal access to information systems. The legislation also will set mandatory penalties, including terms of imprisonment of between one and three years. It is anticipated that the EU will adopt this legislation in early 2004.

- Several countries enacted cybercrime legislation. In October 2003, the New Zealand Crimes Amendment Act added computer-related offenses and authorized law enforcement officials, with court approval, to intercept communications. In November 2003, Singapore enacted the Computer Misuse Bill, which provides broad authorization for law enforcement to prevent threats to essential computer systems. Taiwan's legislature added new computer-related offenses and more severe criminal penalties to the Taiwanese Criminal Code. Lithuania and Mauritus also enacted cybercrime legislation.

Critical Information Infrastructure

- Governments also sought to improve security through changes in network infrastructure and industry practices. In November, the European Commission's proposal to establish an independent European Network and Information Security Agency (ENISA) was adopted by Parliament. ENISA will streamline the cooperation among the European Commission and the Member States in their responses to Internet security failures. Additionally, in October, the European Commission released its first set of computer forensic tools, which may be employed to identify and secure electronic evidence to fight cybercrime.

- In February 2003, the White House released its National Strategy to Secure Cyberspace, which recommends improving cyber-security through, among other things, the development of public-private partnerships. To implement this strategy, the Department of Homeland Security created a division to conduct cyberspace analysis, issues alerts, and respond to breaches in security of critical infrastructures.

- In March 2003, the U.S. House Committee on Government Reform released a report detailing how users of peer-to-peer file sharing applications unwittingly disclose confidential information such as tax returns, personal correspondence and medical records. In September 2003, Representative Henry Waxman introduced legislation that would require "the head of each agency [to] develop and implement a plan to protect the security and privacy of computers and networks of the Federal Government from the risks posed by peer-to-peer file sharing." The bill was not enacted during 2003.

Network Security

- The Maine Public Utilities Commission found that Verizon's failure to install a patch intended to protect its network against the type of attack effected by the Slammer worm in January 2003 was not reasonable under the performance standards set by Maine regulations. *In re Verizon-Maine, Me.* PUC, No. 2000-849 (April 30, 2003).

- In February 2003, a lawsuit filed in California charged that Intuit's Turbotax tax preparation software contained "destructive security software" and other undisclosed technical glitches that resulted in vulnerabilities and the transfer of personal information. *Knabel v. Intuit Inc.,* No. BC 290840 (Cal. Super. Ct., filed February 24, 2003).

- In October 2003, a class action lawsuit filed in California charged that Microsoft's alleged dominance in the computer software industry has increased the risk of computer viruses, and that Microsoft has not provided users with adequate notice of the potential risks. *Hamilton v. Microsoft Corp.,* No. BC303321 (Cal. Super. Ct., filed October 1, 2003).

Personal Information Security

- On July 1, 2003 the California Security Breach Information Act went into effect. This law requires all companies performing business in California to disclose any security breach that results in the unauthorized acquisition of certain types of personal information of California residents. The California Office of Privacy Protection released recommended best practices in October 2003 to comply with the law.

- Actions involving unauthorized access to personal information were legion in 2003. For example, Victoria's Secret agreed in October 2003 to settle a complaint brought against it by the New York Attorney General alleging that its website had disclosed the names, addresses, and order details for certain customers. Similarly, Guess? agreed to implement a comprehensive Internet security review of Guess.com and its other websites in response to Federal Trade Commission allegations that the company exposed consumers' personal information, including credit card numbers, to commonly known attacks by hackers.

- Mrs. Fields Cookies and the Hershey Foods Corporation settled unrelated FTC charges that the companies had violated the Children's Online Privacy Protection Act (COPPA) by collecting personal information from children under the age of 13 without obtaining parental consent. The settlements involved the largest fines to date incurred under COPPA.

- In April 2003, the Canadian federal Privacy Commissioner ruled that a Canadian airline violated federal privacy law by improperly collecting personal information by requiring visitors to its website to permit the installation of cookies on their computers. *PIPED Act Case Summary #162* (16 April 2003).

- In April 2003, U.S.-based ChoicePoint Inc. was accused of purchasing personal information on the citizens of Latin American countries and selling the data to the U.S. Bureau of Customs and Border Protection, the Justice Department, and the Department of Homeland Security. The target countries included Argentina, Brazil, Colombia, Costa Rica, El Salvador, Guatemala, Honduras, Mexico, Nicaragua, and Venezuela. In May 2003, an Argentinean criminal judge initiated an inquiry into the trans-border sale of personal data. In November 2003, Mexican officials arrested three individuals affiliated with ChoicePoint.

Identity Theft

- In January 2003, the FTC reported that identity theft had surged, and throughout 2003, it encouraged individuals, companies, and government entities to employ remedial measures to help prevent identity theft.

- U.S. law enforcement officials took action against perpetrators of identity theft and other Internet scams designed to elicit personal information. The FTC sued a mortgage website that did not make the loans as advertised, but rather sold the personal information in the completed applications to third parties. Federal prosecutors in Massachusetts charged a Pennsylvania teenager with securities, mail, and wire fraud based on his alleged theft of another's identity by hacking into the individual's online brokerage account.

- In the United States, the Fair Credit Reporting Act (FCRA) was amended to provide new tools for consumers and financial institutions to combat identity theft. For example, the amended FCRA enables consumers to place "fraud alerts" in their credit reports, provides a "one-call-for-all" protection for consumers to contact credit bureaus concerning identity theft, restricts access to a consumer's sensitive health information, and prohibits merchants from printing more than the last 5 digits of a payment card on a receipt.

Data Protection in Electronic Commerce

- On October 31, 2003, the European Union's Directive on Privacy and Electronic Communications (2002/58/EC) went into effect. The e-Privacy Directive requires website operators using cookies, spyware, and website tracking devices to provide users with clear information about their use and offer users the opportunity to refuse them, subject to certain narrow exceptions. Following this date, the European Commission initiated proceedings for the failure to implement the Directive against Belgium, Germany, Greece, France, Luxembourg, the Netherlands, Portugal, Finland, and Sweden.

- EU privacy regulators released a number of important recommendations during 2003. In April 2003, the data protection authority of the German state of Baden-Württemberg decided that a U.S.-based multinational company had violated Germany's data protection law by obtaining IP addresses from its German customers without obtaining prior consent. The EU's Article 29 Working Party, comprised of the EU's principal data protection officials, also issued a paper indicating that there may be greater regulation of WHOIS and similar databases in the future because of concerns over misuse of personal data in those lists.

- On May 23, 2003, the "safeguards rule," a key component of the implementation of the Gramm-Leach-Bliley Financial Modernization Act on financial privacy, went into force. The rule requires financial institutions to establish written internal plans for the protection of customer data. April 14, 2003 also was the compliance date for the U.S. Health Insurance Portability and Accountability Act (HIPAA), which sets standards and establishes individual rights concerning the collection and disclosure of certain health information.

- In 2003, California enacted several laws regulating the collection, processing, and transfer of personal information. The Online Privacy Protection Act of 2003 requires commercial website and online service operators that collect personal information from consumers in California to post conspicuously their privacy policies on their websites. The California legislature enacted a law aimed at protecting personal financial information, which requires opt-in consent prior to the financial institutions' disclosure. However, it appears that federal amendments to the Fair Credit Reporting Act will preempt this new California law. In September 2003, California enacted a law that requires businesses that have disclosed personal information within the preceding year for direct marketing purposes to provide consumers with information about the disclosed data and the parties that received the data.

- On January 1, 2004, the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) extended to every organization that collects, uses, or discloses personal information in the course of a commercial activity, whether or not the organization is federally regulated. PIPEDA addresses all commercial activity in provincially regulated sectors unless the province enacts "substantially similar" laws. Quebec is the only province to have implemented privacy laws considered substantially similar by the Privacy Commission. In late 2003, the British Columbia Legislature enacted a new comprehensive privacy law, which will now undergo an examination for substantial similarity.

- The Italian Council of Ministers released a new, comprehensive data protection code in September 2003, which will go into effect in January 2004. The new code consolidates Italy's data protection laws, which had previously been spread among multiple sources and establishes greater protection for individuals, particularly with regard to health information.

- The Japanese Personal Information Protection bill, which was enacted in 2003, sets forth a broad range of restrictions on businesses that handle personal information. Four related bills address personal information stored by government administrations and independent government corporation, and the establishment of a personal information protection commission. Violators may face up to six months in prison or a fine of up to 300,000 yen.

- During 2003, the governments of Malaysia, Mexico, the Philippines, and Thailand all considered draft data protection bills, to regulate the collection, processing, and transfer of personal information.

Compelled Disclosure of Personal Data

- In *Smith v. Doe* 538 U.S. 84 (2003), the United States Supreme Court found that the publication of the name and address of convicted sex offenders on the Internet did not violate the Constitution, holding that the "the principal effect of notification [is] to inform the public for its own safety, not to humiliate the offender." In *Connecticut Department of Public Safety v. Doe,* 538 U.S. 1 (2003), the Court found that Connecticut's sexual offender registration law, which requires the publication of an offender's name, address, and photograph on a website, does not violate the offender's procedural due process rights.

- In March, the Czech Republic's Interior Ministry published a list of Communist StB secret service collaborators on an Internet website. The Czech Republic's Office for the Protection of Personal Data stated that such a publication was not in conflict with the law on the protection of personal data.

- In November, the Florida Supreme Court, citing concerns over the wide distribution of confidential information over the Internet, temporarily ordered the state's judicial clerks to cease the online postings of certain court records. In June, public computers terminals at courthouses in British Columbia were shut down for several weeks after a visitor accessed confidential information concerning pending cases.

Trans-Border Transfer of Personal Data

- In *Criminal proceedings against Bodil Lindqvist,* Case C-101/01 (Nov. 2003), the European Court of Justice held that posting of information on a website that could be accessed globally did not constitute a cross-border transfer of data under the EU Data Protection Directive. The defendant in the underlying case had posted information about others, including details of a colleague's medical condition, on her personal website. The ECJ determined that the posting of the information was governed by the Directive and found that Mrs. Lindqvist's reference to a colleague's foot injury constituted "sensitive" personal information and was subject to rigorous protections. The ECJ ruled, however, that no information is transferred outside the EU when a website offering that information is hosted on an EU server.

- The U.S. Aviation and Transportation Security Act provides that by March 2003, all international airlines must provide the government electronic access to detailed passenger data on all travelers in the airline's computer system. The European Commission indicated that these data requests were not permitted under the EU Data Protection Directive. In December, the Commission indicated that the U.S. had agreed to implement adequate privacy safeguards, and airlines may accordingly transfer the requested airline passenger data to the U.S. This decision is subject to an opinion from the European Parliament.

- The EC Article 29 Working Party adopted a Working Document in June 2003, addressing corporate rules for trans-border transfers of personal information. Corporate rules are an alternative to other instruments that regulate international transfers of data, such as contractual clauses or the Safe Harbor Agreement. Such rules will constitute adequate protection if they are legally enforceable, bind the receiving company, provide third party beneficiary rights, and impose a duty of cooperation with data protection authorities.

- The European Commission recognized that the data protection laws of Argentina and Guernsey satisfy the adequacy requirements of the Data Protection Directive. Based on this adequacy assessment, EU member nations may transfer personal data to these regions. In November 2003, the EC Article 29 Working Party issued a report stating that the Isle of Man's data protection laws provide an adequate level of protection for personal data.

- In late 2003, India backed away from an earlier commitment to draft a comprehensive data protection law, and now plans to amend its existing Information Technology Act 2000. The Indian government also is seeking to persuade the European Commission to allow transfers of personal data to India from organizations based in the EU.

Workplace Privacy

- Following the mainstream view, the court in *United States v. Bailey,* 272 F. Supp. 2d 822 (D. Neb. 2003), found that an insurance company employee did not have an objectively reasonable expectation of privacy concerning his online activities at work when he had actual knowledge that his computer could be searched. In a different context, however, the court in *Fischer v. Mt. Olive Lutheran Church, Inc.,* 207 F. Supp. 2d 914 (W.D. Wis. 2003), indicated that an employer's intentional access to an employee's personal email account stored on a remote server owned by a third party may constitute a violation of U.S. law.

- Privacy issues have also arisen in the context of whether personal emails and other online content stored on government computers are subject to the applicable freedom of information laws. In *State of Florida v. City of Clearwater,* 28 Fla. L. Weekly S682 (Fla. 2003), the court indicated that personal emails transmitted or received by government employees fail to constitute public records based solely on their placement on a government-owned computer.

- However, in *In re Petition of the Board of Arapahoe County Commissioners,* 2003 WL 21664844 (Colo. Ct. App. July 17, 2003), the court found that the question of whether Colorado's Open Records Act exempts several hundred sexually explicit emails between elected officials must be determined through a three-factor test: (a) whether there is a legitimate expectation of confidentiality, (b) whether disclosure serves a compelling government interest, and (c) whether disclosure may be effected with minimal intrusion.

- In France, Portugal, and Great Britain, guidelines were issued concerning employee Internet use and the surveillance of employee emails. These guidelines generally require employers to provide employees with prior notice of monitoring activities and restrict the permissible grounds for engaging in monitoring. Courts in some EU jurisdictions, such as France, have greatly restricted the ability of employers to monitor employee emails and Internet use.

- In Denmark, a decision holding that an employer was justified in dismissing an employee for sending private emails during working hours and for accessing a sexually oriented chat website was reversed because the employer had failed to distribute an Internet-use policy and had not demonstrated that the employee's Internet use had affected his performance. The same court also affirmed a decision finding that an employer justifiably dismissed an employee who had sent racist emails in violation of the company's Internet use policy.

- In *Darwich v. Kaal Australia Party Ltd.,* the Australian Industrial Relations Commission found that an Australian employer did not violate the Workplace Relations Act by terminating the employment of an industrial worker who downloaded pornography onto factory computers.

- The newly enacted South African Regulation of Interception of Communications Act prohibits employers from monitoring employee email or other communications without obtaining the employee's written consent.

REGULATION OF ELECTRONIC MARKETING

Unsolicited commercial electronic mail and telemarketing came under increased political, legal, and regulatory scrutiny in 2003. The explosion in the increase of spam—which now accounts for roughly 15 billion messages per day and nearly 5.5 trillion messages per year—in connection with its associated costs, privacy issues, and security risks, led to regulatory efforts around the globe. Implementation of the national Do-Not-Call List in the United States prompted consumers to register an unprecedented 50 million telephone numbers for protection from unsolicited telemarketing. And governments began to tackle broader issues, including commercial email sent to wireless devices, the relationship between spam and pop-up advertisements, and the problems of cross-border commercial email and telemarketing.

National Telemarketing Regulation

- In the United States, federal telemarketing regulations that took effect on October 1, 2003 created a national Do-Not-Call Registry. Subject to limited exceptions, no telemarketing calls—meaning calls placed for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services—may be made to phone numbers that have been placed on this list. To date, more than 50 million such phone numbers have been added to the Registry. In general, only telemarketing calls made pursuant to an established business or personal relationship, with express consent, or to solicit a charitable contribution are not subject to the list. Violators are subject to fines of up to $11,000 per call.

- In September 2003, two last-minute court decisions blocked implementation of the Registry, which had been scheduled for October 1. On September 23, a federal district court in Oklahoma ruled in *U.S. Security v. FTC,* Civil No. 03-122 (W.D. Okla. 2003), that the FTC lacked statutory authority to promulgate a national do-not-call registry. Within two days, Congress passed a bill that explicitly authorized the FTC to implement and enforce such a list. President Bush signed the legislation immediately, mooting the court's decision.

- The same day that Congress passed the emergency bill, however, a second federal court barred implementation of the Registry on different grounds. In *Mainstream Marketing Services, Inc. v. FTC,* Civil No. 03-184 (D. Colo. 2003), the court held that applying the Registry to commercial telephone solicitations but not to telemarketing on behalf of charities violated the First Amendment because this content-based distinction did not advance any substantial governmental interest. The FTC appealed and asked the lower court to stay its ruling. At the same time, the FCC indicated that it would enforce the Registry even if the FTC could not. On September 29, the district judge refused to stay his ruling pending appeal and pointedly warned of "the substantial body of case law to the effect that a person enjoined cannot do indirectly through another what it is prohibited from doing directly." The FCC, however, maintained its vow to enforce the Registry on October 1.

- On October 7, the Tenth Circuit agreed to the FTC's request to stay the effective date of the district court opinion, finding that the FTC was likely to succeed on its argument that the content-based distinction between commercial and charitable speech in the regulations did not violate the First Amendment. The Tenth Circuit also consolidated the suit against the FTC with the suit against the FCC. Oral argument was held on November 10, and the court has not issued its decision. For now, the Registry is being enforced by the FTC and FCC.

Regulation of Unsolicited Commercial Email

- In November 2003, the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003," or "CAN-SPAM Act," became law. The Act regulates the transmission of "commercial electronic mail messages," which generally are defined as email messages with the primary purpose of advertising or promoting a commercial product or service. All commercial email must contain a web-based mechanism by which a recipient can opt out of future messages. Statutory damages against violators in some cases may exceed $1 million. Following the popularity of the Do-Not-Call List, the Act requires the FTC to submit to Congress a plan for a national Do-Not-Email Registry.

- In Europe, several EU Member States – including Austria, Belgium, Britain, Denmark, Ireland, Italy, and Spain – passed legislation to implement the European Union's Directive on Privacy and Electronic Communications (2002/58/EC). The e-Privacy Directive bans email with a direct marketing purpose unless the consumer has previously consented to receiving such communications. But the Directive contains an exception lifting the prior consent requirement when the sender has an existing relationship with the recipient, obtained the recipient's contact information legally, and is marketing its own products or services similar to those previously acquired by the recipient. This exception for existing customer relationships actually liberalizes laws in countries such as Spain, which previously had even stricter regulations on prior consent.

- Under the e-Privacy Directive, enforcement and imposition of penalties is left to each national government, and the Member States began in 2003 to establish liability and take enforcement actions. Ireland now provides for a €3,000 ($3,800) fine per unsolicited email message, while English law allows for a £5,000 ($9,000) fine in a magistrate's court or an unlimited fine in a jury trial. In May, a Danish court fined software and publishing company Fonn Danmark DKK 15,000 ($2,300) for sending unsolicited emails and faxes without the prior consent of the recipients. According to Denmark's National Consumer Agency, which filed the lawsuit, this was the first time an EU nation fined a company for sending spam.

- Australia passed anti-spam legislation in December 2003. That law also creates an opt-in regime, making it illegal to send commercial emails to or from Australia unless the recipient has provided affirmative consent. Certain organizations are exempted from the prior consent requirement, including educational institutions, registered political parties, and charities; the law also does not apply to messages containing primarily factual information. Offenders may face fines as high as A$1,100,000 ($805,500) for each day of violations.

- Asia, South Korea and Taiwan amended their laws to provide tougher penalties for those who violate rules regulating commercial email. South Koreans who send unsolicited adult messages to minors or use address-harvesting software will now face criminal penalties. Less serious violations, such as repeatedly sending email to recipients who have already opted out, are punishable by fines of up to 10 million won ($8,700). In Taiwan, spammers who flood ISPs could face up to three years in prison and NT$100,000 ($3,000) in fines.

- In Argentina and Colombia, courts issued injunctions for violations of more general privacy laws against bulk emailers who continued to send unsolicited messages after recipients repeatedly tried to unsubscribe from their mailing lists. Although the plaintiffs in the Argentinian case, *Tanus v. Cosa on Habeas Data,* made no monetary claims, Argentinian law allows for fines of up to 100,000 pesos ($34,500) for such offenses.

- Many Latin American countries—including Argentina, Brazil, Chile, Mexico, and Peru—debated anti-spam legislation. In Brazil, for example, draft legislation under consideration would permit companies to send each unsolicited message to a recipient only once and would require disclosure of the sender's name and address. Mexico's Congress has considered several versions of a data protection bill that would include an opt-in regime for email and telephone marketing offers.

- In December, the Direct Marketing Association of Singapore announced that it would establish a do-not-spam list for individuals who do not want to receive unsolicited email or cell phone text message advertisements. The registry is expected to be ready by early 2004.

Spam and Content Regulation

- Most anti-spam and telemarketing regulations include some content-based requirements, from mandatory labeling as an advertisement to required opt-out notices to distinguishing between messages with commercial and charitable purposes. These requirements gave rise to an increasing tension between the privacy rights of consumers and the free speech rights of marketers. Nowhere was this more apparent than in the United States, where an eleventh-hour court decision blocked implementation of the national Do-Not-Call Registry on First Amendment grounds, as discussed above.

- In the Netherlands, an appellate court upheld a ruling against a man who sent more than six million identical email messages to members of the Dutch Lower House, shutting down the government body's network server, against arguments that an order to stop spamming violated the sender's freedom of speech. The court retained some protection for the free speech rights of electronic marketers by limiting its ruling to restrict commercial email only where actual harm had occurred.

- Several countries require the use of specific phrases in all commercial email. In Japan, the Ministry of Economy Trade and Industry issued cease and correct orders in October to two Web site operators who failed to use the mandatory "unauthorized advertisement" indicator when sending unsolicited messages to cellular phones. Cell phone text messages are included in the anti-spam provisions of Japan's Specific Commercial Transaction Law.

- South Korea now requires all senders of unsolicited commercial email to end their subject headings with the @ symbol, making it easier for spam-filtering software to block unwanted messages. All unsolicited messages must also include an unsubscribe link in both English and Korean so that foreigners can block Korean-language commercial email.

- Most other commercial email regulations implemented in 2003 also contain content requirements. For example, United States law requires that all commercial email contain a valid physical postal address for the sender, notice of and the ability to opt out of future messages from the sender, and an identification that the message is an advertisement. The EU now requires that commercial emails truthfully identify the sender and provide a valid address for unsubscribe requests. And Australia mandates that commercial messages include accurate address information and a functional unsubscribe facility.

Spoofing and Deceptive Behavior

- State agencies were active in prosecuting spammers in 2003. Virginia's attorney general filed the first American spam-related felony charges in December, when two men were arrested for sending large volumes of unsolicited emails and falsifying transmission information to disguise the origin of the messages. If convicted, Jeremy Jaynes and Richard Rutowski face prison sentences of up to five years and maximum fines of $2,500 for each of the four felony charges brought against them. Jaynes is ranked eighth on a list of the world's top ten spammers compiled by Spamhaus.org, an anti-spam tracking organization.

- Suits were filed by attorneys general in New York, California, Missouri, and Washington under state anti-spam laws in 2003. One lawsuit, filed after six months of joint investigation by Microsoft and the New York attorney general, alleges that a New York-based spamming ring sent billions of fraudulent emails through 514 Internet Protocol Addresses in 35 countries to conceal the true source of the messages. One of the defendants, Scott Richter, is listed as the world's third most prolific spammer by Spamhaus.org. In *People v. Willis,* a California court awarded a $2 million default judgment under state law against a marketing company that had sent false and misleading email advertisements, and enjoined the company from sending further unsolicited emails.

Expanding Conceptions of Spam

- With so many jurisdictions now regulating traditional spam, the next area of focus may be other techniques by which entities use technology to engage in unsolicited direct marketing. The EU's e-Privacy Directive contemplates this issue and is drafted in technology-neutral terms. The provisions of the Directive apply equally to commercial communications sent to or from automated calling machines, fax, email, and mobile phone text messaging.

- The new U.S. CAN-SPAM Act addresses commercial email sent to wireless devices, requiring the FCC by October 1, 2004 to promulgate regulations to protect consumers. FCC telemarketing rules also address recent technological advances, prohibiting most calls that contain prerecorded messages, calls abandoned by autodialers, and calls made by telemarketers that do not include accurate caller identification information.

- In June, the Australian Communications Authority expanded its definition of spam to include text messages sent to mobile phones. Messages may only be sent with prior consent, and every message must provide information on how to unsubscribe. The regulations authorize penalties of up to A$250,000 ($167,300) per violation.

- South Korea also is targeting unsolicited advertisements distributed to mobile phones, including text messages and recorded or real-person voice messages. The new initiative establishes an opt-in standard for commercial email to wireless devices and bans all unsolicited advertising to cell phones between 9:00 p.m. and 8:00 a.m.

- In Germany in *T. v Dr. R., LG Dusseldorf,* No. 2a O 186/02, the Dusseldorf Regional Court held that chains of exit pop-up windows in Internet browsers are contrary to proper public order and therefore illegal under Germany's law against unfair competition. The court called these exit pop-ups a "burdensome or otherwise unwanted disturbance" for the user and compared them to spam.

- In *Federal Trade Comm'n v. D Squared Solutions LLC, No. AMD 03CV3108 (N.D. Md. Nov. 6, 2003), the court issued a* temporary restraining order against Internet promoters charged with using a feature of an instant messaging service to bombard computers with pop-up advertising and then offering for sale software to stop the onslaught of advertisements. The FTC's complaint was that the pop▪up advertising was creating undue interference with the consumers' reliable use of their machines.

Trans-Border Electronic Marketing

- Governments around the world began to address the problems of cross-border enforcement and uniform standards in 2003. For example, in January 2004, the European Commission released a formal Communication that identified a series of actions to complement EU rules regulating spam, including Member State enforcement, international cooperation and technical and self-regulatory measures.

- Australia and South Korea signed a memorandum of understanding in October to promote international spam regulation and exchange anti-spam information and techniques.

- The issues involving cross-jurisdictional marketing regulations apply to states within the U.S. as well as between countries. The CAN-SPAM Act preempts all state laws that expressly regulate commercial email, except to the extent that such state laws regulate falsity or deception. Aside from these provisions, state laws no longer apply whether they are more or less stringent than the federal law; thus, the opt-in regime set forth in California's new anti-spam law is preempted. However, state laws that are not specific to email, such as trespass, contract, or tort law, as well as state laws on fraud and computer crime, are not affected.

INTELLECTUAL PROPERTY

The year 2003 brought significant attacks on the provenance of the open source operating system Linux, the viability of its no-fee distribution system, and legitimacy of the General Public License (GPL), the intellectual bedrock of the open source movement. Unauthorized online exchange of music files in the U.S. reportedly slumped by fifty percent or more, perhaps due to the publicity surrounding hundreds of enforcement actions commenced by the Recording Industry Association of America (RIAA); the RIAA's preliminary success in enforcing subpoenas forcing Internet service provides to identify their file-swapping customers; and the emergence of lawful, licensed online music sources such as Apple Computer's iTunes. The U.S. Digital Millennium Copyright Act (DMCA) continued to be the source of litigation this year, including the first decision holding that a manufacturer of after-market supplies (in this case, printer cartridges) containing integrated circuits that interoperate with the initial product (in this case, laser printers) could rely on the DMCA to foreclose others from producing equally interoperable supplies. In the EU, significant new steps were taken in 2003 to establish uniform and higher standards of copyright enforcement and copy protection, while the prospects for any powerful legal protection for software patents there seemed to languish.

Copyright: General Developments

- SCO Group (formerly Caldera) filed suit against IBM in early 2003 alleging that IBM's distribution of Linux operating system software violated SCO's intellectual property rights and breached IBM's contractual obligations. Darl McBride, CEO of SCO, has described the general public license (GPL), which is often used in connection with open source software, such as Linux, as inconsistent with basic business principles and as unconstitutional. A trial is scheduled for 2005. SCO also announced plans to sue major users of Linux. A group of companies led by IBM and Intel have announced plans to establish a legal defense fund for use by corporate Linux users defending against SCO suits.

- In early 2003, the European Commission released a proposed "Directive on measures and procedures to ensure the enforcement of IPRs." The Directive would harmonize E.U.-wide the rules relating to the enforcement of copyrights and other intellectual property rights. The Commission's proposal, which is limited to infringements committed for "commercial purposes" or causing "significant harm," includes rules on civil *ex parte* searches, damages, injunctions and criminal penalties. Right holders seek to expand the Directive's scope to cover all infringements and otherwise strengthened, but some Member States have expressed concern over the EU's ability to legislate broadly in this area. ISPs have opposed the proposal, expressing concerns that it will impose burdens on them. The European Parliament is expected to vote on the proposal during the first quarter of 2004.

- The European Commission referred eight Member States to the Court of Justice for failing to implement the EU Directive on the harmonization of certain aspects of copyright and related rights in the Information Society, which was adopted by the European Parliament and the Council in 2001 and which Member States were required to implement by the end of 2002. The Commission explained that implementation of this directive is particularly important given that it serves as the means by which the European Union and its Member States implement the above WIPO treaties.

- Five new countries (Cyprus, Macedonia, Poland, Serbia and Montenegro, and Togo) signed the World Intellectual Property Organization Copyright Treaty in 2003, bringing the total number of adherents to 43. These treaties protect "literary and artistic works," including books, computer programs, music, art, and movies, in the digital world.

- The U.S. Supreme Court upheld Congress's extension of the copyright term by twenty years as a permissible exercise of Congress's power under the U.S. Constitution's copyright clause. *Eldred v. Ashcroft,* 123 S. Ct. 769 (2003).

- Publisher National Geographic won a case brought by freelance journalists who contributed to *National Geographic* magazine. In *Faulkner v. National Geographic Society,* No. 97 Civ. 9361 (LAK) (S.D.N.Y. Dec. 11, 2003), the court dismissed copyright infringement claims based on the Society's creation and sale of *The Complete National Geographic ("CNG"), a CD-ROM* and DVD compendium of past issues of *National Geographic* magazine in which the plaintiffs' works originally appeared. The *CNG* was produced through a digital scanning process to create an exact image-based reproduction of the magazine. The court found that the CNG was sufficiently faithful to the original print publication to constitute a privileged revision under Section 201(c) of the Copyright Act. The court distinguished *New York Times v. Tasini,* 533 U.S. 483 (2001) and disagreed with the pre-*Tasini* decision of the Eleventh Circuit in *Greenberg v. National Geographic Society,* 244 F.3d 1267 (11th Cir. 2001). In the continuation of the *Greenberg* litigation, however, a jury entered damages against National Geographic. In the 2001 Eleventh Circuit decision, the court held that the CNG infringed the copyright of another freelance contributor to *National Geographic* magazine on grounds that the CNG was a new collective work, e.g., due to its incorporation of a searchable electronic index. In the 2003 damages trial following this decision, the jury concluded that the Society's actions were willful and awarded Greenberg $400,000 in damages.

- The U.S. Court of Appeals for the Ninth Circuit revised its opinion in *Kelly v. Arriba Soft Corp., which* involved Arriba's use of thumbnail images and inline linking. In early 2002, the court held that Arriba's use of thumbnail images in its search engine constituted fair use, but that its inline linking (also known as framing, *i.e.,* importing the image from another web site and displaying it as part of its own web page, framing the image with text and advertising), was not fair use. 280 F.3d 934 (9th Cir. 2002). In July 2003, the

court withdrew this opinion and issued a replacement. In its new opinion, the court declined to address the inline linking issue on ground that parties had not moved for summary judgment on the issue, and remanded the issue for additional proceedings.

- In *U-Haul Int'l, Inc. v. WhenU.com, Inc.,* 279 F. Supp. 2d 723 (E.D. Va. 2003), the court held that software distributor WhenU.com does not infringe a web site owner's copyright in the web site content and appearance by virtue of WhenU.com's distribution of software that triggers pop-up advertising when that site is browsed. The court noted that this practice, known as "gatoring," did not alter the web page and therefore found no copyright infringement. Similarly, in a separate case against WhenU.com, the court in *Wells Fargo & Co. v. WhenU.com, Inc.,* 2003 WL 22808692 (E.D. Mich. 2003), held that the display of a pop-up ad does not create a derivative work in violation of a website operator's copyrights in its website because there was no access, incorporation or alteration of the website.

- In November 2003, the Federal Communications Commission adopted rules requiring manufacturers of digital television (DTV) equipment to include, by July 2005, the capability to recognize a "broadcast flag" encoded in DTV broadcast programming and to restrict the output or recording of so-called "marked" programming to approved technologies providing adequate protection against "indiscriminate redistribution" of the programming. The rules were adopted, at the behest of the movie studios and broadcasters and over the objections of computer and consumer electronics manufacturers and consumer rights advocates, with the goal of ensuring that high-value video content is available for over-the-air digital broadcast.

Copyright: Controlling Online Piracy

- The Recording Industry Association of America made headlines by executing a broad and coordinated copyright enforcement campaign targeting individual peer to peer (P2P) software users who had offered large numbers of copyrighted music works for others to download. By July 2003, the RIAA had served upon Internet Service Providers nearly 1,000 Digital Millennium Copyright Act (DMCA) subpoenas and, by December 2003, it had sued a total of 382 individuals. Reports indicate that it settled at least 220 of those lawsuits for payments in the range of $1,000-5,000. In addition, the RIAA offered an amnesty program to file-swappers who confess to unlawful file-sharing and promise under oath to delete all illegal files from their hard drives.

- Two rulings clarify the line between contributory infringement and non-liability for technology providers for infringing file sharing in P2P networks. In *Metro-Goldwyn-Mayer Studios (MGM) v. Grokster,* 259 F. Supp. 2d 1029 (C.D. Cal. 2003), the court took a bright-line approach to the Supreme Court's *Sony Betamax* decision, absolving from liability two companies that distributed P2P file trading software but had little ongoing involvement in their users' subsequent infringing online activity. The court held that Grokster and StreamCast, two of three distributors of P2P software for the FasTrack network, were not contributorily liable because, like sellers of VCRs and photocopy machines, they lacked knowledge of the specific acts of infringement at a time when they could use that knowledge to prevent the infringement. The court also held that defendants were not vicariously liable because they did not have the direct ability to police the user's conduct. The court's ruling turned on the fact that, unlike Napster, the defendants did not provide server-based directories that facilitated the use of their software to trade files, although the court hinted that the third FasTrack software distributor, Sharman Networks, whose similar case is still pending, might have some such involvement and therefore potential liability. The court indicated that there is no general duty to design software to prevent use in infringement and that providing general post-distribution product support or having the ability to communicate with users and upgrade their software is not enough to give rise to liability.

- By contrast, in *In re Aimster Copyright Litigation,* 334 F.3d 643 (7th Cir. 2003), the Seventh Circuit affirmed a district court's injunction shutting down a P2P network run by Aimster, a company that, like Napster, both distributed P2P software and supported the resulting network by providing server based directory functions. Judge Posner, writing for the Seventh Circuit in *Aimster,* affirmed the lower court's grant of a preliminary injunction against Aimster, a P2P service that, like Napster, ran a central server through which searches were directed. Aimster sought to defend on the grounds that it had designed its software to encrypt communications within the network so that, unlike Napster, it could not identify infringing transactions by examining information on its own servers. The Court held that this amounted to willful blindness and therefore satisfied the actual knowledge requirement for contributory infringement. In the process, Judge Posner sought to extrapolate the principles of *Sony to* provide some shelter from liability to companies that offer a service component, in cases where the burden of identifying and stopping infringing activity on their network would be disproportionate to the harm.

- On November 7, 2003, the U.S. Court of Appeals for the Seventh Circuit held that a senior member of an organization that disseminated copyrighted software freely over the Internet was not entitled to a jury instruction on "fair use" in his conspiracy trial where members' downloading of the software was not a noncommercial or educational use. The court said that it "strained credulity" to argue that the use was noncommercial because members did not pay for downloaded software and educational because a professor operated the Internet site. *United States v. Slater,* 348 F.3d 666 (7th Cir. 2003).

Copyright: Digital Millennium Copyright Act (DMCA)

- In *Recording Industry Association of America (RIAA) v. Verizon Internet Services, No.* 03-7015 (D.C. Cir. Dec. 19, 2003), the court reversed a district court ruling that the RIAA could use DMCA subpoenas to obtain the identities of P2P music file sharers from ISPs that merely provide them with Internet access accounts. The court relied on the plain language of Section 512(h), requiring a subpoena application to identify the specific material "to be removed or access to which is to be disabled" to conclude that the subpoena only applies to situations involving the storage of infringing material or links on the ISP's own servers. So interpreted, the subpoena authority extends to activities falling under the caching, hosting/storage and information locating tool safe harbors of Sections 512(b),(c) and (d), but not to activity such as the routing of email, instant messages, or P2P file transfers subject only to the "mere conduit" safe harbor of Section 512(a).

- The courts struggled with application of the DMCA's anti-circumvention provisions. In *Chamberlain Group, Inc. v. Skylink Tech., Inc.,* 2003 WL 22038638 (N.D. Ill. 2003), the plaintiff manufactures a garage door-opener system that operates through copyrighted technology. Defendant Skylink's universal garage door-opener achieved interoperability with Chamberlain's system by copying aspects of that technology, and Chamberlain sued under the DMCA. The court held that Skylink's conduct did not satisfy the statutory definition of "circumvent," which requires the defendant to have acted without the copyright owner's authorization. The court emphasized that Chamberlain imposed no post-sale restrictions on the use of its garage door-opening system, and that purchasers of its system had a legitimate expectation that, if their original garage door-opener is lost or damaged, they would be able to open their garage doors by using a replacement.

- By contrast, the court in *Lexmark Int'l v. Static Control Components, Inc.,* 253 F. Supp. 2d 943 (E.D. Ky. 2003), issued a preliminary injunction on similar facts. Lexmark's printers employ a cryptographic "secret handshake" that prevents any but its own toner cartridges to function with them and the defendant copied Lexmark's software to achieve interoperability so that its cartridges would work in Lexmark printers. These apparently conflict-

ing decisions have added a second front for critics charging that the DMCA tips the balance too far in the direction of protection of copyright holders, and brought in allies from longer standing antitrust law debates over whether manufacturers should be able to insulate themselves from competition in the aftermarket for replacement parts for their own products.

- In *Bonneville Intern. Corp. v. Peters*, 347 F.3d 485 (3d Cir. 2003), the court upheld the Copyright Office's rulemaking under the DMCA and the Digital Performance Right in Sound Recordings Act of 1995 relating to Internet streaming of AM/FM radio broadcasting programming. As a result, webcasters must pay record companies that hold performance rights in digital sound recordings for broadcasting these recordings over the Internet.

- On October 28, 2003, the Library of Congress announced four exemptions from the DMCA's prohibition against circumvention of technology that effectively controls access to a copyrighted work. The exemptions cover (1) lists of sites blocked by commercial Internet content filtering software, but not including spam-blocking lists; (2) computer programs protected by hardware dongles (i.e., anti-piracy devices) that are broken or obsolete; (3) computer programs or video games that use obsolete formats or hardware; and (4) e-books containing access controls that prevent "read-aloud" or other handicapped-user formats from being able to function. The DMCA requires the Library of Congress to consider every three years whether the operation of the statute adversely affects digital content users' ability to make non-infringing uses of particular classes of works. These exemptions do not, however, apply to the prohibitions on trafficking in circumvention devices.

- A Norwegian appeals court upheld the acquittal of Jon Lech Johansen, who created the DeCSS program used to pirate DVDs. DeCSS descrambles content encrypted with the CSS content protection system, which is used to encrypt DVD content. He had been charged with violating Norway's data protection laws.

- In August, the Supreme Court of California held that a preliminary injunction did not violate the state or federal free speech rights of a California computer programmer named Andrew Bunner, who posted DeCSS on the Internet. *DVD Copy Control Ass'n, Inc. v. Bunner,* 4 Cal.Rptr.3d 69 (Cal. 2003). The court held that the injunction burdened no more speech than necessary to serve the government's interest in encouraging innovation and development. It remanded the case to the Court of Appeals to assess whether there was a sufficient factual basis to support the injunction under California trade secret law.

Patents

- The U.S. Federal Circuit overturned a jury's fraud verdict in *Rambus, Inc. v. Infineon*, 318 F.3d 1081 (2003), which was based on Rambus's failure to disclose its patents and patent applications relating to the SDRAM standard adopted by a standards body known as JEDEC. The court stated that "A [patent disclosure] policy that does not define clearly what, when, how, and to whom the members must disclose does not provide a firm basis for the disclosure duty necessary for a fraud verdict." The FTC has charged Rambus with violations of antitrust and unfair competition laws on the same conduct, and that proceeding is ongoing.

- In September, the European Parliament took an initial vote on the draft Directive on software patents proposed by the European Commission. The Parliament's amendments would make it more difficult to obtain software patents in the EU and would ban patenting of algorithms or business methods. This action marks a significant step in the development of this Directive, but additional debate and compromise would be necessary before it is adopted.

- Enforcement of Internet-related patents has continued to rise with several large patent infringement verdicts resulting this year In *Eolas Technologies Inc. v. Microsoft Corp.*, No. 99-C626 (N.D. Ill. 2003), damages of $520.6 million were awarded in an infringement suit based on Microsoft's inclusion of patented web browser technology in Internet Explorer. In *Imagexpo LLC v. Microsoft Corp.,* No. 3:02CV751 (E.D. Va. 2003), the jury awarded $62.3 million in a patent infringement suit relating to Microsoft's NetMeeting software, an amount which would be tripled if willful infringement is found.

Trademarks and Domain Names

- In *Dastar Corp. v. Twentieth Century Fox Film Corp.,* 123 S. Ct. 2041 (2003), the Court reversed a Ninth Circuit decision relating to the defendant's inclusion of a copy of a television series that was in the public domain in a video without attribution to the creator. The Ninth Circuit had ruled that the absence of attribution constituted reverse passing off in violation of Section 43(a) of the Lanham Act. The Court interpreted "false designation of origin" to protect only producers of tangible goods and not creators of ideas or communications.

- In *U-Haul Int'l, Inc. v. WhenU.com, Inc.*, 279 F. Supp. 2d 723 (E.D. Va. 2003) and *Wells Fargo & Co. v. WhenU.com, Inc.*, 2003 WL 22808692 (E.D. Mich. 2003), the courts found no trademark infringement where WhenU used one company's trademarks to trigger the display of a pop-up ad from that company's competitor. In contrast, in *1800 Contacts v. WhenU.com and Vision Direct, Inc.*, 2003 WL 2299270 (S.D.N.Y. Dec. 22, 2003), the court stated that it disagreed with the above cases and was not bound by their findings.

- The Fourth Circuit overturned an arbitration decision requiring the transfer of a domain name to the City Council of Barcelona, Spain, affording the decision no deference "because a UDRP decision is susceptible of being grounded on principles foreign or hostile to American law." *Barcelona.com, Inc. v. Excelentisimo Ayuntamiento de Barcelona,* 330 F.3d 617 (4th Cir. 2003). Further, the court overturned the district court's application of Spanish trademark law and applied the Lanham Act to conclude that the Barcelona City Council had no trademark in the name "Barcelona" and had no right to the "Barcelona.com" domain name.

- In a groundbreaking decision, *America Online, Inc. v. aol.org*, 259 F. Supp. 2d 449 (E.D. Va. 2003), the court ordered the Public Interest Registry, which controls the ".org" domain name registry, to transfer the domain name of a foreign registrant of aol.org to America Online. The court held that where there is no personal jurisdiction over the registrant, and where a foreign registrar is uncooperative and declines to comply with a proper ACPA transfer order, a court may order a U.S.-based domain registry to effect the transfer.

- In *Pinehurst, Inc. v. Wick,* 256 F. Supp. 2d 424, 431 (M.D. N.C. 2003), the court held that, in view of "the unique nature of domain names in commerce," actual dilution of the plaintiff's mark necessarily results when the mark is incorporated in domain names by a third party, because "Plaintiff is unable to engage in electronic commerce under these domain names, which has reduced the selling power of Plaintiff's marks." In so holding, the court squared existing case law with the seismic 2003 U.S. Supreme Court decision on U.S. trademark dilution law in *Moseley v. V Secret Catalogue, Inc.,* 537 U.S. 418, 433 (2003).

- In *Interactive Products Corp. v. A2Z Mobile Office Solutions, Inc.*, 326 F.3d 687 (6th Cir. 2003), the court distinguished the use of another's trademark in a domain name, which, according to the court, sends an important signal to users about the source of origin and can constitute trademark infringement, from the use of a trademark in a portion of a URL other than the domain name, which does not typically signify the source of origin and is

therefore unlikely to create confusion and constitute trademark infringement. In *Paccar Inc. v. Telescan Technologies LLC,* 319 F.3d 243 (6th Cir. 2003), the same court rejected a fair use defense to a claim of domain name trademark infringement and found that users would be initially confused by adoption of plaintiff's trademark in the defendant's domain name and that the disclaimer of affiliation appearing on the defendant's website appeared too late.

CONTENT LIABILITY AND JURISDICTION

Free speech on the Internet continued to be contentious in 2003. The U.S. Supreme Court upheld a federal law requiring filtering software to be installed on computers in libraries that receive public funds against a First Amendment challenge, but a lower federal court struck down a law that prohibits making available content that is harmful to minors. The Council of Europe continued to garner signatures for its controversial protocol outlawing racist and xenophobic speech on the Internet. The content immunity for online service providers under the U.S. Communications Decency Act continued to be strongly enforced by courts, although two significant decisions seriously question its underpinnings. In the United States, courts have begun moving toward a "purposeful availment" test of jurisdiction, and in the European Union, a new regulation on choice of law threatens to undermine the beneficial "country of origin" rule established in the EU's E-Commerce Directive.

Regulation of Internet Content

- The Council of Europe convention outlawing racism and xenophobia on the Internet was opened for signatures in January. By the end of 2003, the agreement, which is a separate protocol to the convention on cybercrime, had been signed by 20 Member States, including France, Germany, and the Netherlands. Neither the United States nor Canada is a signatory.

- On June 23, 2003, the U.S. Supreme Court held constitutional a federal statute that conditioned public libraries' receipt of federal funds on the installation of filtering software on public Internet terminals. In *United States v. American Library Association*, 123 S. Ct. 2297 (2003), the Court held that Congress possesses wide latitude in choosing what activities to subsidize with federal support. The Court found that the fact that filtering software blocked content that would be protected by the First Amendment was not fatal because the law permits adults to request that the software be temporarily disabled.

- In *American Civil Liberties Union v. Ashcroft,* 323 F.3d 240 (3d Cir. 2003), the court again held that the Child Online Protection Act, which prohibits making available content that is harmful to minors, violated the First Amendment. The Third Circuit had previously ruled that the Act was unconstitutional, but that decision had been remanded to the court by the Supreme Court. Here, the Third Circuit found that the law failed because it imposes content-based restrictions on speech and restricts speech that is protected by the First Amendment. The court also found that the Act's reliance on adult verification systems impermissibly burdened adults' access to protected materials, and that it did not use the least restrictive means, such as filtering software. On October 14, 2003, the Supreme Court agreed to review the Third Circuit's decision.

- In draft right-of-reply guidelines released on June 30, 2003, the Council of Europe abandoned earlier plans to provide for robust rights of reply for all online content. The original proposal would have required all online media to ensure a right of reply through links attached to the original content. The June draft also abandoned plans to require newspapers to archive continuously updated online editions of their newspapers.

- In *Noah v. AOL Time Warner*, 261 F. Supp. 2d 532 (E.D. Va. 2003), the court held that chat rooms are not places of public accommodation because the Civil Rights Act only protected against discrimination in "establishments," or actual physical places. Accordingly, AOL was not required to take action to prevent anti-Islamic speech in chat rooms and forums.

- In December 2003, the German Commission for the Protection of Minors in the Media announced actions under a German law adopted in June. Website operators are required to identify a user's identity through a two-step process – first verifying that the person is an adult face-to-face, and second providing a PIN number or other feature to verify identity thereafter. The Commission contends that alternative methods, such as requiring bank account numbers to identify an adult, are insufficient because minors can obtain that information. The Commission announced that two websites required users to go to a post office or store for an initial face-to-face registration, which was consistent with the law.

Content Liability and Immunity

- In *Barrett v. Rosenthal*, 5 Cal. Rptr. 3d 416 (Cal. Ct. App. 2003), the court held that the Communications Decency Act's immunity provisions do not extend to a distributor of defamatory information. The decision explicitly challenged the conclusion of *Zeran v. AOL*, 129 F.3d 327 (4th Cir. 1997), the seminal case that determined that distributor liability was also barred by the CDA. The court applied the common law of defamation, particularly that distributors – unlike publishers – are liable if they convey information that they know to be defamatory, to overturn a lower court ruling which had found immunity for an individual who had made newsgroup postings that were alleged to be defamatory.

- In *Doe v. GTE Corp.*, 347 F.3d 655 (7th Cir. 2003), the court considered the applicability of the Communications Decency Act's immunity provisions to a web-hosting company that had hosted a website offering hidden camera videotapes for sale. Although the court found the hosting company not liable on state law grounds, it took a limited view of the CDA's immunity provisions in *dicta*. The court suggested that immunity may be limited to claims for which actual publication is an element, such as defamation. This statement is inconsistent with extensive precedent developed in the wake of *Zeran v. AOL*.

- In *Green v. AOL*, 318 F.3d 465 (3d Cir.), *cert. denied*, 124 S. Ct. 200 (2003), the court held that the Communications Decency Act, which gives interactive computer services immunity from being considered the publisher of content written by third parties, protected America Online from liability for a malicious computer program allegedly sent through an AOL chat room to a subscriber. The case appears to be the first to apply the Act's immunity provisions to computer code distributed through an interactive computer service.

- In two court cases decided this year, the Ninth Circuit continued to apply broadly the Communications Decency Act's immunity for interactive computer services. In *Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119 (9th Cir. 2003), the court held that the Act barred claims against an online dating service for permitting a third party to create a fictitious and allegedly damaging profile. And in *Batzel v. Smith*, 351 F.3d 904 (9th Cir. 2003), the court held that a listserv and website were eligible for immunity from liability for an allegedly damaging statement, which was authored by a third party, posted on its website, and distributed by its listserv. Near the end of 2003, the full membership of the Ninth Circuit declined to review the panel decision in *Batzel*.

- In *Bundesgerichtshof,* No. VI ZR 335/02, BGHZ 89, 376, Germany's highest civil court held that ISPs are not liable for user-posted content if the ISP is not informed of the unlawful content and notified of its precise location. The court said that its ruling instituted a "knowledge" requirement on ISP liability for illegal content and ruled that it is the burden of the complaining party to prove that the ISP was notified of the content and its location. In this case, the complainant stated that he had provided notice, but he had not retained copies.

ISP Disclosure

- In *Heisei 15 wa No. 3994*, a Japanese court ruled that an Internet service provider must disclose the name and address of a user alleged to have posted a defamatory message on the Internet, even if transmitted anonymously. It is apparently the first time an ISP has been ordered to release identifying information in a civil suit. The ruling followed an earlier ruling that Yahoo Japan was required to disclose certain information it possessed (including an IP address) concerning the poster of a statement on Yahoo's bulletin board.

- In *Theofel v. Farey-Jones*, 341 F.3d 978 (9th Cir. 2003), the court found that the defendants had violated the Stored Communications Act when they served a subpoena on an ISP that requested production of emails that were unrelated to the underlying litigation.

- In *La Societe Metro Cash & Carry France v. Time Warner Cable,* 2003 WL 22962857 (Conn. Super. Ct. Dec 2, 2003), a court ordered an ISP to turn over subscriber information to a French company that established probable cause for a defamation action. The plaintiff had sought and obtained an order from a French court requiring disclosure of the name, address and telephone number of the subscriber who opened the Internet account.

- In *Melvin v. Doe*, 836 A.2d 42 (Pa. 2003), the Pennsylvania Supreme Court held that an intermediate court was obliged to consider an appeal of an order seeking the disclosure of the identity of an anonymous Internet poster. The Supreme Court held that the identity of the poster was sufficiently distinct and important to warrant an immediate appeal, and that a meaningful appeal would be lost if the appeal occurred after the release of the poster's identity. The court also noted that "the constitutional right to anonymous free speech is a right deeply rooted in public policy that goes beyond this particular litigation." *Id.* at 50.

Defamation

- In *Dow Jones & Co. v. Harrods Ltd.*, 346 F.3d 337 (2d Cir. 2003), the court upheld a lower court ruling declining a request by Dow Jones & Co., publisher of the Wall Street Journal, that the court issue a declaratory judgment finding that Harrods could not, consistent with the First Amendment and due process, subject it to a libel suit in an English court under English law, which greatly favors plaintiffs. The action concerned a claim by the London retailer that a statement in the Wall Street Journal's online edition was defamatory under English law, although the statement was unlikely to be actionable under U.S. law.

- In *Mitan v. Davis*, 243 F. Supp. 2d. 719 (W.D. Ky. 2003), the court held that a single publication date – the date of first publication – applies to allegedly defamatory materials posted on the Internet. The single publication date has the effect of starting the applicable statute of limitations on any action brought alleging liability because of the statement. The court found that Kentucky state courts had not addressed similar issues since 1899, and the court looked to a 2002 New York Court of Appeals case, *Firth v. New York,* 98 N.Y.2d 365, 775 N.E.2d 463 (2002), for guidance.

- In *Varian Medical Systems v. Delfino,* 113 Cal. App. 4th 273 (2003), the court ruled that former employees, who had posted allegedly defamatory information about their former employer, were not protected by the anonymous or unverified nature of Internet communications. The defendants had argued that, because the Internet is filled with anonymous postings of uncertain veracity, a typical person would not believe that their 13,000 posted statements were factual. Separately, the court ruled that part of the injunction barring the defendants from making future Internet postings about their former employer was an unconstitutional prior restraint on their First Amendment rights of free speech.

- In *Bahlieda v. Santa*, [2003] 64 O.R. 3d 599, the Ontario Court of Appeals overturned a lower court ruling finding that Internet postings of information are equivalent to broadcasting on television or radio. The effect of the earlier ruling was to make defamatory information published on a website subject to the province's libel laws. The court focused on the law's definition of "broadcasting," particularly the reference to "broadcasts from a station in Ontario," to rule that the lower court had erred in its construction of the definition.

Jurisdiction in the United States

- In *Toys R Us, Inc. v. Step Two, SA*, 318 F.3d 446 (3d Cir. 2003), the court held that personal jurisdiction is not appropriate when a defendant has failed to purposefully avail himself of the forum state, even if the defendant operates a fully interactive website that is accessible from the forum state. The Third Circuit found that more recent cases have required additional factors – such as targeting the residents of the forum state or conducting business with those residents – even if the website in question is highly interactive. In this case, the court found that the defendant's website did not target New Jersey consumers, was in Spanish and had address forms that did not fit U.S.-based addresses. The court noted that its reasoning was consistent with the Fourth Circuit's decision in *ALS Scan, Inc. v. Digital Serv. Consultants, Inc.*, which relied on factors additional to mere interactivity. In early 2003, the Supreme Court declined to review the *ALS Scan* case. 537 U.S. 1105 (2003).

- In the spring of 2003, the U.S. Supreme Court declined to review two cases related to personal jurisdiction based on Internet contacts with the forum state. The court let stand a Fourth Circuit ruling holding that a Connecticut newspaper website could not be subject to personal jurisdiction in Virginia on the basis that the newspaper had not directed its content at Virginia residents. *Young v. New Haven Advocate*, 315 F.3d 256 (4th Cir. 2002), *cert. denied*, 123 S. Ct. 2092 (2003). And in *Healthgrades.Com Inc. v. Northwest Healthcare Alliance Inc.*, No. 01-35648 (9th Cir. Oct. 7, 2002), *cert. denied*, 123 S. Ct. 1909 (2003), the court declined to review a Ninth Circuit ruling that a state court can exercise jurisdiction over an out-of-state operator of a website on the basis of foreseeable effects of its web postings.

- In *Gator.com. v. L.L. Bean, Inc.*, 314 F.3d 1072 (9th Cir. 2003), the court held that Maine-based L.L. Bean clothiers was subject to general jurisdiction in California because of the multimillion-dollar merchandise sales made in California over its highly interactive website. The case arose from a declaratory judgment action brought by Gator.com in response to a cease-and-desist letter sent by Bean concerning Gator's software that causes pop-up ads to appear when browsing certain sites, including Bean's. Bean is not registered to do business in California, but the court found that its substantial and continuous contacts with California—based only on Bean's online presence in the state—meant that Bean was subject to general jurisdiction in California even for suits unrelated to its contacts with the state.

- In *MGM Studios v. Grokster Ltd.*, 243 F. Supp. 2d 1073 (C.D. Cal. 2003), the court held that the large number of downloads by residents of California over the defendant's peer-to-peer file-sharing systems was sufficient to establish personal jurisdiction in California. The court noted that the defendants had provided software to millions of California residents, that the defendants purposefully availed themselves of California law by their interactions with California residents, and that the effects of their actions were felt in California.

- In a variety of decisions, courts generally continued to require that website operators direct some of their activity specifically to the forum state for jurisdiction to be found. Websites that were available in the forum state merely because they were available everywhere were ruled insufficient to support jurisdiction in *Hammer v. Trendl,* No. CV02-2462 (ADS) (E.D.N.Y. Jan. 18, 2003) (comment posted on Amazon), *Falwell v. Cohn*, No. CIV.A.6:02 CV00040 (W.D. Va. Mar. 4, 2003) (website critical of religious figure), *Riddell Inc. v. Monica*, No. 03C 3309 (N.D. Ill. July 25, 2003) (website that only permitted the submission of contact information), *Equidyne Corp. v. Doe,* 279 F. Supp. 2d 481 (D. Del. 2003) (comment posted on an online message board), and *Pound v. Airosol Co.*, No. CIV.A. 02-2632-CM (D. Kan. Aug. 21, 2003) (website that invites telephone orders). In *Realuyo v. Villa Abrille*, No. 01 CIV. 10158 (JGK) (S.D.N.Y. July 8, 2003), the court followed this trend to decline jurisdiction over a news website that had some 300 registered users in the forum state.

- Domain name disputes also led to jurisdictional holdings. In *Cable News Network L.P., v. CNNews.com,* No. 02-1112 (4th Cir. Jan. 23, 2003), the court held that the Anticybersquatting Consumer Protection Act's *in rem* jurisdiction provision was sufficient to permit the exercise of personal jurisdiction over a website registrant located in Hong Kong. And in *Radio Computing Services, Inc. v. Roland Computing Services*, No. 00 CIV. 1950 (S.D.N.Y. Mar. 13, 2003), the court held that negotiations over the purchase of a domain address were insufficient to establish personal jurisdiction. The court distinguished prior cases finding jurisdiction when an alleged cybersquatter contacts a mark holder about selling a domain at an inflated price, which amount to attempted extortion within the forum state.

Jurisdiction in Europe

- In Europe, the emerging trend continued in favor of expanding jurisdiction to reach foreign e-commerce websites. In a Dutch case, *Ladbrokes v. De Lotto*, which indicates that a website can be subject to the laws of all the countries where it can be accessed, the Arnhem Court of Appeal ordered bookmaker Ladbrokes to block Dutch residents from placing sports bets on Ladbrokes' website. This injunction was ordered in response to claims by De Lotto, the Dutch sole permit-holder for sports bets, that Ladbrokes was contravening De Lotto's permit by offering gaming services in the Netherlands. The court rejected Ladbrokes' argument that the games offered on its website should not be deemed to be offered in the Netherlands and stated that the decisive element in reaching this decision was that it was possible to participate from computers located in the Netherlands via the Ladbrokes website and receive payment of prize money in Dutch bank accounts. The fact that the text of the website was in English was not considered as relevant.

- The European Commission issued a report stating that the E-commerce Directive (Directive 2000/31/EC), due to have been implemented by January 2002, is now in force in 12 Member States. The remaining countries (France, the Netherlands and Portugal) are in the advanced stages of implementation. The Directive introduced into EU law a "country of origin" principle, under which providers of e-commerce services are generally subject to regulation only in the country in which they are established.

- In Europe, the courts must give effect to the Brussels Regulation (Council Regulation (EC) No. 44/2001), which now has taken effect. The Regulation 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 in the consumer's home country. The scope of Internet activities reached by this term remains undetermined. Conversely, businesses filing suit against a consumer must choose a forum in the consumer's country.

- In connection with an initiative related to the Brussels convention, the proposed Law Applicable to Contractual Obligations (known as the "Rome I Convention"), the European Commission is consulting with stakeholders regarding its intention to modernize and transform the Rome I Convention into EU law. The Convention, which governs what country's law applies to contractual obligations, is based upon the notion that parties can select the law applicable to their contract. If the parties fail to select an applicable legal regime, the Convention applies the "proximity principle" -- the contract is governed by the law of the country with which it "has the closest links." The Commission hopes to modernize the Convention by, among other things, ensuring that it addresses issues such as consumer protection and cross-border employment contracts.

- The European Commission also proposed a new regulation on choice of law in non-contractual disputes, including tort claims such as defamation and invasion of privacy (the "Rome II" regulation). The draft provides that the law of the country in which the damage arises will generally apply. It has been criticized by the business and media communities, which see it as undermining the "country of origin" concept in the E-Commerce Directive. The Rome II draft is likely to be voted upon by the European Parliament in 2004.

- In the U.K., the U.S. online content provider, Amazon.com, was sued for defamation after it posted a critical review of the plaintiff's book on its U.S. website, which U.K. residents then were able to read and download. Although the case remains pending, the U.K. court has determined that it had jurisdiction to resolve the dispute. *Vassiliev v. Amazon.com*, 2003 EWHC 2302 (QB) (2 Oct. 2003) (J. Eady).

- Similarly, a Spanish court ruled in 2003 that it had jurisdiction to decide a copyright infringement claim brought against a U.S.-based website on which illegal "cracks" were placed and made available to Spanish residents. The court ruled it had jurisdiction because the defendant's activity was both organized in Spain and had demonstrable effects there.

ELECTRONIC COMMERCE AND TAXATION

The law of electronic commerce and consumer protection developed at a modest pace in 2003. Existing initiatives to create international legal frameworks remained in the deliberation phase. U.S. legislators continued their efforts to clarify the treatment of information products under existing contract law, and courts reinforced the emerging trend that "clickwrap" agreements will generally be found to be enforceable.

Electronic Contracting

- Two proposed international treatises remain works in progress. The United Nations Commission on International Trade Law (UNCITRAL) continues to draft a convention on electronic contract formation, but the overall scope of the instrument remains a matter of discussion. The Hague Conference on Private International Law narrowed its scope to preparing a framework for jurisdiction and enforcement of judgments that would set rules for courts to enforce provisions in business-to-business agreements that designate a forum for adjudication of disputes.

- In the United States, the sponsor of the Uniform Computer Information Transactions Act (UCITA), the National Conference of Commissioners on Uniform State Laws (NCCUSL), announced in August that it would no longer push for state legislatures to adopt the draft model law that aims to harmonize states' laws concerning e-commerce and set default rules in computer contracts. Consumer groups have criticized UCITA as being anti-consumer and too deferential to the software industry. Only Virginia and Maryland have adopted the law, and at least four states have adopted anti-UCITA measures.

- The American Law Institute and the NCCUSL proposed updates to the Uniform Commercial Code (UCC). To clarify the applicability of the UCC to information products, the drafters of the amendments propose that the definition of "goods" in Article 2 be amended to make it clear that the term does not include information. Under the revised definition, a transaction in pure information, such as software downloaded from the Internet, would not constitute "goods," whereas a "good" which incidentally incorporates information would be considered a transaction in "goods." Drafters will present the final draft law to the ABA's House of Delegates at the ABA's mid-year meeting in February 2004.

- Until the proposed amendments to Article 2 of the UCC come into force, it remains up to the courts to rule on the applicability of the UCC to information products. Courts have favored treating standardized software as goods for purposes of the UCC, such that the UCC default rules will apply to contracts for such software. In *Olcott International & Co. v. Micro Data Base Systems Inc.,* 793 N.E.2d 1063 (Ind. App. 2003), the court held that a contract for the sale of pre-existing software is a contract for the sale of goods, not services. The court distinguished the software from a program that is designed to meet a customer's specific needs, which would be a contract for services. Similarly, in *Pearl Investments, LLC v. Standard I/O, Inc.,* 257 F. Supp. 2d 326 (D. Me. 2003), the District Court of Maine found a contract for the development of customized software to be a contract for services and therefore outside the scope of the UCC.

Securities and Banking

- In the United States, the Check Clearing in the 21st Century Act (C21) was enacted in October. C21 permits banks to send a paper "substitute" check that is an image of the original, instead of having to return original checks to customers' banks once they have been processed. For legal purposes, the substitute check carries the same validity as the original.

- EU Member States are moving forward in implementing the Distance Marketing of Consumer Financial Services Directive (2002/65/EC). The Directive, which must be implemented by October 2004, sets rules for the sale of retail financial products (such as credit cards, mortgages, investment funds and pensions) to consumers without face-to-face contact. The supplier must give consumers minimum levels of information about the firm before entering into the contract and ensure that consumers can cancel certain types of contracts within a specified time limit. In the U.K., the financial services regulator, the Financial Services Authority, has stated that it intends to publish its rules in March 2004.

- Italy's securities regulator, CONSOB, published in May updated guidelines for companies disclosing price-sensitive information, the first update of the guidelines to take into account the use of Internet technology. The guidelines make it clear that the distribution of false, preferential or other price-sensitive information by electronic means is subject to the same rules, limits and penalties as those already in place for other forms of official communication.

- South Korea's financial regulator, the Financial Supervisory Commission, issued in September guidelines extending brokerage record-keeping requirements to email and instant messaging communications. The guidelines require securities companies to maintain a back-up database of business email, instant messaging communications and web-based email messages generated from their brokerage and research operations.

Clickwrap and Browsewrap Agreements

- A number of United States courts addressed the enforceability of so-called online clickwrap and browsewrap consumer agreements. Typically, clickwrap 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 before gaining access to the product. Browsewrap agreements typically state that the user, by staying to browse the website, consents to the terms that are available for online viewing at any time.

- In *Ticketmaster Corp. v. Tickets.com Inc.*, CV 99-7654-HLH (VBKx) (C.D. Cal. Mar. 7, 2003), the District Court for the Central District of California held in March that although the court preferred a rule of law that would require that a contract could only be formed where there was a manifestation of "unmistakable assent," such as a click through, case law did not support such a rule. Instead, the court said that case law involving cruise tickets and parking tickets has established that such assent is not necessary for contract formation and ruled that a contract can be formed by proceeding into the interior web pages after knowledge (or, in some cases, presumptive knowledge) of the conditions accepted when doing so.

- In addition, in *Net2Phone Inc. v. Superior Court,* 135 Cal. Rptr. 2d 149, 153 (Cal. Ct. App. 2003), the court that a consumer contract containing a forum selection clause is not unenforceable merely by reason of the fact that the forum selection clause is disclosed to consumers via an Internet hyperlink or because it is presented to Net2Phone for users as a "take it or leave it" proposition and not vigorously "bargained for."

Electronic Signatures

- The European Commission found that most Member States have implemented the Electronic Signatures Directive (1999/93/EC) in a proper manner. It also found that several non-EU countries, including accession countries and members of the European Economic Area such as Norway, had based electronic signatures laws on the Directive. The study concludes that all European countries recognize to varying degrees the legality of "advanced" electronic signatures that meet certain requirements. However, only eight countries have transposed explicitly the Directive's requirement that electronic signatures be treated in the same way as regular signatures. Spain is currently enacting new legislation on electronic signatures.

- Mexico and Hong Kong introduced legislation in 2003 that gives legal effect to electronic signatures. The Hong Kong legislation is designed to supplement existing legislation that only gives legal recognition to signatures generated by certain forms of technology. The new bill aims to give legal recognition to all forms of electronic signatures for transactions that do not involve the government and to permit the service of documents in electronic form where service is required to be by mail or in person.

Distance Selling

- In Turkey, the government enacted legislation that deals with online transactions, similar in many respects to the Distance Selling Directive that has been implemented by all 15 EU Member States. The Distance Selling Directive aims at reinforcing protection of consumers involved in contracts concluded in non face-to-face situations, in particular over the Internet, and by mail, telephone and fax, and gives consumers certain cancellation rights.

Provision of Internet Services

- In *Waters v. Earthlink, Inc.*, No. 02-1385 (1st Cir. Oct. 31, 2003), a U.S. court upheld the judgment of a district court that an arbitration clause contained in an ISP agreement is not enforceable against the subscriber, absent evidence demonstrating that the subscriber should have seen links to the customer agreements posted on the ISP's web site.

- In *America Online, Inc. v. St. Paul Mercury Insurance Co.*, 347 F.3d 89 (4th Cir. 2003), the court held that an ISP's insurer has no duty to defend the ISP against allegations that its software altered customers' existing software, disrupted their network connections, caused the loss of stored data, and caused their operating systems to crash. The consumers' underlying complaints claimed damage to software. The insurance policy at issue covered liability for "physical damage to tangible property," not damage to data and software.

Online Pharmacies

- In *Rx Network of South Florida v. Drug Enforcement Administration*, 03-CV-6192 (SD Fla., 2003), a federal judge rejected a request by an Internet pharmacy to block the Drug Enforcement Administration from suspending its certificate of registration, after it was shown to the court that prescription diet pills had been sold online without the consumers having first been examined by a physician.

- In Europe, in *Deutscher Apothekerverband e.V. v. DocMorris NV*, C-322/01 (2003), the European Court of Justice ruled in December on the legality of a German law that prohibits imports of medicines by mail order by pharmacies authorized in other Member States in response to individual orders placed on the Internet. In regard to medicines authorized for sale on the German market, the court stated that a national prohibition on the sale of medicines by mail order is a restriction on the free movement of goods and that therefore the prohibition was unjustified in relation to non-prescription medicines. In relation to prescription medicines, the court held that allowing sale by mail order posed a risk to consumers and that the prohibition was justified. In regard to medicines that had not been authorized in Germany, the court found the prohibition laid down by German law to be in line with EU law requiring medicines to be authorized.

Internet Gambling

- Courts both in the United States and in Europe considered issues surrounding Internet gambling in 2003. In the United States, in *Retailers National Bank v. Harding*, No. VG03097502 (Cal. Super. Ct. Aug. 7, 2003), the court held that it is illegal to compel a California resident to pay credit card debts incurred in online, casino-style gambling, because the collection of such debts is against public policy and because the financial services companies, by processing the transactions, further criminal activity. Legislation is also under consideration in the United States that would prohibit the use of credit cards, wire transfers and other financial instruments to fund Internet gambling.

- In *Piergiorgio Gambelli,* No. C-243/01, the European Court of Justice ruled that licensed U.K. bookmakers are free to take bets from gamblers in Italy through data transfer centers in Italy, despite Italian legislation reserving the taking of bets for state or state-licensed undertakings. The judgment implies that any betting organization that is established in another European Member State and carries out its activities in accordance with the legislation of that State should also be permitted to carry out business in any other Member State, unless restrictions imposed by that State are justified on consumer protection grounds.

Other Consumer Protection Developments

- In the United Kingdom, the Office of Fair Trading and 55 local trading standards authorities carried out in April an investigation into websites in the travel industry sector, to identify those making potentially misleading claims about travel deals. The investigation was part of an international sweep, conducted in conjunction with 87 enforcement agencies in 24 countries. Initial analysis of the U.K. results is reported to suggest that 40 per cent of the U.K. websites investigated contained potentially misleading claims.

- In Germany, a local court in *Harder v. MSM Fotoshop*, AG Westerburg, No. 21 C 26/03, 2003, held that an Internet trader must comply with an electronic contract containing an error in price, because the trader did not rescind the contract "promptly" as is required under the German Civil Code.

- Also in Germany, in *Zentrale zur Bekämpfung unaluteren Wettbewerb e.V.*, 26 O 33/02 CR (2003), the Irish airline Ryanair.com Limited lost a lawsuit against the German Competition Protection Counsel with regards to Ryanair's online terms and conditions. The District Court of Cologne ruled that Ryanair's terms and conditions were void because they were not generally understandable to a consumer. The court based this judgment on the fact that text on a computer screen is not as easy to read as that from a hard copy, regardless of the fact that consumers can print out the online terms and conditions. Ryanair has appealed.

Internet Tax Legislation

- In the United States, Congress did not pass an extension to the Internet Tax Freedom Act ("ITFA"). Originally passed in 1998, the ITFA created a three-year moratorium on multiple or discriminatory taxes on electronic commerce and limited state authority to impose new taxes on accessing the Internet.

- In 2003, bills were introduced in both the U.S. House and Senate (H.R. 49 and S. 150) to make the Internet tax moratorium permanent. The House passed its version of the Internet tax moratorium in September 2003, but the Senate never brought its version to a vote. Both the House and Senate versions of the bill permanently extended the existing Internet tax ban, eliminated certain Internet taxes currently being imposed by some states (*i.e.* the states that were exempted from ITFA), and expanded the definition of Internet access to make all forms of technology used to provide such access nontaxable.

- Legislation was introduced in both the U.S. House and Senate (H.R. 3184 and S. 1736) to give qualifying states the authority to require retailers to collect legally owed sales and use taxes on remote transactions. Qualifying states would have the authority to require collection of sales taxes even in states where the retailer does not have a physical presence. To qualify, states would have to simplify their sales tax systems based on criteria in the Streamlined Sales Tax Project ("SSTP"), an effort by over thirty states to simplify sales tax systems as an inducement to get retailers to collect. Small businesses

with gross remote taxable sales nationwide of less than $5 million in the preceding calendar year would be exempt from the collection requirement.

- The 39 states and the District of Columbia currently participating in the SSTP continued to work towards the launch of a nationwide uniform sales tax system. States participating in the SSTP adopt the Streamlined Sales and Use Tax Agreement ("SSUTA"). This agreement sets forth common definitions of taxable goods, creates uniform sourcing rules, and restricts the number of sales tax rates within a state. The agreement also creates state-level administration of all sales and use taxes, requires local jurisdictions to use the same tax base as the state, and imposes other simplifying administrative changes. Uniformity in the assessment and collection of state sales and use taxes is intended to help states overcome restrictions on the collection of sales and use taxes by out-of-state vendors, such as Internet retailers.

- Under the terms of the SSUTA, the uniform state sales tax system does not take effect until 10 states, representing 20 percent of the population of the states with sales and use taxes, are certified as having conformed to the terms of the agreement. In June, North Carolina adopted conforming legislation, bringing the total number of states that have adopted the SSUTA to 17 and raising the population percentage to just above 20 percent. To "certify" that these states have conformed to the terms of SSUTA and, therefore, officially launch the streamlined sales tax system, a formal governing body for the SSTP must be formed. In November, the participating states approved a plan that began laying the groundwork for a governing board. Officials estimate that the system will be launched in 2005.

- The European Union passed a new law, effective July 1, 2003, requiring non-EU companies to collect value-added taxes (VAT) on digital goods sold online. The law applies to a broad range of digital products, including digital delivery of software and computer services generally, cultural, scientific, educational, entertainment, and similar services, as well as television and radio broadcasting services.

PRIMARY OFFICE CONTACTS

Washington

Mark Plotkin
202.662.5656
mplotkin@cov.com

Kurt Wimmer
202.662.5278
kwimmer@cov.com

New York

Bert Wells
212.841.1074
bwells@cov.com

San Francisco

Evan Cox
415.591.7073
ecox@cov.com

London

Lisa Peets
+44.(0)20.7067.2031
lpeets@cov.com

Brussels

Dave Harfst
+32.(0)2.549.5251
dharfst@cov.com

Individual biographies and additional information about the firm and its practice appear on the firm's website, www.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 32.2.549.5230
Fax 32.2.502.1598

www.cov.com