WORLD INTERNET LAW REPORT

Volume 3, Issue 7 July 2002

Monthly News & Comment on Internet Law and Regulation from Around the World

HIGHLIGHTS

NEWS

ARGENTINA'S Supreme Court judges passed a resolution requesting the government to enact legislation expressly penalising hackers, after the Court's website was vandalized. (Page 3)

THE EUROPEAN PARLIAMENT has approved draft legislation requiring ISPs and telephone companies to retain traffic data records for possible scrutiny by crime-fighting authorities, despite protests by industry and privacy campaigners (Page 5). A new **French ISP** has initiated a system that refuses to store any data about users' on-line activity. (Page 8)

CAMPAIGNERS in the United States are also criticizing the expansion of investigatory powers for the FBI (Page 13), while the Federal Communications Commission's deadline is imminent for service providers to install surveillance-enabling technology. (Page 16)

ELECTRONIC MONEY INSTITUTIONS are having to meet stringent new regulations in the United States (Page 14) and the United Kingdom (*Anna Tweedale of Eversheds*) (Page 12); and Luxembourg too has implemented the E.C. Directive on electronic money institutions (*Stéphan Le Goueff of* LE GOUEFF*@vocats.com*) (Page 9).

CASE REPORTS

IN CANADA, an on-line lottery with a valid provincial licence has nevertheless incurred criminal penalties because the lottery would not be conducted entirely within that province (*Theodore C. Ling and Arlan Gates of Baker & McKenzie*). (Page 18)

AN ISP in Canada has been ruled entitled to change the terms of its contracts with users by notices via a website, even though the alterations did not appear on its homepage (*Theodore C. Ling and Arlan Gates of Baker & McKenzie*). (Page 19).

TENNIS PLAYER Steffi Graf successfully sued an ISP in Germany for objectionable content posted on its server by a private user. (Page 21)

IN THE UNITED KINGDOM, the High Court has held that search engine "optimization" can amount to trademark infringement even if a website owner's use of another's trademark is invisible to Web surfers (*Charlie Swan of The Simkins Partnership*). (Page 22)

A FORUM STATE in the United States could exercise jurisdiction over a domain registrar who had transacted some 5,000 domain name registrations with residents of the state, ruled the 6th Circuit (Page 23).

SERIAL CYBERSQUATTER John Zuccarini has been barred from carrying on his deceptive activities, in a suit brought by the Federal Trade Commission. (Page 25)

A CONTRACT for the sale of real property was upheld by the Massachusetts Superior Court although it was concluded entirely by e-mail. (Page 27)

COMMENTARY

POLAND: Poland Gears Up For E-Commerce (*Jerzy Gawel, and Pawel Litwinski and Marek Swierczynski of Traple, Konarski, Podrecki Law Office*). (Page 30)

ITALY: Electronic Money: The New Italian Rules (*Alessandro del Ninno of Studio Legale Tonucci*). (Page 33)

INTERNATIONAL DEVELOPMENTS

NETWORK SECURITY: The OECD is revising its guidelines on the security of information systems to make them more accessible to computer users. (Page 36)

IN THIS REPORT

NEWS

CASE REPORTS

COMMENTARY

INTERNATIONAL DEVELOPMENTS

Submissions by Authors: The editors of *World Internet Law Report* invite readers to submit for publication articles that address issues arising out of the regulation of the Internet and e-commerce, either on a national or transnational level. Articles with an appeal to an international audience are most welcomed. Prospective authors should contact The Editor, World Internet Law Report, c/o BNA International Inc, Heron House, 10 Dean Farrar Street, London SW1H 0DX; tel. (+44) (0)20 7559 4800; fax (+44) (0)20 7233 2313; or E-mail: deborah_hicks@bna.com. If submitting an article by mail please include a diskette with the article typed in plain text or in Microsoft Word or WordPerfect formats.

WORLD INTERNET LAW REPORT

WORLD INTERNET LAW REPORT is published monthly by BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., Washington, D.C., U.S.A. Administrative headquarters: Heron House, 10 Dean Farrar Street London SW1H 0DX, England. Tel. (+44) (0)20-7559 4801; Fax (+44) (0)20-7222-5550; E-mail marketing@bnai.com. In the U.S. call toll-free on: 1-800-727-3116. Subscription price: U.S. and Canada U.S.$925/U.K. and rest of world £550. Additional copies of this publication are available to existing subscribers at half price when they are sent in the same envelope as a standard subscription. Reproduction of this publication by any means, including facsimile transmission, without the express permission of The Bureau of National Affairs, Inc. is prohibited except as follows: 1) Subscribers may reproduce, for local internal distribution only, the highlights, topical summary and table of contents pages unless those pages are sold separately; 2) Subscribers who have registered with the Copyright Clearance Center and who pay the $1.00 per page per copy fee may reproduce portions of this publication, but not entire issues. The Copyright Clearance Center is located at 222 Rosewood Drive., Danvers, Massachusetts (USA) 01923; tel. (508) 750-8400. Permission to reproduce BNA material otherwise may be obtained by calling (202) 452-4471; fax (202) 452-4084. Website: *www.bnai.com* *ISSN 1468-4438*

Editorial Director: **Joel Kolko** ***Editor:*** **Jean Campbell** ***Production Manager:*** **Nitesh Vaghadia**

Correspondents: *Berlin:* David Graber; *Geneva:* Daniel Pruzin; *Manila:* Jason Gutierrez; *New Delhi:* Harbaksh Singh; *Ottawa:* Peter Menyasz; *Paris:* Lawrence Speer; *Rome:* Eric Lyman; *Tokyo:* Toshio Aritake

News From Around the World

ARGENTINA

Supreme Court Demands Anti-Hacking Legislation

BUENOS AIRES—Argentina's Supreme Court has formally asked the Justice Ministry to sponsor anti-hacking legislation in Congress after its own website was vandalized and a federal judge acquitted the intruders saying there was no law punishing cyber attacks (see *WILR*, 3:5, p. 15).

The top tribunal requested the government May 7, 2002 to "promote the necessary legislation to penalize conduct such as the one that has been investigated, since the absence of an explicit legal framework led the case to end in an outcome that was harmful for the administration of justice."

The court judges were reacting to the March 20 acquittal of all six members of a group calling itself "X-Team," who had been charged with defacing the site in 1998 with suggestions that the Supreme Court was allegedly helping cover up the murder of a journalist.

Resolution 30/02, signed by seven of the nine top tribunal members, pointed out that because of lack of adequate legislation, all defendants were set free by federal judge Sergio Torres despite an exhaustive probe into Argentina's first major hacker case. Expressing concern over such "grave circumstances," the seven-paragraph resolution stressed the "need to let the agencies that may be concerned know about these facts so steps can be taken to prevent this kind of situation."

Website Not Covered by Law, Ruled Judge

Judge Torres ruled that hacking the Supreme Court website was not a crime because the law only protects persons, animals and material things. "A website cannot be included under the concept of 'thing'," he said in his 5,300-word ruling. "This is so because given its nature it is not a corporeal object, neither can it be detected materially." He went on to say that there was clearly a legal void in Argentina's legislation, and cited examples of Bills presented by legislators to give specific protection to electronic data. Before being hit by the worst economic crisis in its history, Argentina was one of the Internet pioneers in Latin America.

The prosecution did not appeal the acquittal, conceding that there is no law in Argentina specifically punishing hacking. In a recent interview with *WILR*, federal prosecutor Jorge Alvarez Berlanda said that from a legal standpoint the judge's decision was "impeccable." He added that Intellectual Property Law 11723 was recently amended to protect software, but websites were not expressly mentioned and Argentina's law bans the use of analogies. To be shielded, a website needs to be specifically mentioned, Alvarez Berlanda said.

Judgment Widely Criticized

But many experts criticized the ruling. Martin Caneque, a lawyer specializing in Internet legislation, told *WILR* that although new laws would be welcome, the existing set of rules could have sufficed to take legal action against the defendants had Judge Torres had the inclination to do so. "Among other things, there was invasion of and damage caused to public property—that is clearly a crime," he said of the January, 1998 hacking of the top court website to mark the first anniversary of the brutal murder of photojournalist Jose Luis Cabezas.

Juan Carlos Tirante, a former police chief specialized in electronic data criminology who teaches Information Safety at the Universidad Tecnologica Nacional, agrees. "Information is protected by many existing laws," he told *WILR*. "Sure, we need new, flexible laws targeting hacking, but there are other current rules that could have been used in this case."

Caneque believes that part of the problem was that Argentine judges in general are way out of touch with the latest technology developments. "I've attended 95 percent of all the courses and seminars on information technology legislation and I think I met there only one judge, once. This is very serious," he said.

He, and other experts who asked not to be identified, suspect that the fact that all nine members of the Supreme Court are facing impeachment on several counts of graft, alleged misconduct and political bias could have played a significant role in the acquittal of their aggressors. "It was an attack on the Supreme Court, so the judge decided to look the other way," Caneque said.

Background

The X-Team posted in the court's website pictures of Cabezas and a banner demanding the case be solved, along with suggestions that the top tribunal was involved in a cover-up of the murder. Cabezas was found dead and his body charred during a 1997 probe into Alfredo Yabran, a business tycoon who was under investigation for his alleged association with organized crime. Yabran later committed suicide after a judge ordered his arrest.

Yabran also had links to then-President Carlos Menem, currently under investigation for alleged misconduct; most Supreme Court members have been accused of having a pro-Menem bias.

The Cabezas case has become a symbol for groups and individuals accusing top Argentine officials of covering up human rights abuses and other offences.

The day after the cyber attack Supreme Court President Julio Nazareno presented legal charges against the unknown hackers, triggering a protracted investigation. The police and intelligence service agents interviewed informers, tapped suspects' telephone lines and the

on-line chat system ICQ, and questioned journalists who had interviewed some of the X-Team members for stories about the hacking. It eventually identified all six members —five men and one woman, all in their twenties, and arrested them. A number of raids on their homes and offices led to the confiscation of several computers and floppy and compact disks. But in the end Judge Torres acquitted them all.

AUSTRALIA

Survey Finds Computer Crime On The Rise

The *2002 Australian Computer Crime and Security Survey,* released May 20, 2002, shows the level of computer crime in Australia now exceeds that in the United States. Of organizations surveyed, 67 percent have been attacked in 2002—twice the 1999 level—and 35 percent of these organizations experienced six or more incidents.

Jointly produced by Deloitte Touche Tohmatsu, AusCERT and the N.S.W. Police, the survey across Australia's top 300 companies and other public and private sector organizations details the growing extent and nature of computer security incidents in Australia and enables comparison with the U.S. findings in the 2002 Computer Security Institute/FBI *Computer Crime and Security Survey.*

Deloitte's Head of IT Security Consulting, Dean Kingsley, said that the *2002 Survey* shows computer security incidents are not only growing rapidly in number but the source and nature of the attacks is changing:

"Employees continue to represent a significant source of attack (with 50 percent of companies reporting security breaches being attacked from within). However with the increase in e-business and networking between businesses, external attack is now for the first time the greatest threat (affecting 87 percent of companies reporting security breaches).

"Also alarming is the rapid increase in financial loss experienced. Although organizations find it difficult to estimate the broader financial losses associated with computer security incidents it is clear computer crime is no longer just nuisance value, but a serious threat to customer relationships and ultimately bottom-line profitability.

"While 70 percent of organizations surveyed increased their spending on IT security last year they continued to experience an increase in computer security incidents, with 60 percent stating that changing user attitudes to computer security is the biggest barrier to incident prevention."

Graham Ingram, General Manager of AusCERT, Australia's national computer security incident response team based at the University of Queensland, said 56 percent of organizations surveyed acknowledged that keeping up to date with threat and vulnerability information presented real difficulties and challenges. "Organizations are struggling to deal with what are critical and complex issues in an environment which is rapidly changing," he said. "The trends reported in this Survey are consistent with those observed by AusCERT which show that the number of organizations reporting computer security incidents and seeking response advice is growing. It is unlikely that the underlying trends will improve next year, which means organizations will need to work harder just to maintain the *status quo*."

Detective Superintendent Megan McGowan, Head of the N.S.W. Police Computer Crime Unit, said 61 percent of organizations surveyed took no legal action whatsoever following computer attack. However, they need to realise that what may appear to be benign is often the pathway to something more sinister:

"With the recent strengthening of the N.S.W. Crime Act, police can now prosecute hackers for simply entering a company's computer system and there is no need to prove a further offence has taken place. Hackers now face penalties of up to ten years' imprisonment. The N.S.W. Computer Crime Unit is working with dedicated investigation teams around Australia and internationally with agencies such as the FBI, to exchange intelligence and crack down on what is a growing problem; however, organizations need to report incidents if this community problem is to addressed effectively."

Other survey findings:

- 98 percent of companies had experienced either computer security incidents/crime or some other form of computer abuse (such as network scanning, theft of laptops or employee abuse of Internet access or e-mail).
- The areas of greatest financial impact were data or network sabotage, virus and trojan infection, computer fraud and laptop theft.
- Areas of lower financial loss but frequent incident were denial of service attacks and network scanning.
- After changing user attitudes, other most-cited barriers to improving security were management of software upgrades and bug patches.
- 43 percent of Australian organizations surveyed are willing to hire ex-hackers to deal with security issues, three times more than in the U.S.

The full survey results are available at *www.auscert.org.au/Information/Auscert_info/2002cs.pdf.*

EUROPEAN UNION

New Regulation Relating To *.eu* TLD

By Stéphan Le Goueff of LE_GOUEFF@vocats.com, extracted from "the l.i.n.k." (a free monthly electronic newsletter on Information Society legal issues edited by LE.GOUEFF@vocats.com. To subscribe mail to contact@thelink.lu with "subscribe" in the subject box).

European Community Regulation No 733/2002 of April 22, 2002 on the implementation of the ***.eu***

top-level domain ("TLD") was published in the *Official Journal* in April 2002 (the "Regulation"). (See *WILR*, 3:5, p. 4.)

The creation of the ***.eu*** top-level domain aims to accelerate electronic commerce in the e-Europe initiative. It should indeed promote the use of the Internet networks and the virtual market-place based on the Internet by providing a complementary domain to existing country code top-level domains ("ccTLDs") and generic top-level domains ("gTLDs"). Thus, choice and competition should be widest.

The objective of the Regulation is to establish the conditions of implementation of the ***.eu*** TLD, to provide for the designation of a Registry (entity which organises, administers and manages domain names; this includes notably maintenance of the corresponding databases and the associated public query services).

The Commission shall enter into a contract with the Registry which shall specify the conditions according to which the Commission supervises the organization, administration and management of the ***.eu*** TLD by the Registry. The contract between the Commission and the Registry shall be limited in time and renewable. The Registry, which shall be a non-profit organization, may not accept registrations until the registration policy is in place.

The Commission shall submit a report to the European Parliament and the Council on the implementation, effectiveness and functioning of the ***.eu*** TLD one year after the adoption of the Regulation and thereafter every two years.

The text of the regulation is available at *http://europa.eu.int/eur-ex/en/dat/2002/l_113/l_11320020430en00010005.pdf.*

EUROPEAN UNION

Parliament OKs Plan to Require Data Retention, "Opt-in" for Commercial E-mail

BRUSSELS—Reversing an earlier stance on Internet privacy, the European Parliament May 30, 2002 approved a legislative draft requiring service providers and telephone companies to retain traffic data for possible scrutiny by law enforcement agencies.

Voting on a directive drafted by the executive European Commission, deputies agreed by 351–133 to approve a series of amendments negotiated behind closed doors by leaders of the Parliament's two dominant parties and the Spanish government, current holders of the rotating presidency of the E.U.

Approval of the "compromise amendments" is likely to cut short legislative procedures. If the deal is also accepted by the E.U. Council of Ministers, representing the 15 E.U. member states, ministers will be free to sign the draft into law without further formality.

Previously, the main disagreements about the draft had involved issues of unsolicited telephone sales calls, faxes, and e-mails. As a measure against "spamming," the revised draft will introduce an E.U.-wide "opt-in" requirement for commercial e-mails—an idea ridiculed by British Socialist Bill Cashman. He argued that "an opting-in system will not stop one iota of spam because spammers operate offshore."

On the use of "cookies," the compromise requires that users should receive "clear and comprehensive information" on the purposes of cookies in advance, enabling users to refuse them.

Commissioner Erkki Liikanen, responsible for E.U. "information society" affairs, said he was prepared to accept the deal agreed between the Parliament and the Spanish presidency, which he said involved "sound and balanced solutions."

Draft Questioned on Constitutional Grounds

Last-minute protests by Internet companies, civil liberties organizations, and the Parliament's own Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (CFRJHA) failed to influence the plenary vote.

"In my own company, we only maintain log files only for billing purposes," said Sjoera Nas, public affairs officer for Dutch ISP XS4ALL. "This legislation will cause tremendous problems if we have to store data on individuals' web-surfing. The cost of the exercise is unquantifiable at this stage, but it's likely to be heavy."

Opponents of the Bill among the Parliament's minority parties questioned the revised draft on constitutional grounds. British Liberal Baroness Sarah Ludford complained: "This proposal began life as an attempt to secure alignment of national telecoms legislation, as part of a move to free up E.U. markets. But now it deals with fundamental issues of human rights and civil liberties…[and would] confer broad powers requiring telcos to keep records mapping people's lives, their movements, and contacts."

She viewed the measure as "dangerous and premature and of doubtful legality, as a criminal justice add-on to what is supposed to be a trade liberalization measure," adding: "There is a case for creating powers to investigate serious organized crime and terrorism, but this draft goes far beyond that by appearing to allow even proactive searches for evidence."

Dutch Liberal Elly Plooij-van Gorsel pointed out: "Many European governments do not have these powers in national law. Ministers are trying to secure at E.U. level powers they would not be able to get from their own electorates."

On the eve of the May 30 vote, debate on the draft was relegated to a midnight session, with no more than five deputies present. They did not include senior figures from either the Christian Democrat-led European People's Party or the Socialists, who together account for 411 of the Parliament's 625 serving members, and who negotiated the deal with the Spanish government.

Telco Records, Proof of Identity

Elsewhere, the legislation will require telephone companies to keep records of telephone calls and may even require mobile phone users to present proof of identity when they buy "refill" payment cards, according to Italian legislator Marco Cappato who has been acting as point man on the draft for the CFRJHA.

Cappato saw his recommendations, heavily backed by the all-party CFRJHA, rejected in the plenary vote on a measure originally touted as a measure to protect Internet privacy and to boost confidence in e-commerce (*European Parliament and Council Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector,* Commission document COM [2000] 385). Cappato claimed that concerns about terrorism were being exploited by ministers who wanted to give their security forces "*carte blanche* to mount investigations, with no proper justification or explanation." He said: "It appears that lack of data was not the problem in failing to avert the events of September 11, but a failure to interpret the information that was available."

Data Retention Compromise

On data retention, the compromise draft said states may ease data privacy in order to conduct criminal investigations or safeguard national or public security, when this is a "necessary, appropriate and proportionate measure within a democratic society." For the retention of data "for a limited period" states are free to adopt legislative measures, which must be in accordance with the general principles of E.U. law. Interceptions should also be in accordance with the European Convention of Human Rights and with the rulings of the European Court of Human Rights.

The legislation will be reviewed when it has been in force for three years.

EUROPEAN UNION

Draft Directive On Distance Selling Of Financial Services

By Stéphan Le Goueff of LE_GOUEFF@vocats.com, *extracted from "the l.i.n.k." (a free monthly electronic newsletter on Information Society legal issues edited by* LE.GOUEFF@vocats.com. *To subscribe mail to contact@thelink.lu with "subscribe" in the subject box).*

Following extensive discussions between the member states during the past three years, the European Parliament finally adopted in May the proposed directive concerning the distance selling of financial services (the "Proposed Directive").

The text finally approved by the Parliament follows a broader directive adopted in 1997, which currently covers all products and services except financial services.

The purpose of the Proposed Directive is to enhance cross-border sales of financial services while ensuring adequate protection of consumers' interests. To this end, the text adopted by the Parliament foresees, *inter alia*:

- an obligation on the supplier to disclose to consumers a complete list of information prior to conclusion of the contract. The objective is, on the one hand, to draw up a list of information items which have added value in the context of distance contracts and, on the other hand, to bring this list into line with existing rules regarding other sectorial directives (non-life insurance, life insurance, UCITS, prospectus, and investment services). In this respect, it should also be noted that the text provides that member states have the option of maintaining or introducing more stringent consumer protection rules with regard to that information;
- an obligation on the supplier to communicate the contractual terms and conditions. The text provides indeed that the contractual terms and conditions, and a summary thereof including the pre-contractual information, must be communicated in writing or on a durable medium before conclusion of the contract; and
- the implementation of a right of withdrawal. Thus, the text establishes a general right of withdrawal. The period during which the consumer may withdraw will, in normal circumstances, be from 14 to 30 days, in the case of life insurance and personal pensions.

The Proposed Directive is due to be approved at the next Council meeting before entering into force.

The full text in English of the Proposed Directive can be accessed at *wwwdb.europarl.eu.int/oeil/oeil_ViewDNL.ProcViewCTX?lang=2&procid=3044&HighlighType=1&Highlight_Text=financial%7B_SPACE_%7Dservices*.

FRANCE

ADSL Taking Off, Says Telecoms Regulator

PARIS—The use of high-debit Internet access sky-rocketed in France during 2001, but a regulatory lapses saw nearly all new clients picked up by former monopoly France Telecom, according to a new report on the development of the Internet published by the top telecommunications regulator June 3, 2002.

The number of high-debit Internet users in France tripled during 2001, from 200,000 to 600,000 of the country's estimated seven million Internet users, according to the new report from the French Telecommunications Regulatory Authority (Autorité de Régulation des Télécommunications, ART).

While the cable market doubled in 2001, from 100,000 to 200,000 clients, most of last year's growth in high-debit access came from the ADSL sector, which rose from 70,000 to 400,000 clients, more than 90 percent of whom are registered with France Telecom, ART

said. ART welcomed the growth, but noted that the penetration rate would be "much higher" if "alternative ISPs had the means to really compete with (France Telecom-owned) Wanadoo."

ART admitted that France Telecom's lockhold on the ADSL market ran counter to its objectives of ensuring efficient and competitively-priced markets that offer consumers choice and service innovation.

The annual report noted that consumer prices for household ADSL access are currently hovering around EUROS 45 ($42) per month, which is near the European average, but still too high. The regulator admitted that "there is no question that prices should continue going down, but only under conditions that will allow operators to cover their costs," ART said.

In the overall Internet access market, ART noted that France's 30 percent household penetration rate was in the lower third of the European market, alongside that of Latin neighbours Italy and Spain, but below that registered by northern neighbours Belgium, Germany and the United Kingdom, where household penetration hovers around the European Union average of 38 percent, and far behind the 60 percent rates seen in the Netherlands or the Scandinavian countries.

ART cites a number of factors to explain the slow uptake of household Internet penetration in France, from the low levels of household computer use to the country's failure to deregulate local telephony and confusing and unsatisfactory pricing levels established for ISPs wishing to offer clients all-inclusive telecom and Internet access packages. It insists that if 2001 was the year of ADSL uptake, 2002 should be the year that competition takes off for ADSL services.

The new ART report on Internet Development in France during 2001 is available, in French, at *www.art-telecom.fr*.

FRANCE

Government Investigates On-line Gambling

PARIS—French government officials have begun investigating on-line gambling sites located in foreign jurisdictions as part of wider plans to overhaul antiquated betting laws and crack down on Internet casino operations aimed at French punters.

Magistrates from Paris area courts opened investigations in May 2002 into a U.S.-based site—*www.kipari.com*, which is French slang for "*Who's Betting?.com*"—that advertises its sports betting and casino games on popular French-language Internet sites in a non-camouflaged bid to attract French bettors.

Complaints against kipari.com, which is based in New Jersey and owned by a group of French entrepreneurs, allege that it is intentionally competing with government-operated gambling operations, such as lottery company "la Française des Jeux" or off-track betting specialist PMU, and thus in violation of French law. Kipari.com co-founder Franck Delmas does not deny that his site seeks out French gamblers, but he has noted in a series of interviews with the local press that the operation is a U.S. company, covered by American law, and thus outside the reach of French magistrates or laws.

A report published in early 2002 by French Senator Francois Trucy seems to back up Delmas' contention. "French law outlaws by definition all Internet casinos and any implantation of website servers on the national territory," according to the report, titled *Games of Change and Money in France: The State as Croupier, The Parliament's Irrelevance?*

"Yet the law is incapable of penalising French gamblers who bet on-line, as are the applicable laws in most other countries," said the report, published March 20.

"A Legal Limbo"

Senator Trucy says that the current legal limbo "hurts everyone involved," noting that the government loses revenues to non-licensed gambling operations, licensed French casino operators are prevented from competing in a new sector of activity, and gamblers are left to fend for themselves in a totally unregulated environment deeply penetrated by organized crime.

Executives at leading Internet advertising placement services have been walking a tightrope through this legal limbo for years, with many unable to resist the temptation posed by cash-heavy ad buyers from offshore betting sites. Some, like France Telecom-owned Wanadoo Regies or the French office of U.S.-based DoubleClick, have recently opted to ban casino ads until the regulatory situation becomes clear, while others, like HiMedia, have admitted the legal "fuzziness" of accepting gambling ads while continuing to place them across the French-language Web.

Patrick Partouche, general manager of Groupe Partouche SA, France's largest casino operator, joined the fray in late May by going public over his firm's ill-fated efforts to license a foreign national to manage an on-line casino under its brand from the tiny Central American nation of Belize. Interior Ministry officials quickly called on Groupe Partouche to close the site in question—*www.casino-partouche.com*—noting that it fell foul of national gambling laws.

Partouche says that the French regulatory framework—two laws dating to 1983 and 1836—is in need of a complete overhaul, taking into account the borderless development of the Internet and the reality of more than 1,400 on-line casinos now accessible from France. He hopes to jump-start the process—and eventually open the Web to his firm's offerings later this year, with the publication of a White Paper on on-line gambling.

The White Paper, to be drafted after meetings with officials from the Interior Ministry's betting division, representatives of the customs department, the legal profession, and licensed casino operators, will call for full legalization of Internet gambling, to be accompanied by tight operating rules and stiff transparency standards.

The French Senate report into on-line gambling, *Les jeux de hasard et d'argent en France: l'État croupier, le Parlement croupion?* ("Games of Change and Money in France: The State as Croupier, The Parliament's Irrelevance?") may be consulted, in French, at *www.senat.fr.*

FRANCE

ISP Refuses to Keep Logs on Internet Users

PARIS—Outraged over privacy-sapping measures included in omnibus anti-terrorism legislation approved by Parliament in late 2001, a French Internet Service Provider has launched a new connection system that eliminates all use of personal data.

The service—*www.no-log.org*—was launched in April by GlobeNet, a user-based ISP that groups more than 200 progressive NGOs, and has already recruited more than 1,500 Internet users.

GlobeNet officials say their objective in launching the new ISP was to help Internet users protect their privacy in the wake of new action taken in recent months by European authorities and the French government.

The anti-Big Brother ISP was launched in April 2002, as a direct response to Article 29 of the Law on Daily Security (No. 718-01), which obliges ISPs to conserve connection data and user logs for one year and make records available to police and judicial officials upon request.

Passed as part of the immediate reaction to the September 11 terrorist attacks on the United States, the new law—which also allows the government extended powers to eavesdrop in cyberspace—has come under sharp attack from civil liberties advocates and privacy experts.

GlobeNet vowed to fight the law's privacy-sapping provisions, which it claims run counter to France's longstanding privacy protection measures. It launched the *no-log.org* ISP April 7, 2002, advertised as a "privacy protecting" mode of Internet access where "no personal information is required to establish accounts."

The ISP identifies clients through a simple system of "log-ins," passwords and telephone numbers, and refuses to stock any data about users' on-line activity, such as connect time, sites visited, mail sent and/or received, and the IP addresses from which connections emanate.

All connection logs are destroyed daily, making it impossible for GlobeNet to collaborate with law enforcement requests for information on users.

Legal Position Shaky

French Internet sector experts say that GlobeNet is currently "walking a tightrope" between its users' demand for absolute privacy and the new law's requirements for all ISPs. The NGO/ISP will likely be forced to "toe the line" later this year, the experts say, when France's newly elected centre-Right government publishes a series of administrative decrees formalizing the exact nature of ISP responsibility concerning co-operation with law enforcement agencies.

The decrees, which will complement the law initially passed in October 2001, will specify the type of data ISPs must stock, the duration of this data warehousing, and detail compensation law enforcement agencies must pay for use of this data.

GlobeNet has pledged to store the minimum amount of information necessary to avoid legal conflict, "once the rules of the game are clear," and vows that its logs will be encrypted to avoid any uses that could violate client privacy.

In the interim, GlobeNet continues its pro-privacy battle, using its home page to denounce a May 30 European Parliament decision to allow European Union member states wide-ranging rights to eavesdrop on citizens' conversations and Internet activity and store personal data for law enforcement use. *(See p. 5 above.)*

Further information on the pro-privacy ISP run by GlobeNet is available, in French, at *www.no-log.org.*

FRANCE

Electronic Signatures Finally Fully Recognized

PARIS—France has finalized its legal framework for digital signatures with the June 8, 2002 publication in the *Official Journal* of an administrative order establishing a new agency to oversee firms that certify the reliability of electronic signatures.

The French Accreditation Center (Centre Français d'Accréditation, COFRAC) will oversee all entities that seek to evaluate and certify the validity or reliability of electronic signatures and other documents, according to the May 31 administrative order.

COFRAC will ensure that certification agencies abide by the terms of France's electronic signature law (Decree No. 2001-272, March 30, 2001), which states that the certification agencies will guarantee a "presumption of trust" in the use of electronic signatures. COFRAC will also ensure that would-be certification agencies adhere to industry-wide certification norms, use all applicable technological solutions and abide by best practices in electronic certification activities, according to the administrative order.

The administrative order grants COFRAC wide-ranging powers to investigate would-be certification agencies, and allows it to issue operating permits on a two-year renewable basis.

COFRAC—which was born in 1994 as an industry association known as the French Accreditation Committee—will co-ordinate its oversight of certification agencies with that carried out by similar organisms from other European Union member states, according to the administrative order.

LUXEMBOURG

Bill On Electronic Money Institutions Finally Adopted

By Stéphan Le Goueff of LE_GOUEFF@vocats.com, extracted from "the l.i.n.k." (a free monthly electronic newsletter on Information Society legal issues edited by LE.GOUEFF@vocats.com. To subscribe mail to contact@thelink.lu with "subscribe" in the subject box).

On April 17, 2002, the Luxembourg Parliament passed a law aimed at implementing Directive 2000/46/EC o*n electronic money institutions* (hereinafter the "Law").

This Law is intended to promote consumer confidence in the use of e-money by establishing a regulatory framework to ensure the financial stability, integrity and soundness of electronic money institutions (hereafter the "EMIs").

Thus, the approach retained by the Grand-Duchy of Luxembourg consists in regulating EMIs on similar terms as credit institutions, which implies that they will be required—save in certain limited cases—to obtain a licence before being allowed to conduct business. However, in order to make the market more accessible to new players, the Law provides for less burdensome capital requirements for those institutions than for credit institutions.

In order to ensure effective protection of e-money users, the Law foresees, in addition, that EMIs will only be authorized to invest the funds received, in exchange for the issued e-money, in risk-averse and liquid assets. Those establishments will also be obliged to redeem, upon request, the e-money issued without charging excessive commissions.

It should be stressed that EMIs will be entitled to provide closely related financial and non-financial services such as the administering of electronic money by the performance of operational and other ancillary functions related to its issuance, and the issuing and administering of other means of payment but excluding the granting of any form of credit. Those institutions will also be able to offer their services as regards electronic money issuance throughout the European Community in compliance with a mutual recognition regime provided by Directive 2000/12/EC.

The full text in French of this Bill can be accessed at: *www.chd.lu/fr/portail/role/lois/detail.jsp?order=descend&project =13&mode=date&page=1.*

LUXEMBOURG

Legal Protection For Conditional Access Services

By Stéphan Le Goueff of LE_GOUEFF@vocats.com, extracted from "the l.i.n.k." (a free monthly electronic newsletter on Information Society legal issues edited by LE.GOUEFF@vocats.com. To subscribe mail to contact@thelink.lu with "subscribe" in the subject box).

On March 26, 2002, the Luxembourg Government issued a Bill on the legal protection of services based on, or consisting of, conditional access (hereafter the "Bill").

An ever-increasing number of services providers now have recourse to some form of encryption or other conditional access techniques to ensure they receive proper remuneration. However, the market development of pay-TV, video-on-demand, and other conditional access activities is currently threatened by the parallel development of piracy techniques. In order to offer better protection to the services providers against the piracy activities, the Luxembourg authorities have decided to implement locally European Directive 98/84/CE (hereafter the "Directive").

Thus, the Bill defines the activities which, from now on, will be prohibited, and considered under the laws of Luxembourg as constituting a criminal offence. These include:

- the manufacture, import, sale or possession for commercial purposes of illicit devices (including but not limited to decoders and smart cards);
- the installation, maintenance, or replacement of an illicit device; and
- the use of commercial illicit devices.

The Bill, in compliance with the provisions set forth by the Directive, also foresees the possibility for service providers to take appropriate legal action to effectively safeguard their rights. Thus, the service providers whose interests are affected by infringing activities would be entitled to apply for an injunction or claim for damages. Pursuant to the Bill, the district court will, in addition, be competent to decide on the seizure and destruction of illicit devices.

As the legislative process is still at an early stage, the Bill is not expected to be adopted before the beginning of the autumn.

The full text of this Bill, in French, can be accessed at: *www.chd.lu/fr/portail/role/lois/detail.jsp?order=descend&project =0&mode=number&page=1.*

SOUTH KOREA

More E-Commerce Laws Planned

SEOUL—South Korea will add two new laws to an already growing list of e-commerce laws and regulations with the aim of increasing on-line protection of intellectual property rights and boosting the rights of consumers buying on-line.

The Law on On-line Digital Content Industry Development and the Law on Consumer Protection in Electronic Commerce, enacted December 2001 and February 2002 respectively, will take effect in July, giving the government more power to enforce copyright protection and fair trade rules on the Internet.

The digital content law, scheduled for implementation from July 15, prohibits unauthorized duplication and transmission of part or the whole of commercial digital content for the first five years from the date it is published on the Internet, with violations punishable by one year's imprisonment or 20 million won (about $16,000) in fines.

The new law also puts a ban on making, selling or providing in other ways techniques, services or devices for unauthorized commercial duplication or transmission of protected digital content. The law allows the author of infringed content to file a lawsuit seeking an award of damages.

In cases where the existing Copyright Law and the Computer Program Protection Law also apply, their provisions will prevail over those of the new law. "This law is intended to promote the creation of digital content and ensure its orderly distribution on the Internet," said Suh Sung-il, assistant director at the information and communication policy bureau at the Ministry of Information and Communication.

Meanwhile, the E-Commerce Consumer Protection Law, effective from July 1, gives the Fair Trade Commission the power to suspend business and impose fines if e-commerce merchants violate fair trade rules. Refusal to honour cancellation requests, which are valid for seven days from the placing of an order, and false advertising fall into this category of violation. The new law also requires e-commerce business operators to set up insurance to cover repayments or compensations to customers.

Consumers Lack Protection Under Current Laws

According to the FTC, the existing consumer protection provisions under the Law on Door-to-Door Sales are inadequate to bolster the rights of consumers purchasing products on-line. Data published by the E-Commerce Mediation Committee under the Ministry of Commerce, Industry and Energy show that the number of e-commerce consumer complaints filed with the committee jumped to 457 in 2001 from 83 in the previous year. Most complaints were related to shipping, cancellation, privacy, product defects and false advertisements.

SPAIN

Adoption of E-Money Lagging

MADRID—Faced with a growing e-commerce environment and legal uncertainties, Spanish lawyers and legislators are debating whether existing legislation is sufficient to regulate forms of payment in the electronic realm.

Legal experts met near Madrid May 22–23 for Spain's third annual E-Commerce Law Conference. In addition to studying the "electronification" of traditional payment methods such as cheques or bills of exchange, they also took a look at newer methods such as payment with mobile phones or e-money.

"From the legal standpoint, electronic money is fully legal tender" Mariliana Rico Carrillo, a business lawyer specializing in electronic commerce, said. Nonetheless, "while electronic money can guarantee anonymity in transactions, this can also be an inconvenience." Whether through specific software and verification information stored on hard drives or through cards with "rechargeable" chips, e-payment is a growing phenomenon in Europe. E-Cash and Digi-Cash are two well-known systems.

At present, e-money entities are regulated by Directive 2000/46/EC, which defines electronic money, dictates which institutions may be considered electronic money entities and establishes certain requisites. E-money entities, for example, must have a minimum starting capital of one million euros, and 2 percent of the entity's financial obligations must be made up of its own funds. The directive places certain limitations on investments by such firms, and demands "sound and prudent" management.

Mobile Commerce Gaining

While Spain has nearly the lowest Internet penetration rate in Europe—and low levels of electronic commerce—it may nonetheless prove to be at the forefront in establishing integrated mobile commerce. In a country of nearly 40 million, there are 30 million mobile phone users. Of these, 29 million phones using GSM technology are potential users of the universal mobile telephony payments platform Mobipay. The Mobipay system will allow consumers to pay shops, taxis, vending machines, fast food restaurants and other merchants with little more than a mobile phone and a PIN, with purchases linked to credit, debit, or pre-paid cards.

"All operators and all payment methods in Spain have come together," Julián Inza Aldaz of Mobipay said. The new company's shareholders reportedly include all mobile operators, 80 percent of the Spanish financial system and the main payments systems processors, "something that doesn't usually happen in the rest of the world."

Where emerging payment platforms may require new legislation, the electronification of old payment systems may simply require modification of existing legislation. Such is the case with printed cheques, Isabel Ramos Herranz, a business law professor, said. "If the electronic system is more secure than the paper version, why not reinterpret existing law?" she asked.

Ramos suggested reinterpreting Spain's Exchange and Cheque Law (19/1985) to allow for electronic signatures to act as substitutes for handwritten ones. She also advocated a possible modification of the law to adapt to new technologies and to "avoid forced interpretations." At present, Spanish credit institutions electronically send data taken from printed cheques to the National Electronic Compensation System, but the written cheque doesn't disappear, given that it is the

original document. Ramos said this process could be eliminated by directly issuing electronic cheques.

The case of electronic bills of exchange might be somewhat more complicated, said another business law professor, María José Morillas Jarillo. In fact, its very name is misleading, since "it's not a bill, it's not exchangeable and it's not electronic." While data from the original paper document might be transferred, current Spanish law is an obstacle to the creation of an exclusively electronic document. This is mainly because an official stamped document already exists and a signature is required. In Spain, said Morillas, "the law is still stuck with the idea of a handwritten signature."

Spain's Exchange and Cheque Law (19/1985) is available at *http://noticias.juridicas.com*. Directive 2000/46/EC is available at the Europa website, *http://europa.eu.int*.

SPAIN

Legal Experts Debate Whether Anti-Spam Proposal Will Impede E-Commerce

MADRID—While Spain is one of European Union's less wired nations, its current Electronic Commerce Bill attempts to pioneer aggressive legislation governing unsolicited commercial e-mail and other electronic "commercial communications."

Bill 621/000066 on information society services and electronic commerce, drafted by the Ministry of Science and Technology, was approved recently by the Spanish Congress of Deputies and is currently before the Senate. The law is expected to pass, given that the ruling Popular Party enjoys an absolute majority and can enact any legislation it chooses.

The proposed law partially incorporates into Spanish law two directives of the European Parliament and Council. Directive 2000/31/EC of June 8, 2000 (known as the electronic commerce directive) addresses certain legal aspects of information society services, in particular e-commerce, in the Internet Market. Directive 98/27/EC of May 19 deals with injunctions for the protection of consumer interests.

Firm Stand on "Spam"

Title III of the new Bill, which includes Articles 18 through 21, deals specifically with "Commercial Communication by Electronic Means." In a clear prohibition of spam, Article 20 declares unsolicited commercial e-mail illegal. It specifically mentions "advertising or promotional messages by electronic mail or equivalent means of electronic communication." Article 19.1 states that any electronic advertising must begin with the word "advertising" and clearly identify the sender. This is in compliance with Article 6 of Directive 2000/31/EC, which states that "a commercial communication shall be clearly identifiable as such."

Article 21 of the Bill states that when electronic service providers require consumers to list an e-mail address for a contract or subscription—with the intention of sending commercial messages later on—they must inform consumers of their intentions and get their permission before finishing the subscription process. Consumers may at any time revoke their previous consent by notifying the service provider.

"I think that in Spain, the way things are going, we're going to be the first in protecting consumers from spam," said Gema Botana García, professor of civil law and member of the Advertising Self-Regulation Association (*Asociación para la Autorregulación de la Comunicación Comercial*, known as Autocontrol or the AAP). "And I think that's very, very unfortunate, an excess that, rather than protecting consumers, is going to leave consumers without a market in which to consume. To protect consumption, there needs to be consumption," she said.

After Greece, Spain has the second lowest Internet penetration rate in the European Union. In a country where sales by catalogue never had much success, electronic commerce has been a hard sell.

Commercial Communication, Broadly Defined

Current E.U. law defines "commercial communication" as "any form of communication designed to promote, directly or indirectly, the goods, services or image of a company, organization or person pursuing a commercial, industrial or craft activity or exercising a regulated profession."

The European electronic commerce directive nonetheless "flees from the use of the word 'advertising' out of fear that new forms of Internet advertising, as yet unknown, may not be included in the traditional concept of advertising," said Beatriz Patiño Alvés, advertising lawyer and associate professor at the European University of Madrid-European Centre of Higher Studies.

According to Patiño, the directive and the Spanish Bill are very similar, and contain few specific rules with respect to commercial communications. At present, the very definition of commercial communications is broad enough to include Web pages, banners, interstitials, search engines, metanames, nested links, push advertising and other forms of Internet-specific publicity. Government legislation at present, said Patiño, has yet to catch up with the codes of conduct already in place at certain associations. Self-regulation agencies such as the AAP "by way of their codes of conduct, present Internet advertising regulation that is much more exhaustive and detailed," she said.

Directive 2000/31/EC encourages E.U. member nations to draw up codes of conduct, while respecting "the voluntary nature of such codes and possibility for interested parties of deciding freely whether to adhere to such codes."

Patiño and Botana were both participants in the third annual *Electronic Commerce Law Conference*, held near Madrid May 22–23.

The text of Bill 621/000066 is available (in Spanish) at the website of the Congress of Deputies of Spain, *www.congreso.es*. The text of Directives 98/27/EC and 2000/31/EC is available at the website of the European Union, *http://europa.eu.int*.

UNITED KINGDOM

Tightening the E-Purse Strings

By Anna Tweedale, solicitor, IT and E-Commerce, in the Birmingham office of Eversheds (www.eversheds.com); e-mail: annatweedale@eversheds.com

On April 27, 2002, the Financial Services Authority introduced a new regime for the regulation of e-money issuers with the aim of protecting consumers and facilitating innovation in the world of e-commerce. The regime is based on two European directives which have been implemented into U.K. law by the Financial Services and Markets Act 2000 (Regulated Activities) (Amendment) Order 2002. All businesses issuing electronic purses and wallets need to take account of the new regime.

The new regime is set out in a specialist sourcebook, the *Electronic Money Sourcebook Instrument 2002*. Its introduction followed a consultation period during which the FSA received responses from a range of potential e-money issuers, including banks, mobile phone operators and the Electronic Money Association. Generally, the e-money industry welcomes the new regime.

What Is E-Money?

For the purposes of the FSA's new regime, e-money is cash value stored on an electronic device such as a mobile phone, PC or smartcard, which is accepted as a means of payment by persons other than the issuer. E-money could be downloaded from an ATM or shop-based terminal or from the Internet. Potentially, e-money could be used to buy goods and services, or it could be redeemed for physical cash or it could be exchanged from person to person.

E-purses offer e-money issuers a means of tapping into the spending power of consumers who previously would have only used cash, for example, teenagers using prepaid mobile phones. E-purses offer the consumer an alternative means of payment in low-value transactions, for example on public transport or in car parks.

The FSA has set the limit on e-purses at £1,000 to protect holders of e-money by restricting their individual loss should they lose the e-purse or the issuer become insolvent. This is especially important as the Government has decided that the Financial Services Compensation Scheme will not apply to e-money issuers, which means that consumers will have no access to compensation should an issuer become insolvent.

The key characteristics of the FSA's new regime are:

(i) FSA authorization: Firms must apply to the FSA for permission to issue e-money and meet certain threshold conditions relating to matters such as resources and suitability. They will also have to meet ongoing supervisory requirements of the FSA. Periodic fees and an application fee will be payable to the FSA.

(ii) Restriction on business activities: Non-bank or building society e-money issuers will be prohibited from undertaking activities that are not closely related to the issue of e-money. In particular, they may not make any loan or grant any form of credit nor pay interest on the e-money. This effectively "ringfences" the e-money activity.

(iii) Restrictions on investments: Funds held in exchange for the issue of e-money must be invested in high quality liquid assets.

(iv) Minimum capital requirement: E-money issuers will be required to maintain minimum levels of capital. The initial threshold is one million euros and, once authorized, the issuers' funds must be equal to or above 2 percent of the higher of its current amount, or the average of its preceding six months' total amounts, of outstanding e-money.

(v) Resistance and controls: E-money issuers must have sound and prudent systems and adequate internal control mechanisms and must comply with the FSA's money-laundering requirements.

(vi) Discounts: E-money issuers may issue e-money at a discount for marketing purposes in certain tightly controlled circumstances.

The FSA is empowered to grant waivers from the regulations to small or locally-based firms, although they will still have to submit periodic information about their businesses.

Businesses already issuing e-money on April 27, 2002 will enjoy a six months' "grandfathering" period until October 27, 2002 during which they will be presumed authorized. If they have not secured the necessary FSA authorizations or waivers by then, they will lose their ability to issue e-money legally.

The effect of the new regime is likely to be that it will lead to greater consumer confidence in e-money, encouraging more consumers to take it up and more retailers to accept it.

UNITED KINGDOM

Distance Selling and Delivery Charges

By Suzanne Mercer, a partner in the London office of Eversheds (www.eversheds.com); e-mail: suzannemercer@eversheds.com

Amazon.co.uk and BOL.com have bowed to pressure from the Office of Fair Trading to refund delivery charges in addition to the price when customers return goods within the legal cooling-off period.

The Distance Selling Regulations apply to contracts for the sale of goods or services to consumers by mail order, over the Internet, by telephone, or by fax. They give consumers a "cooling-off" period of seven working

days after receipt on most goods, during this period consumers can withdraw from the contract. The OFT's view is that the normal postage and packing charges for the delivery, but not the return, of distance sales purchases must always be refunded in addition to the cost of the goods when orders are cancelled during the cooling-off period.

Suppliers remain entitled to charge for the cost of return of rejected goods provided that the contract states that the consumer is obliged to return the goods to the supplier.

The OFT is in negotiation with a number of other companies under the Distance Selling Regulations regarding the refunding of delivery charges. This approach is in line with the Regulations and suppliers should check that their contracts provide for the refund of standard delivery charges.

UNITED STATES

New DoJ Rules Allow FBI Greater Use of Web

Civil libertarians blasted new guidelines released May 30, 2002 by the Justice Department for FBI investigations that would expand the ability of agents to use the Web and data mining to probe for terrorist activities, as well as visit churches and other public places regardless of whether there is reason to suspect criminal activity.

In the wake of the September 11 terrorist attacks, Attorney General John Ashcroft said the new rules—the greatest overhaul of the guidelines since their creation in the 1970s—were necessary to enhance the FBI's ability to prevent future terrorist attacks.

The new guidelines would provide the FBI with authority to do on-line research or use a commercial data mining service for counter-terrorism purposes regardless of whether it is conducting a specific investigation, a requirement for such activities under the old rules. In addition, it would allow FBI agents to visit public places—including churches, mosques or libraries—as part of the agency's efforts to try to detect or prevent terrorist activities, Ashcroft said. FBI agents lacked clear authority for such activities under the old guidelines. "In many instances, the guidelines bar FBI field agents from taking the initiative to detect and prevent future terrorist attacks," Ashcroft said during a news conference with FBI Director Robert Mueller to announce the changes. "The FBI can't surf the Web in the same way you and I can to look for information. Nor can FBI investigators simply walk into a public event or public place to observe ongoing activities...These restrictions are a competitive advantage for terrorists who skilfully utilize sophisticated techniques and modern computer systems to compile information for targeting and attacking innocent Americans." The changes come one day after the FBI announced a major shift of the agency's mission toward a greater emphasis on preventing terrorist attacks.

The new guidelines, which went into effect immediately, also will enhance the ability of FBI field agents to act without gaining prior approval from FBI headquarters in Washington.

In addition, Ashcroft extended the amount of time that the FBI would have to conduct preliminary inquiries, which are based on an allegation but may not be include any "reasonable indication" of criminal activities, from 90 days to up to a year. Under these preliminary inquiries, FBI agents are allowed to use all legal investigative techniques except mail openings and wiretaps.

"The guidelines will help remove bureaucratic obstacles" to preventing and detecting terrorism, Mueller said.

Civil Libertarians Alarmed

But civil libertarian groups and others voiced strong concerns about the new rules.

The new rules allowing greater use of the Web apply to more than just counter-terrorism and could be extended to all other investigations, said Jim Dempsey, deputy director of the Center for Democracy and Technology. In response to Ashcroft's contention that the new rules would do little more than allow the FBI to use data mining and other information-gathering services available to businesses, Dempsey argued that the difference is that "marketers (use the information) to just send spam...They (the FBI) can arrest you."

Laura Murphy, director of the American Civil Liberties Union's Washington National Office, said the Bush administration was "rewarding failure" instead of investigating why the FBI was unable to prevent the September 11 terrorist attacks.

The ACLU also expressed concern that the new FBI powers might lead to some of the excesses that prompted the issuance of the guidelines in the first place such as the collection of files and information on civil rights leader Martin Luther King Jr. and other political figures. But Ashcroft insisted that FBI agents would be prevented from abusing this new authority by current laws and constitutional restrictions. In addition, he said the new rules include restrictions that would prevent such domestic spying.

"The abuses that once have been alleged about the FBI decades ago about keeping files or records about prominent figures in this country would not be allowed under the guidelines or under statutes regarding privacy incorporated into the guidelines," he said. President Bush said he supports Ashcroft's changes and said the FBI's recent performance shows that the "organization didn't meet the times."

EPIC to Seek Congressional Hearings

"Our most important job is to protect America. And the initiative that the attorney general [outlined] will guarantee our Constitution, and that's important for the citizens to know," Bush told reporters.

Still, Marc Rotenberg, executive director of the Electronic Privacy Information Center, said his group and others plan to call on Congress to conduct hearings into whether the Justice Department has the legal authority to grant the FBI the new powers. "There has to be congressional oversight," he said. There are "real constitutional problems with transforming the FBI into a domestic spying agency."

UNITED STATES

New Regulation Sets Forth Standards for Banks' Electronic Services

Effective June 17, 2002 financial institutions have the green light to engage in a broad range of electronic commerce activities, including participation in on-line "malls" by a final rule issued by the Office of the Comptroller of the Currency May 17 (6 Fed. Reg. 34,992, 5/17/02) following a rulemaking process lasting about two years. The OCC guidelines also set out a test for determining when federal regulation of banking pre-empts states' attempts to regulate on-line activity.

The issuing of the new regulation, while it might be largely considered a restatement of existing doctrine on banking regulation, is important, according to one practitioner in the field, because "it really does make it very clear, maybe to a level not understood before, that banks have very broad authority to conduct business electronically." The new final regulation on electronic activities, most of which became effective June 17 and is codified at 12 C.F.R. Part 7, Subpart E, includes provisions on banks' acting as "finders" for buyers and sellers and selling access to excess electronic capacity. Banks' acting as digital certification authorities is specifically authorized by the rule. Additionally, the regulation offers standards regarding how to determine whether banks are permitted to engage in some new electronic activity.

Garnering Previous Policy Statements

The new regulation is largely an attempt by the agency to tie together in one place a series of principles that have been developing over the years in separate proceedings, P. Michael Nugent Jr., an electronic commerce and banking lawyer with Heller, Ehrman, White & McAuliffe, New York, told *WILR:* "What the OCC had been doing over the years is issuing opinions and interpretations of the regulation that was in place at the time. What developed was a patchwork quilt of opinions and interpretations.This regulation puts all the thinking and the theory into a new regulation format and cleans up and clarifies what had been a number of opinions that had grown over the years." This articulation of the OCC's goals was echoed by the official under whose authority they were issued. The OCC has been aware over the years of the growing importance of the development of the electronic environment, Julie L. Williams, the OCC's chief counsel and first senior deputy comptroller, told *WILR*.

"We've received a fair number of questions regarding whether banks are permitted to engage in certain types of activities and we decided it would be desirable to pull together all the thinking on the authority of national banks" to engage in new activities, Williams said. "There were questions that were consistently coming up about whether certain activities were permissible or not and we wanted to get ahead of the questions by providing a lot of information about what we think is permissible."

Future Developments Anticipated

To a large extent, Nugent said, the OCC is following the lead of the Board of Governors of the Federal Reserve, but it amounts to a message that national banks have broad authority to conduct economic, financial, and banking activities in an electronic environment. Furthermore, this regulation might become a platform for future expansion of the kinds of activities federally regulated financial institutions are authorized to engage in.

The regulation should be an aid to banks in determining going forward whether new activities that have not yet become known to the industry or to regulators are permitted, Williams said. This guidance is set forth in §7.5001 of the regulation, which sets forth four considerations designed to determine whether the OCC will consider an electronic activity to be "part of, or incidental to, the business of banking":

"(i) Whether the activity is the functional equivalent to, or a logical outgrowth of, a recognized banking activity;

(ii) Whether the activity strengthens the bank by benefiting its customers or its business;

(iii) Whether the activity involves risks similar in nature to those already assumed by banks; and

(iv) Whether the activity is authorized for state-chartered banks" (12 C.F.R. §7.5001(c)).

The section additionally requires that the OCC ensure that the activities in question are "subject to standards or conditions designed to provide that the activities function as intended and are conducted safely and soundly, in accordance with other applicable statutes, regulations, or supervisory policies."

"Our basic thinking is that this ought to be viewed by financial institutions as a constructive set of standards for them going forward in engaging in electronic activities, not limited to the Internet," Williams said.

Participation in On-line Malls Permitted

There is one portion of the rule that offers a standard on an area that has not been addressed explicitly before, Nugent said. This provision, §7.5010, has to do with "shared electronic space," situations in which banks are co-operating with other businesses in an electronic presentation, such as an Internet mall.

In such cases, the regulation said, [n]ational banks that share electronic space, including a co-branded website ... must take reasonable steps to clearly, conspicuously and understandably distinguish between products and services offered by the bank and those offered by" the other parties involved.

Pre-emption, Jurisdiction Issues Addressed

The rule also sets forth in §7.5002(c) the OCC's views on federal pre-emption of state regulation of banking activities on the Internet as well as jurisdictional issues.

The first principle arising from the OCC's pre-emption statement is that OCC rules pre-empt any state regulation if the state's action acts as an obstacle to a bank's exercising of powers granted under federal authority.

With regard to jurisdiction, the OCC took the position in §7.5008 that a finding that a national bank—that is, one chartered and regulated under federal authority—is located in a particular jurisdiction may not be based solely on the existence of "an electronic point of presence," such as an Internet server or an automated teller machine. Additionally, under §7.5009, if a bank is operating as an "Internet bank," then its "home state" for purposes of banking regulations is the state under whose laws the company is organized. This is an issue when, for example, determining exporting interest rates for credit cards.

Certification Issue Arises from Proceedings

The agency also had another reason for embarking on the rulemaking proceeding, Williams said. The OCC wanted input from the banking industry regarding "whether there were aspects of current regulations that were acting as impediments to the ability of banks to engage in electronic activities or issues where it would be helpful for banks to have more regulation, in the context of helping to define whether an activity is allowable or not."

This aspect of the proceeding bore fruit in the final rule's provision, §7.5005, stating that national banks are permitted to act as certification authorities and issue digital certificates. This provision "goes beyond" the agency's previous position, Williams said, because it does not merely authorize banks to engage in identifying parties:

"A national bank may issue digital certificates verifying attributes in addition to identity of persons associated with a particular public/private key pair where the attribute is one for which verification is part of or incidental to the business of banking. For example, national banks may issue digital certificates verifying certain financial attributes of a customer as one of the current or a previous date, such as account balance as of a particular date, lines of credit as of a particular date, past financial performance of the customer, and verification of customer relationship with the bank as of a particular date," 12 C.F.R. §7.5005(b).

"Finder" Authority Modified

Section 7.1002 of the regulation, which is not part of the new Subpart E, has been modified in order to address the electronic applications of banks' authority to act as "finders," in the manner of classified advertisements or other forms of "bringing together interested parties to a transaction."

There are some new activities enumerated related to acting as a finder through electronic means that were not explicitly authorized previously by the OCC, although they might already have been approved by the Board of Governors of the Federal Reserve, according to Williams. The approved activities in this section include communicating with buyers and sellers regarding available goods and services and their prices and terms, processing of communications exchanged and keeping of records in such transactions, and arranging for discounts for bank customers. Banks are not necessarily limited to the finder activities enumerated in the regulation, though, according to Williams. "Although we have listed lots of examples of finder activities or other permissible electronic activities, all of the illustrations are just examples. They're not exclusive," she said. "It just means that a bank would have to ask us on a case-by-case basis if they don't see an activity listed in the regulation."

Traditional Services Analogized

Many of these activities, of course, are electronic analogies of activities banks already engage in. For example, Williams compared digital certification authority to notary services and finder services to flyers and advertisements for goods and services included with bank statements. Along these lines, §7.5002 addresses the "furnishing of products and services by electronic means and facilities," which authorizes, among other things, the establishment of websites on behalf of merchants, hyperlinking to third-party sites, hosting an "electronic marketplace," providing electronic bill presentment services, offering electronic stored value systems, and offering services for "safekeeping for personal information or valuable confidential trade or business information, such as encryption keys."

Excess Capacity Must Be Legitimately Acquired

Finally, the regulation sets forth in §7.5004 standards for banks' selling "excess electronic capacity" to third

parties. The list of such electronic capacity includes data processing services, Internet access, electronic security system support services, and electronic imaging and storing. The key to this provision, Williams said, was §7.5004(d), which states that the bank may sell such capacity only if it was acquired for the purpose of conducting an authorized banking activity. The excess might be present either because the service in question is periodic and demand for capacity fluctuates, or because the bank is anticipating future needs, she said.

"If they've got down time then they can use it for other things, but they don't have general authority to go out and buy computers to process any kind of data," Williams said.

The text of the Office of the Comptroller of the Currency's final rule on electronic activities of banks and supplemental information from the Federal Register is available at the OCC's website, *www.occ.treas.gov/fr/fedregister/67fr34992.pdf._Hlt11907452_Hlt11907692_Hlt11907737*. The OCC press release is available at *www.occ.treas.gov/ftp/release/2002-44a.pdf.*

UNITED STATES

Deadline Looms as FCC Reaffirms Electronic Surveillance Capabilities

Telecommunications carriers face a June 30, 2002 deadline to have in place technology that enables law enforcement to engage in lawfully authorized electronic surveillance of modern-day telecommunications. The deadline stems from the 1994 enactment of the Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279, which was intended by Congress to ensure that electronic surveillance by law enforcement could keep up in the age of digital technology and wireless services. The June 30 deadline applies to wireless, cellular, and broadband Personal Communications Services (PCS).

On April 11, the Federal Communications Commission issued an order that reinstated four Department of Justice/Federal Bureau of Investigation electronic surveillance capabilities that telecommunications carriers must comply with by June 30. Those four capabilities, along with other electronic surveillance capabilities, were mandated by federal regulators in 1999, but were vacated by a federal court in 2000.

Rodney Small, an economist in the FCC's office of engineering and technology, told *WILR* that carriers can file individual petitions for extensions of the June 30 deadline. He added that a number of carriers already have done just that.

Extensions of Time to Comply

It may difficult for some carriers to meet the June 30 deadline, Small said. Carriers are "in different positions, because some vendors are further along in having developed" the electronic surveillance capabilities carriers are now required to have in place. He added that any appeal of the FCC's April 11 order would have to be filed with the D.C. Circuit by July 30.

Michael Altschul, senior vice president and general counsel with the Cellular Telecommunications & Internet Association, said he believed that "nearly all the carriers" have waivers already in place that extend the time they will be given to comply.

The universe of carriers, Altschul said, includes six national carriers and about 140 other carriers. Altschul said he did not know how frequently law enforcement would need to carry out electronic surveillance using the technological capabilities carriers now must have in place. Peter M. Connolly, a telecommunications attorney with Holland & Knight LLP, told *WILR* that "most carriers are trying to comply" with the FCC's order.

Punch List Capabilities

The four so-called "punch list" electronic surveillance capabilities that were vacated by a federal court in 2000 and were reinstated by the FCC on April 11 are:

- dialled digit extraction, which gives law enforcement access to the digits punched in by a surveillance subject after a call connects. Dialled digit extraction comes into play, for example, if a subject dials an 800 number, and subsequently dialled numbers are of interest to law enforcement;
- party hold/join/drop messages, which allows law enforcement to identify the parties to a conference call;
- subject-initiated dialling and signalling information, which gives law enforcement information about features such as call forwarding or call waiting; and
- in-band and out-of-band signalling information, which informs law enforcement of signals sent to a telephone, such as a busy signal or a call waiting signal.

D.C. Circuit Ruling

The punch list and other parts of a 1999 FCC order were challenged in court by the telecommunication industry and privacy groups. They argued, among other things, that the capabilities were not authorized under CALEA and that the privacy and security of communications were not adequately protected. In 2000, the U.S. Court of Appeals for the District of Columbia Circuit vacated the four punch list requirements, finding the FCC had not explained why those capabilities were required by CALEA, *United States Telecom Association v. FCC, 227 F.3d 450 (D.C. Cir. 2000)*. The D.C. Circuit sent the matter back to the FCC. Two punch list items were not appealed: subject-initiated conference calls and timing information.

In response, the FCC requested and received comment, and on April 11, reaffirmed its earlier conclusion that the punch list electronic surveillance capabilities

were authorized by CALEA, and provided what it hoped was an acceptable explanation of its reaffirmance.

"We find it reasonable to require wireline, cellular, and broadband PCS carriers to implement all punch list capabilities by June 30, 2002," the FCC wrote in its April 11 order. The deadline is acceptable, the FCC continued, because carriers have been aware of the CALEA capabilities under consideration since 2000. "In addition, the record indicates that much of the software required to implement the punch list items has already been developed, which should significantly speed implementation."

Challenge to FCC Order Not Anticipated

Lawrence Sarjeant, a vice president and the general counsel of the United States Telecom Association, said the USTA has no current plans to appeal the FCC order. USTA was among the parties that filed the court challenge that led to the D.C.

Circuit's 2000 Decision

The June 30 compliance deadline, Sarjeant said, "hits individual companies differently, which is why the system ... allows for waivers" to be filed. David L. Sobel, general counsel of the Electronic Privacy Information Center, said that EPIC will not seek an appeal of the FCC's April 11 order. EPIC also filed a legal challenge that led to the D.C. Circuit's decision. The 2000 ruling by the D.C. Circuit, Sobel said, was "not a perfect outcome but a reasonable accommodation of the privacy issues and the law enforcement interests," and EPIC largely accomplished its goals with respect to CALEA two years ago, he said.

Sobel said, in fact, that the two biggest issues for EPIC involve not the punch list capabilities but two other items mandated by the FCC under CALEA: location tracking capabilities for cellular phones and packet-mode interception capabilities. "We feel like those were, to a certain extent, limited by the court in 2000," Sobel said.

Location Tracking of Cell Phones

Sobel explained that location tracking for cell phones referred to a requirement that all cell phones be equipped so that law enforcement could be informed of the location of the nearest cell tower at the beginning and the end of a call by a targeted individual.

That requirement was left standing after the D.C. Circuit's decision, Sobel noted, but the court left open the question of what legal authority would be needed by law enforcement to engage in cell phone location tracking, he said. "In other words, what piece of paper do they [law enforcement] have to give to the cellular phone company to get that information? There was some suggestion that the law enforcement position might be that if they got a pen register order, that might be adequate authority," Sobel said, but the D.C. Circuit indicated it its 2000 ruling that something more than a pen register would be needed. A pen register records call-identifying information such as whom a target called and when.

Sobel said a pen register order is very easy to obtain, and he said it is not yet clear what kind of authority law enforcement is needed for location tracking of cellular phones. "It remains an open legal question. It's somewhat amazing that this capability exists, as required by CALEA, and no one is clear on what the legal requirement is for the government to exercise that ability, except that it's something more than a pen register order," he said. Sobel added that he has specifically asked two Justice Department attorneys who are "in a position to know the answer to that question, and they refused to go on the record" with an indication of what specific legal authority is required for location tracking.

Packet-Mode Interception

The other item that EPIC was concerned about but which was somewhat addressed by the D.C. Circuit decision pertains to packet-mode interception capabilities. Packet-mode interception, he said, differs from traditional telephone technology, which involves a dedicated line between two parties. "It's easy to put a pen register on one telephone line or put a wiretap on one line," he said. If, instead, "the data is moving digitally in so-called packet-mode, there are all these packets moving through a network and not just one dedicated line."

"There's a big data pipe containing bits and pieces of thousands of conversations, so there's an issue of how law enforcement gets access to either the pen register information or the wiretap information in that environment." He said it is another issue that is still being resolved between industry and the government. "The government's answer, thus far, is the Carnivore system," he said, which monitors network traffic. The items on the FCC punch list that go into effect June 30, Sobel said, involved "lesser capabilities."

Sobel said that "the basic problem is that it is very complex and technologically difficult to ensure the same degree of privacy protection in this new technology as there was in the old." He noted, for example, that in the days of old-style telephones, it was relatively easy for law enforcement authorities to "surgically" tap a person's telephone, and not affect a neighbor's telephone line. "But in the digital environment, as everything moves in packet-mode, as part of a flood of data. it's not individual, dedicated lines anymore," he said. "Once you give law enforcement access to that data stream, there are a whole range of new issues and privacy problems that arise."

The FFC's April 11 Order on Remand is available on the Internet at *http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-02-108A1.pdf*. Information on CALEA is available on the FCC's website at *www.fcc.gov/calea*.

CANADA

■ ON-LINE LOTTERY VIOLATES CANADIAN CRIMINAL CODE

Reference Re Earth Future Lottery (P.E.I.) (2002 PESCAD 8)

Province of Prince Edward Island in the Supreme Court – Appeal Division, April 24, 2002

In a reference to the Prince Edward Island ("P.E.I.") Supreme Court (the "P.E.I. Reference"), an on-line lottery was held to violate the Canadian *Criminal Code* despite holding a provincial lottery licence, one of the limited exceptions under which a lottery may legally be operated in Canada. The Court found that the provincial lottery licence was *ultra vires* the provincial licensing authority, since the lottery would not be conducted entirely within the province granting the licence. The Court also held that the lottery violated the Criminal Code prohibition against lottery schemes operated on or through a computer.

The P.E.I. Reference confirms that contractual deeming provisions regarding the place of contract and governing law are not sufficient to shield an on-line lottery from the application of criminal laws. However, as the first known case to consider the legality of on-line lotteries in Canada, the P.E.I. Reference also does little to clarify several important legal aspects of how lotteries are conducted on-line. For example, it does not address where the contract between a ticket purchaser and the on-line lottery is formed. It also provides little guidance on the broader question of what factors will indicate in what jurisdiction a lottery operates. Most importantly, the case fails to identify what conditions would need to be met for an on-line lottery to operate legally in Canada.

In 2001, Earth Future Lottery, an environmental charity, applied for and was issued a licence allowing it to conduct, manage, and promote a lottery from its place of business in P.E.I. Purchasers could order lottery tickets either by phone or on-line using the lottery's website. The Rules and Regulations of the lottery and the terms of the provincial licence both provided that transactions were to be deemed to occur within the province of P.E.I. and to be governed by the laws of P.E.I. and the Canadian *Criminal Code*. Although the purchase of tickets was to take place primarily on-line, winning numbers were to be selected, not by computer, but by using conventional mechanical drums containing numbered balls. In addition, all coordination of lottery operations was to take place entirely within P.E.I.

Lotteries Generally Prohibited In Canada, But Exceptions Apply

Lotteries in Canada are generally prohibited under Section 206 of the *Criminal Code*. However, Section 207(1) of the *Code* provides a number of exceptions to this prohibition. One exception specifically allows charitable lotteries, but only where the lottery has been licensed by the province in which it operates, is conducted entirely within that province and, pursuant to Section 207(4) of the *Code*, is not operated "on or through a computer".

The two key questions the Court was asked to consider were, therefore:

(1) whether the lottery was a wholly provincial operation, thereby giving the provincial government licence-granting authority; and

(2) whether the lottery was operated on or through a computer.

Criminal Law Applies Regardless Of Where Contract Formed

The first question turned on whether an on-line lottery advertised over the Internet and therefore targeting potential purchasers outside P.E.I. could still be said to take place within the province, as required by the exception in the *Criminal Code*. The Court held that while the lottery would be based in P.E.I., the fact that it would likely attract purchasers from outside P.E.I. meant that not all of its operations would occur within provincial borders. Moreover, it held that the deeming provisions contained in the Rules and Regulations and the provincial licence did not affect liability under criminal law.

In assessing whether the lottery was conducted "on or through a computer", the Court simply noted that while the management and administration of the lottery and the drawing of winning numbers would take place off-line, advertising and the sale of tickets were activities to be conducted primarily through the use of computers. Moreover, the Court found that the Earth Future lottery depended on the use of computers to operate.

Court Declined To Comment On Key Issues

In part because the case originated as a reference from the P.E.I. government, the number of issues on which the Court was asked to rule was limited. Even on the questions the Court did consider, the approach taken was narrow and literal, resulting in little clarification or guidance on several important issues.

For example, the Court failed to consider questions surrounding where and how a lottery transaction is concluded in light of new provincial legislation establishing functional equivalency for on-line transactions, and in view of the contextual analysis increasingly being

employed by Canadian courts in other cases involving on-line issues.

The Court also provided little guidance on the question of what criteria should be used to determine the jurisdiction in which an on-line lottery is conducted, and how these criteria would differ when applied to consumer protection and other non-criminal business regulation as opposed to criminal law. The Court's conclusion, reflecting its focus on criminal law, was that any unauthorized extra-provincial element would be enough to invoke the prohibition on conducting a lottery out-of-province.

Legal Status of On-line Lotteries Remains Unclear

Most importantly, while the Court found that contractual deeming provisions do not prevent a finding that a lottery is conducted outside a province for the purpose of liability under criminal law, it gave no indication as to what conditions would allow a lottery to operate legally on-line.

The Court did not comment, for example, on whether technical barriers or other solutions aimed at preventing access by purchasers outside the licence-granting province might be sufficient to avoid criminal liability. It also did not reflect on whether a statement in the Rules and Regulations to the effect that non-residents are ineligible to participate, or that the lottery is void where prohibited, would satisfy the provisions in the *Criminal Code*.

Answering these questions will be essential to determining on what basis, if any, lotteries can legally be conducted on-line in Canada under existing law. The narrow interpretation of the *Criminal Code* adopted by the Court in the P.E.I. Reference suggests that conventional lotteries in Canada may not legally use the Internet in any significant aspect of their operations, in particular in relation to the sale of tickets. Moreover, the interpretation adopted by the Court offers little scope for the legal operation of lotteries that operate primarily on-line, or of Internet-based gambling operations, which are governed under the same sections of the *Criminal Code* as lotteries.

The P.E.I. Reference points to the need for a more sophisticated and contextual analysis by Canadian courts in future on-line lottery and on-line gambling cases, and likely to the need for legislative reform to the extent that Canadian laws unfairly restrict the operation of on-line lotteries. Recent comments by both provincial lotteries regulators and federal elected officials suggest that legislative reform may happen sooner rather than later. Until courts or legislatures revisit the conclusion reached in the P.E.I. Reference, the legal status of on-line lotteries in Canada will remain unclear.

The full text of the P.E.I. Reference can be downloaded from *www.gov.pe.ca/courts/supreme/reasons/923.pdf.*

* * * * *

Report by Theodore C. Ling and Arlan Gates of Baker & McKenzie's Information Technology & Communications Group, Toronto, with the assistance of Alexandra Wilson (student); website: www.bakernet.com; e-mail: theodore.c.ling@bakernet.com; arlan.gates@bakernet.com.

CANADA

"WEB-WRAP" AMENDMENTS TO ON-LINE SERVICES CONTRACTS

Kanitz v. Rogers Cable Inc. [2002] O.J. No. 665

Ontario Court of Justice, February 22, 2002.

The Ontario Court of Justice has held that where an on-line service provider states in its user agreement that posting notice of amendments on a website will constitute sufficient notice, an amendment may be enforced whether or not users make themselves aware of it. The decision is believed to be the first Canadian judgment to enforce "web-wrap" amendments that have not been actively accepted by users.

Rogers Cable, the cable division of a large Canadian media company, offers a high-speed cable Internet service to residential customers. Before installing the physical equipment necessary to receive service, Rogers requires customers to sign a user agreement in paper form. The agreement provides that Rogers may make amendments at any time, and expressly states that notice of amendments may be communicated to users in one of three ways: by e-mail, by postal mail, or via a notice posted on the company's website. The agreement further provides that continued use of the Rogers service by users constitutes acceptance of any amendments.

In November 2000, Rogers sought to amend its user agreement by adding a clause that provides for mandatory arbitration and includes a waiver of users' rights to participate in class action litigation against Rogers. Rogers posted the arbitration clause to its website, and placed a notice on the customer support page stating that the user agreement had been amended. The "last amended" date in the agreement was modified. Rogers also mailed an "iToolbox" kit to users, which contained a copy of the amended user agreement and included a guide that invited customers to visit the customer support site on which the notice of amendment was posted, in order to view "important information".

In July 2001, five plaintiffs alleging deficiencies in the quality and availability of service attempted to bring a class proceeding against Rogers. Rogers sought to stay the action on the basis of the arbitration provision in the amended user agreement. The plaintiffs contended that adequate notice of the amended user agreement was not effectively communicated to them and the change to include arbitration was therefore not binding on them because:

(i) the website notice was not placed on the home page of the Rogers website;

(ii) the amended agreement was hidden in the website;

(iii) the arbitration clause was buried in the agreement, and

(iv) the arbitration provision was unconscionable.

Website Postings May Constitute Sufficient Notice

In assessing the arguments brought by the plaintiffs, the court held that the provision in the user agreement for amendments to be posted to Rogers' website did not require that notice be posted directly on the home page. The court found that the customer support page met the notice requirements of the user agreement, and would be a logical part of the site on which to post such a notice. The court also held the agreement itself was not hidden on the website. It noted that locating specific information on any website might involve a trial and error process, and that in this case the user would view only five screens before arriving at the amended user agreement. The court found no evidence that the added clause was buried in the agreement, and determined that a clause requiring the parties to arbitrate disputes did not meet the legal test for unconscionability.

Subscribers To On-Line Services Consent To Communicate Electronically

The court did not ignore the fact that the plaintiffs, and the vast majority of other Rogers users, are individual consumers, whose poorer bargaining position normally merits a higher level of protection from the court than would be available for two parties of equal standing. On this point, however, the court considered the nature of the service at issue and found that it would be reasonable for users of on-line services to communicate with their on-line service provider using the same electronic format. The court also noted that while Rogers could have sent a notice via e-mail, as long as it used one of the communication methods specified in the user agreement, it could not be faulted for not having used another.

Scope Of Decision May Be Limited

While the judgment is important, several factors suggest that it may not have broad application. It is unclear, for example, that the ruling would apply to user agreements where the service provider operates a website but does not provide the services in question primarily on-line. Similarly, while Canadian courts have generally upheld "click-wrap" agreements, in which users must positively indicate acceptance, they have previously provided little if any guidance on the enforceability of web-wrap agreements, in which acceptance is simply deemed by a user's continued use. It is therefore not clear that amendments notified on-line will be upheld where the original agreement that provides the manner in which amendments may be made, is presented in web-wrap rather than click-wrap form or paper form.

Other issues are also unclear. For instance, the court does not mention at what point or after how many screens, an amendment to an agreement, or a notice thereof, will be considered to be buried or hidden on a website. Myriad factors contribute to how easily specific website information can be located, and variables such as the size and organization of the site and the capabilities of users are likely to figure in the determination. At what point users will be found to consent to receive contractual notices through electronic communications is also open to debate, given electronic commerce legislation in Ontario and most other Canadian provinces that generally provides that the use of electronic documents is voluntary absent express or implied consent.

These uncertainties, combined with the particular facts of this case, make it doubtful that courts will now automatically enforce all contract amendments notified on-line. The case does suggest, however, that Canadian courts may be more willing to enforce web-wrap amendments in certain circumstances.

The full text of the case is not available on-line, but can be obtained by contacting the authors.

* * * * *

Report by Theodore C. Ling and Arlan Gates of Baker & McKenzie's Information Technology & Communications Group, Toronto, with the assistance of Alexandra Wilson (student); website: www.bakernet.com; e-mail: theodore.c.ling@bakernet.com; arlan.gates@bakernet.com.

DOMAIN NAME ARBITRATION

UDRP CLAIM FOR *PAINT.BIZ* NET NAME

Valspar Sourcing Inc. v. TIGRE (Case No. FA0204000112596)

National Arbitration Forum, June 4, 2002

A complainant's use of the PAINT.BIZ mark in commerce as well as its registering the mark in France and applying for registration in the United States establishes rights in the mark requiring the transfer of the *paint.biz* domain name from the registrant who has no such rights, a National Arbitration Forum arbitrator ruled June 4. In a Start-up Trademark Opposition Policy action against TIGRE, the registrant of the *paint.biz* domain name, the arbitrator ordered the transfer of the domain name registration to complainant Valspar Sourcing Inc., which he determined had rights in the mark PAINT.BIZ stemming from its obtaining a trademark registration in France and applying for one in the United States.

Complainant Registered Mark in France

The respondent is a small business in Yuma, Ariz., engaged in the manufacture and sale of fine craftsmanship wood products. TIGRE asserted that it registered

the domain name *paint.biz* without the intent to disrupt complainant's business or to create a likelihood of confusion with complainant's mark.

The complainant is a wholly-owned subsidiary of multinational coatings company Valspar Corp. It is the registered owner of the trademark PAINT.BIZ in France and has applied for a U.S. trademark for PAINT.BIZ as well. Valspar has also been selling its product in cartons displaying its PAINT.BIZ mark since 2001.

Valspar alleged that the respondent tried to register the *paint.biz* domain name after it had developed and/or registered its trademarks. The domain name is identical to its mark, the complainant argued. In addition, under U.S. law, Valspar said that registration of a trademark is constructive notice of the registrant's claim of ownership. On the other hand, TIGRE alleged that it intended to use the *paint.biz* domain name to market its unique products and it is not in competition with the complainant or its competitors. The respondent also claimed that the claimant's French trademark registration is dated May 23, 2001 and its U.S. trademark application is dated September 27, 2001, after the Internet Corporation for Assigned Names and Numbers's May 15 announcement of the introduction of the ***.biz*** top level domain. TIGRE alleged that Valspar only sought to establish rights in the mark after the announcement of the introduction of the ***.biz*** TLD.

Proved Each Element of Paragraph 4(a)

In ordering the transfer of the domain name registration from TIGRE to Valspar, Arbitrator Karl V. Fink found pursuant to the requirements of paragraph 4(a) of the Stop policy that complainant Valspar had rights in the mark PAINT.BIZ, respondent TIGRE had no rights or legitimate interests in the disputed domain name, and the respondent registered the domain name in bad faith.

Concerning the complainant's rights in the mark, the arbitrator said that Valspar had demonstrated that before the domain name was registered it had used the mark in commerce, had registered the mark in France, and had applied for registration of the mark in the United States. The arbitrator also found that the respondent had no rights or legitimate interests in the domain name *paint.biz* because there was no evidence that it or any business it is affiliated with is commonly known as PAINT.BIZ or paint.biz.

Finally, the arbitrator said that when TIGRE registered the disputed domain name it was on notice of Valspar's rights in PAINT.BIZ because it received notice of Valspar's IP Claim and this, therefore, was evidence of bad faith registration of the domain name.

The text of the decision is available on the National Arbitration Forum's website at *www.arbforum.com/domains/decisions/112596.htm*.

FRANCE

■ STIFF PENALTIES FOR "BREAK-UP SPAMMING"

Noos v. Philippe P.

Tribunal de Grande Instance de Paris, May 24, 2002

PARIS—A French court has imposed stiff fines and a four-month suspended prison sentence on a computer programmer who sent more than 360,000 "spam" messages to clients of a local cable-based Internet Service Provider at the tail-end of an on-line emotional relationship that developed, and then turned sour. The criminal court issued its unusual Internet ruling after Noos—an ISP owned by Franco-Belgian communications and utilities giant Suez—provided evidence documenting the Internet user's spamming activities in early 2002 and their devastating impact on the company's network.

Noos showed in court that Philippe P.—French law prohibits the use of full names in on-line databases—sent 20,000 and 40,000 spam messages to Noos clients on January 2 and January 4 respectively, at the end of the relationship. Numerous clients reported the "break-up spam" to Noos, which initially cut Philippe P.'s Internet connection for intentionally violating contractual terms of service. The connection was re-established in late January, at which time Philippe P. issued a second wave of more than 320,000 spam messages to Noos clients, paralyzing the network and causing a system shut-down for more than 10 hours.

The court found Philippe P. guilty of violating Section 323-2 of the Penal Code—"intentionally damaging the operation of an automated data processing system"—and ordered fines of EURO 20,000 ($18,800) and the four-month suspended sentence.

Observers say that the stiff fine and suspended sentence—which went far beyond the penalties sought by state prosecutors—were aimed at sending a message to would-be spammers that judges will not look kindly on actions that damage network functioning.

France's previous spamming rulings have been issued by civil courts, which usually limited damages to low four-figure sums.

GERMANY

■ ISP LIABLE FOR CONTENT PRIVATE USER PUT ON MSN COMMUNITY FORUM

Graf v. Microsoft GmbH (Case No.15 U 221/01)

Oberlandesgericht in Zivilsachen Köln, May 28, 2002

BERLIN—The Microsoft Network Internet service provider is responsible for the content placed on

its server by private users because the company created the posting forum in such a way as to allow for the objectionable activity, the Cologne High Regional Civil Court held May 28. The court, upholding a lower court ruling, found that Microsoft GmbH was responsible for the content of the community "Celebrities," under Section 5, paragraph 1 of the law on the use of teleservices. Private users can post text and images into the various "communities" forums.

From the point of view of an objective user, the content of the objectionable community should be attributed to Microsoft, the court said, because it provided the infrastructure for the community, established the topic, permitted the posting over its own Web pages, framed the community site with its own product advertisements, and stipulated the basic rules of use for participating.

The court rejected Microsoft's contention that it should not be held liable for the posted content because the user is clearly not affiliated with the company, the user has the option of anonymous posting, and the company specifically states on its site that it is not responsible for content.

Microsoft Declined to Block Future Postings

The complaint was brought against Microsoft by tennis celebrity Steffi Graf. Initially, she asked Microsoft to remove the pictures—consisting of her face pasted on photos of naked bodies—which a private user had posted and made available for downloading and for sale. Microsoft responded to her request and closed the site June 21, 2001. However, Graf filed suit when the ISP declined to sign a declaration to halt such postings in the future, or be subject to a fine. The lower court, the Cologne regional court, October 5, issued a temporary injunction against Microsoft, prohibiting it from allowing users to publish, disseminate, or sell the doctored photos.

Ramifications Exaggerated

The implications of the case for electronic commerce in Germany have been highly exaggerated in press reports, according to Michael Terhaag, an attorney specializing in Internet law for the law firm Strömer Rechtsanwälte in Düsseldorf. Microsoft created a forum for publishing such pictures, he said. "In this particular case, the ruling was correct and unambiguous," he stressed.

This is not a case of assigning providers broad responsibility for content posted by users, and should not be a cause for worry for auction or other electronic commerce sites, Terhaag stated. A final decision in the matter is still awaited, and the decision does not yet carry legal force, he noted.

UNITED KINGDOM

INVISIBLE TRADEMARK INFRINGEMENT

Reed Executive PLC and Reed Solutions PLC v. Reed Business Information Ltd, Reed Elsevier (UK) Ltd and totaljobs.com Ltd

High Court of Justice, May 20, 2002

The recent High Court decision in the *Reed* "invisible trademark" case has confirmed that search engine "optimization" techniques can amount to trademark infringement and passing off even if a website owner's use of another person's trademark is invisible to people searching on the Internet.

For the defendant Reed Business Information Ltd ("RBI"), part of the Reed Elsevier publishing group, recruitment advertising is a key revenue stream. The economics of recruitment advertising, where advertisements are actively sought by their target market, have been fundamentally altered by mass access to the Internet. By the mid-1990s, stand-alone recruitment sites ("job boards") were beginning to compete directly with traditional print media and RBI's revenues from recruitment advertising began to fall. RBI formed a plan to create what they described in a brief to advertising agency CDP as the "leading horizontal United Kingdom-based recruitment site" to be known as *totaljobs.com*.

There had always been a certain amount of confusion between Reed Elsevier and the claimants ("Reed Employment"), a leading High Street employment agency group. This had not been confusion of the passing-off variety because the two businesses—publishing and employment agencies—were quite distinct. The two groups came into conflict after RBI set up *totaljobs.com*. RBI was now in a similar line of business to Reed Employment and the use of its name Reed was now a legal issue.

A Reed Employment company was the registered proprietor of the trademark REED in respect of "Employment Agency Services, included in Class 35". Although RBI's site had a completely different, generic name, the word "Reed" appeared on the *totaljobs.com* site in a visible manner in RBI's logo, in Reed Elsevier's logo and in the copyright line. The judge found that this gave rise to relevant confusion as to origin for the purposes of Section 10(2)(b) of the Trade Marks Act 1994 and also for the purposes of the passing-off claim.

One very interesting aspect of the judgment is its dissection of various invisible uses of the word "Reed" in the context of RBI's optimization tactics. *totaljobs.com* was promoted both in traditional advertising media and by means of standard Web optimization techniques. These "invisible matters" became relevant when they involved use of the word "Reed."

Four of RBI's methods of optimization were considered:

(i) use of the word Reed in invisible metatags on the website;

(ii) use of the word in directory entries;

(iii) banner advertisements including mock search results on purchased keywords; and

(iv) Yahoo! banner advertising where "Reed" was a keyword.

Metatags Not Necessarily Infringing

The judge did not consider that every metatag use of a trademark would necessarily amount to an infringement. The judge questioned whether users of search engines would suppose that when they searched against, say, "Reed jobs", the sites shown in the search results had any connection with Reed Employment. A search including the word "Reed" would typically show many results having no connection with Reed Employment at all.

The judge felt that a "description" metatag displayed by a search engine alongside a hit would amount to infringement if it included the trademark. But he was less convinced that there could be infringement where material such as this did not appear on search engine results.

Banner advertisements triggered by the word "Reed" specified by RBI were also objectionable. However, where the trigger was the word "jobs", for example, and banners came up in response to a search for "Reed jobs", this could not be an infringing use.

There was an allegation of bad faith against RBI relating to its use of a robots.txt file. Although unfounded, this allegation demonstrates the sophisticated techniques with which the courts must now come to terms when dealing with the trademark aspects of Internet marketing. The suggestion that the robots.txt file on the site had some sinister purpose came apart as a result of expert evidence as to the contents of historic pages on the site. This evidence was based on material obtained from *web.archive.com*, a vast electronic library of sites on the Internet.

The judge decided that his conclusions on passing-off in relation to invisible optimization matters mirrored his conclusions on trademark infringement, the answer turning on whether RBI could be said to be responsible in any way for the appearance of the site in response to a search against the word "Reed."

* * * * *

Report by Charlie Swan, partner in London media law firm The Simkins Partnership (www.simkins.com); e-mail: charles.swan@simkins.com.

UNITED STATES

■ DOMAIN NAME REGISTRATIONS IN FORUM SUPPORTS JURISDICTION

Bird v. Parsons (Case No. 00-4556)

U.S. Court of Appeals for the Sixth Circuit, May 21, 2002

An allegation that a domain name registrar transacted about 5,000 domain name registrations with residents of Ohio supported the exercise of specific personal jurisdiction over the registrar under the U.S. Constitution and the Ohio long-arm statute, the U.S. Court of Appeals for the Sixth Circuit ruled May 21. The court reached the conclusion that a nation-wide domain name registrar could be subject to specific personal jurisdiction after first finding that it could not be subject to general jurisdiction, because the domain name transactions were not sufficient to establish minimum contacts with Ohio.

However, the court also held that the registration and auction listing of a domain name that included the plaintiff's trademark was not a "commercial use in commerce" under the Lanham Act and, therefore, could not be the basis for a trademark claim.

Plaintiff Owned Rights in "*Financia*"

Since 1983, the plaintiff, Darrell J. Bird of Dayton, Ohio, had operated a software business using the name Financia Inc. In 1984, he obtained a U.S. trademark for the term FINANCIA and in 1995 he registered a copyright for a manual and a computer program called "Financia." The company had also registered the domain name *financia.com*. In 2000, defendant Marshall Parsons of California registered the domain name *efinancia.com* with defendant domain name registrar Dotster Inc. of Longview, Wash. The day after Parsons registered the domain name, Afternic.com Inc. of New York listed *efinancia.com* on its domain name auction website.

Bird brought suit against Parsons, Dotster, Afternic, and two Dotster principals charging trademark infringement under the Lanham Act of 1946, 15 U.S.C. §1114(1)(a); unfair competition under 15 U.S.C. §1125(a); trademark dilution under 15 U.S.C. §1125(c); cybersquatting under the Anticybersquatting Consumer Protection Act of 1999, 15 U.S.C. §1125(d); and copyright infringement under the Copyright Act of 1976, 17 U.S.C. §106.

Constitutional Due Process Applied

In determining that the court could legitimately exercise personal jurisdiction over Dotster, Judge Ronald Lee Gilman analyzed the facts under the due process clause of the U.S. Constitution and standards for both general and specific jurisdiction.

Such a jurisdiction question must be analyzed both under the U.S. Constitution and under the state

long-arm statute. Even though the Ohio long-arm statute was not coterminous with the Fifth Amendment, the court addressed the constitutional question first. The due process clause, as interpreted by *International Shoe Co. v. Washington, 32 U.S 310 (1945),* requires that the exercise of personal jurisdiction over an out-of-state defendant be consistent with "traditional notions of fair play and substantial justice." This standard is applied by a finding of whether the defendants have sufficient minimum contacts with the forum state such that the defendant would reasonably expect that he or she might be haled into a court in that state. Based on Dotster's admission that they had registered a total of about 333,000 domain names, the plaintiff estimated that about 5,000 of those were in Ohio. This figure was reached by dividing by 50 the 70 percent of registrations, which occurred in the United States. The plaintiff argued that these 5,000 registrations in addition to the accessibility of Dotster's site was enough to support a finding of minimum contacts.

Contacts Do Not Create General Jurisdiction

These contacts do not support an exercise of general personal jurisdiction over the Dotster defendants, the court concluded, after comparing them to minimum contacts alleged in *Helicopteros Nacionales de Colombia SA v. Hall, 466 U.S. 408 (1984).*

Helicopteros rejected the claim that a number of purchases of helicopters from a Texas company established sufficient minimum contacts with Texas under *International Shoe.* These helicopter purchases, the court said, were similar to the domain name registrations in this case. Jurisdiction based on the accessibility of a website had also been rejected by previous decisions, such as *Cybersell Inc. v. Cybersell Inc., 130 F.3d 414 (9th Cir. 1997).*

Cybersell rejected jurisdiction based on an accessible passive website; however, its principle applies in this case, the court said, because Dotster's registration website merely allows the company to do business with Ohio residents. According to *Bancroft & Masters Inc. v. Augusta National Inc., 223 F.3d 1082 (9th Cir. 2000),* "engaging in commerce with residents of the forum state is not in and of itself the kind of activity that approximates physical presence within the state's borders," which is the ambit of general jurisdiction.

Specific Jurisdiction Found

Turning to the question of specific jurisdiction, the court concluded that the plaintiff had, indeed, established a prima facie case that an exercise of personal jurisdiction over the three Dotster defendants would not offend constitutional due process and would be permitted by the state's long-arm statute.

The standard for specific jurisdiction is a three-part test set forth in *Southern Machine Co. v. Mohasco Industries Inc., 401 F.2d 374 (6th Cir. 1968).* Under this test:

- "[T]he defendant must [have] purposefully avail[ed] himself of the privilege of" doing business in the forum state.
- "The cause of action must [have] arise[n] from the defendant's activities there."
- "[T]he acts of the defendant or consequences caused by the defendant must have [had] a substantial enough connection with the forum state to make the exercise of jurisdiction reasonable."

A website accessible in Ohio and an allegation that 5,000 transactions were conducted with Ohio residents were sufficient to established the purposeful availment prong of the test, the court concluded, citing to *Neogen Corp. v. Neo Gen Screening Inc., 282 F.3d 883 (6th Cir. 2002).* According to *Neogen,* purposeful availment can be found "if the website is interactive to a degree that reveals specifically intended interaction with residents of the state." The allegation of 5,000 transactions with Ohio residents was enough to show "that Dotster regularly chooses to do business with Ohio residents."

Under the second prong of the test, the court concluded that Dotster's registration business "at least marginally related to the alleged contacts between the Dotster defendants and Ohio." This portion of the test imposed a "lenient" standard on the plaintiff, the court said. Even though the specific registration of the *efinancia.com* domain name was not one of Dotster's Ohio transactions, under *Third National Bank in Nashville v. Wedge Group Inc., 882 F.2d 1087 (6th Cir. 1989),* "[t]his factor 'does not require that the cause of action formally "arise from" defendant's contacts with the forum; rather, this criterion requires only "that the cause of action, of whatever type, have a substantial connection with the defendant's in-state activities."

The fact that the plaintiff's claim arose out of Dotster's registration business and that Dotster's contacts with Ohio arose out of that business were sufficient to satisfy this prong, the court said. Finally, the court said, if the first two factors are met, then it may infer that it is reasonable to subject the defendant to the jurisdiction of the court. For this principle, the court cited to *Compuserve Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996),* which said: "if we find, as we do, the first two elements of a prima facie case—purposeful availment and a cause of action arising from the defendant's contacts with the forum state—then an inference arises that this third factor is also present."

Under *Compuserve,* there are a number of factors that may influence the reasonableness consideration, including "the burden on the defendant, the interest of the forum state, the plaintiff's interest in obtaining relief, and the interest of other states in securing the most efficient resolution of controversies." The court concluded that although the state of Washington had an interest in the dispute, all the other factors weighed in favour of a finding of reasonableness.

Claim Passes Test of Long-Arm Statute

With regard to the state long-arm statute, Ohio Rev. Code §2307.283(A) and Ohio R. Civ. P. 4.3(A)(4), permit an exercise of personal jurisdiction when the defendant's act or omission has caused tortious injury in Ohio provided that the defendant "regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered" in Ohio. Violations of the Lanham Act are analogous to torts, the court said, citing *to Panavision International LP v. Toeppen, 141 F.3d 1316 (9th Cir. 1998)*. Furthermore, the harm suffered from the trademark violation was suffered in Ohio, under *Panavision* and *Zippo Manufacturing Co. v. Zippo Dot Com Inc., 952 F. Supp. 1119 (W.D. Pa. 1997)*.

Claims Not Trademark Law Violations

However, the court went on to hold that the actions alleged by the plaintiff against Dotster and Afternic did not constitute violations under federal trademark law. The basic principle of a trademark infringement or unfair competition claim, the court said, is that the defendant must be using the mark in commerce.

According *to Academy of Motion Picture Arts & Sciences v. Network Solutions Inc., 989 F. Supp. 1276 (C.D. Ca. 1997),* a domain name registrar is merely executing the technological function of providing a link between a domain name and an Internet protocol address, an "purely nominative function that is not prohibited by trademark law." *Lockheed Martin Corp. v. Network Solutions Inc., 985 F. Supp. 949 (C.D. Cal. 1997)* analogized domain names in this respect with vanity telephone numbers, concluding that just because a domain name could be used in a manner that might violate a trademark holder's rights, it does not mean that the mere act of registering the domain name is, on the part of the registrar, a trademark violation.

"A registrar that grants a particular domain name to a registrant simply grants it an address," the court said. "The fact that the registrant can then use its domain name to infringe on the rights of a registered trademark owner does not subject the registrar to liability for trademark infringement or unfair competition."

Similar reasoning was applied to the claim against Afternic, the auctioneer: "The possibility that its customers might buy or sell infringing domain names does not alter the fact that Afternic does not use those names. Moreover, even a domain name that could be used to violate a registered trademark does not necessarily do so."

No Claim Stated for Dilution

The dilution claim against Dotster was also thrown out based on *Lockheed Martin's* principal that the "acceptance of domain name registrations is not a 'commercial use' within the meaning" of the statute. With regard to Afternic, the court did acknowledge that there might be a possibility that the auctioneer might be trading on the commercial value of the plaintiff's trademark when selling the domain name. However, in this case, the plaintiff had not offered evidence to support such a claim. Significantly, according to the court, there was no allegation "that Afternic's profits vary according to the ultimate selling price of the domain names that are auctioned on the site." Again, the court said, those who purchase domain names from Afternic might not be employing the plaintiff's mark in commercial use. "Simply posting a domain name on an Internet auction site ... is insufficient to establish the commercial use of a trademark," the court concluded. "This reasoning also applies to an entity, such as Afternic, that operates an on-line auction site."

Cybersquatting, Copyright Claims Also Rejected

With regard to the cybersquatting claim, the court noted that a violation of the ACPA can be found only when the defendant is found to have registered, used, or trafficked in a domain name. The ACPA only imposes liability for use of a domain name on the registrant. The only domain name registrant in this case was Parsons; therefore, Dotster and Afternic could not be found liable for registering or use. Finally, the court also found that neither Dotster nor Afternic had trafficked in the domain name.

"They did not purchase, sell, or otherwise participate in any transaction involving the 'transfer for consideration' or 'receipt in exchange for consideration' of Parsons's domain name," the court said. "Dotster's fees stem from its registering the domain name and allowing registrants to host their Web page[s] on its 'Futurehome page.' Afternic provides a virtual auction site, but the fact that its services might be used for trafficking in a domain name does not render it liable for trafficking." Finally, the court rejected the plaintiff's claim under copyright law, finding that the word "Financia" did not meet the required threshold of creativity to be protected by the federal copyright statute.

Judges Alan E. Norris and Eugene E. Siler Jr. joined in the decision.

UNITED STATES

■ COURT SHUTS DOWN CYBERSCAM PERMANENTLY

Federal Trade Commission v. Zuccarini

U.S. District Court for the Eastern District of Pennsylvania, April 9, 2002

A U.S. District Court has ordered the perpetrator of an Internet scheme to halt his illegal practices. The defendant employed more than 5,500 copycat Web addresses to divert surfers from their intended Internet destinations to one of his sites, and hold them captive while he pelted their screens with a barrage of

adult-oriented ads. At the request of the Federal Trade Commission, the court permanently barred the defendant from diverting or obstructing consumers on the Internet and from launching websites or Web pages that belong to unrelated third parties. The court also has barred the defendant from participating in advertising affiliate programs on the Internet, and has ordered him to give up more than $1.8 million in ill-gotten gains.

In October 2001, the FTC charged that the defendant, John Zuccarini, was registering Internet domain names that were misspellings of legitimate domain names or that incorporated transposed or inverted words or phrases. For example, Zuccarini registered 15 variations of the popular children's cartoon site, *www.cartoonnetwork.com,* and 41 variations on the name of teen pop star Britney Spears. Surfers who looked for a site but misspelled its Web address or inverted a term—using *cartoonjoe.com*, for example, rather than *joecartoon.com*—were taken to the defendant's sites. They were then bombarded with a rapid series of windows displaying ads for goods and services ranging from Internet gambling to pornography. In some cases, the legitimate website the consumer was attempting to access also was launched, so consumers thought the hailstorm of ads to which they were being exposed was from a legitimate website.

Once consumers were taken to one of the defendant's sites, it was very difficult for them to exit. In a move called "mousetrapping," special programming code at the sites obstructed surfers' ability to close their browser or go back to the previous page. Clicks on the "close" or "back" buttons caused new windows to open. "After one FTC staff member closed out of 32 separate windows, leaving just two windows on the task bar, he selected the 'back' button, only to watch the same seven windows that initiated the blitz erupt on his screen, and the cybertrap began anew," according to papers filed with the court.

Unfair and Deceptive Practices

The FTC alleged that the practices were unfair and deceptive, in violation of federal law. The court order permanently bars the defendant from redirecting or obstructing consumers on the Internet in connection with the advertising, promoting, offering for sale, selling, or providing any goods or services on the Internet, the World Wide Web or any Web page or website; and from launching the websites of others without their permission. The defendant will also be required to give up $1,897,166 in ill-gotten gains. The court also ordered certain bookkeeping and record-keeping requirements to allow the FTC to monitor the defendant's compliance with the court's order.

The Commission's complaint names John Zuccarini, doing business as The Country Walk, JZDesign, RaveClub Berlin, and more than 22 names incorporating the word "Cupcake," including Cupcake Party, Cupcake-Party, Cupcake Parties, Cupcake Patrol, Cupcake Incident, and Cupcake Messenger.

Copies of the complaint and Judgment and Permanent Injunction are available from the FTC's website at *www.ftc.gov.* The text of the court's order is available at *http://pub.bna.com/eclr/01cv4854.pdf.*

UNITED STATES

WEBSITE OPERATOR CHARGED WITH FRAUD

SEC v. Gold-Ventures Club (Case No. 1:02-CV-1434)

U. S. District Court for the Northern District of Georgia, May 28, 2002

The Securities and Exchange Commission on May 28 filed a complaint in the U. S. District Court for the Northern District of Georgia and obtained a temporary restraining order against Russian-based Internet website operators who allegedly targeted U.S. investors by using schemes promising exorbitant investment returns. The SEC also said that in one instance, the website operators impersonated an SEC attorney to raise additional funds.

200 percent Returns Promised

Specifically, the SEC said that Russia-based Gold-Ventures Club and Alexander Khamidouline, a resident of Russia, violated the anti-fraud and securities registration provisions of the federal securities laws. The SEC alleged that since at least March 2002, Gold Ventures and Khamidouline defrauded investors, through the Gold Ventures' website, *www.gold-ventures.net,* and mass spam e-mail campaigns targeting U.S. investors. According to the SEC, Gold Ventures' website—which claimed to have 900 members—falsely guaranteed that investors would gain 200 percent returns on their investments every 14 days, virtually risk free.

Impersonating SEC Staff

The SEC also alleged that after Gold Ventures became aware of the SEC investigation, it impersonated an SEC staff attorney in an attempt to blackmail an investor into sending more money to Gold Ventures. According to the SEC, one of Gold Ventures' investors received an e-mail that purported to come from an SEC staff attorney but was actually sent by Gold Ventures. The e-mail promised to close the SEC's investigation if the investor sent additional funds to an account controlled by Gold Ventures.

The SEC said that in addition to the temporary restraining order and asset freeze ordered by the court, it is seeking preliminary and permanent injunctions, disgorgement plus pre-judgment interest, and monetary penalties against Khamidouline.

The Commission also said that it is working with Russian securities regulators to carry out the relief ordered by the court.

UNITED STATES

■ COPYING E-MAILS STORED ON COMPUTER'S HARD DRIVE

Thompson v. Thompson (Civil No. 02-91-M, Opinion No. 2002 DNH 108)

U.S. District Court for the District of New Hampshire, May 30, 2002

The copying of e-mail messages from the hard drive of a personal computer does not constitute interception of electronic communication for the purposes of the Electronic Communications Privacy Act of 1986, the U.S. District Court for the District of New Hampshire ruled May 30. In so holding, the court relied on the decision in *Steve Jackson Games Inc. v. U.S. Secret Service, 36 F.3d 457 (5th Cir. 1994)*, rejecting an invitation to rule that *Steve Jackson Games* was wrongly decided.

The plaintiff, Basil W. Thompson, was in the midst of divorcing his wife, Anne M. Thompson. The plaintiff alleged that the defendants—Mrs. Thompson and her brother, Michael Trachemontagne—had copied e-mail messages that were stored on the hard drive of the plaintiff's computer. The plaintiff charged that the copying constituted a violation of the Wiretap Act, as amended by the Electronic Communications Privacy Act, 18 U.S.C. §2510, and the Stored Communications Act (Title II of the ECPA), 18 U.S.C. §2701.

The ECPA sets penalties for a person who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," 18 U.S.C. §2511(1)(a).

No ECPA "Interception" Here

Judge Steven J. McAuliffe held that the copying of the stored e-mail messages did not constitute interception under this section, citing to *Steve Jackson Games*. In that case, the U.S. Court of Appeals for the Fifth Circuit held that retrieving unread bulletin board messages that had been stored on the computer used to operate the board was not interception, because the accessing of the messages did not take place simultaneously with the sending of the messages.

That decision was based on a comparison of the definitions of "wire communication" and "electronic communication" given in the statute. Wire communications included messages in electronic storage, whereas electronic communications did not. Interpreting *Steve Jackson Games,* the court said:

"[B]ecause §2511 proscribes the interception of electronic communications, and because the category of 'electronic communications' includes the transfer but not the storage of various forms of data, the acquisition of stored e-mail—electronic data that are no longer in the process of being transferred—does not qualify as the interception of electronic communications."

The court brushed off the plaintiff's suggestion that *Steve Jackson Games* was wrongly decided, noting in particular that the Ninth Circuit had withdrawn its opinion in *Konop v. Hawaiian Airlines Inc., 236 F.3d 1035 (9th Cir. 2001),* the only case to have reached a contrary conclusion.

UNITED STATES

■ SALE OF REAL PROPERTY BY E-MAILS

Shattuck v. Klotzbach (Civil Action No. 01-1109A)

Massachusetts Superior Court, December 11, 2001

A series of electronic mail messages including the typewritten name of the authors at the end of each message constituted a valid "written" and "signed" memorandum or note as required by the state's statute of frauds, the Massachusetts Superior Court held December 11. In holding that e-mail messages that included the text of negotiations conducted by e-mail regarding the sale of real property were sufficient to satisfy the statute of frauds, the court cited to cases that upheld telegrammed messages as sufficient writings. The court reached its conclusion based on the common law without reference to the federal Electronic Signatures in Global and National Commerce Act of 2000.

The parties had been involved in negotiations regarding the sale of a house in Marion, Mass. The plaintiff had sent a message by electronic mail to the defendants and the message included an offer to purchase the property for $2 million.

Defendant David Klotzbach replied by e-mail, "expressing his appreciation for a reasonable offer, and stated that he would be willing to except *[sic]* $2,250,000." The message also expressed enthusiasm for the offer and indicated that he preferred to communicate by e-mail. In April 2001, the parties signed a sales agreement and the plaintiff made a deposit. However, the sellers then failed to meet one of the conditions of the agreement, the agreement was terminated, and the deposit returned. Negotiations recommenced a few months later and in July, the plaintiff made an offer of $1.83 million. The defendants counter-offered for $2 million and then after another month had passed asked the plaintiff if he was still interested in going through with $1.83 million offer. Eventually, the plaintiff indicated that he had asked his attorney to draw up an agreement. The defendants replied, saying "[o]nce we sign the [purchase and sale agreement] we'd like to close ASAP. You may have your attorney send the P&S and deposit check for 10 percent of purchase price ($182,500) to my attorney."

At the end of each e-mail message, the sender had typed his name.

Signature Indicates Intent to Authenticate

Justice Ernest B. Murphy rejected the defendants' claim that the plaintiff had failed to produce any signed writings evidencing the formation of a contract.

The Massachusetts statute of frauds, Mass. Gen. Laws. ch. 259, §1, states that an agreement for the sale of lands

is enforceable only when "some memorandum or note thereof, is in writing and signed by the party to be charged therein." The defendants argued that the e-mail messages did not satisfy this writing requirement.

First, the court referred to *Irving v. Goodimate Co., 320 Mass. 454 (1946)*, which stated that the statute of frauds is satisfied so long as the writing "is signed by the person to be charged in his own name or by his initials, or by his Christian name alone, or by a printed, stamped or typewritten signature, if signing in any of these methods be intended to authenticate the paper as his act."

Applying such an intent standard, the court held that a trier of fact could reasonably conclude that the typing of names at the end of the messages was done "with the intent to authenticate the information contained therein as his act."

The court then compared the e-mail messages to telegrams, which had been held as satisfying the statute of frauds in *Providence Granite Co. v. Joseph Rugo Inc., 362 Mass. 888 (1972)*, and *Hansen v. Hill, 340 N.W. 2d 8 (Neb. 1983)*. In fact, the court said, an e-mail message is even more indicative of the sender's intent to authenticate, because unlike in a telegram, the sender of an e-mail message usually types his or her name himself. In the case of a telegram, the whole message, including the signature, is executed by a telegram operator.

In this case, Klotzbach typed his name "intentionally and deliberately" at the end of his e-mail messages.

The text of the court's opinion is available at *http://pub.bna.com/eclr/011109.htm*.

UNITED STATES

■ FORMATION OF CONTRACTS WEBSITE SUPPORTS JURISDICTION

Gorman d/b/a Cashbackrealty.com v. Ameritrade Holding Corp. (Case No. 01-7085)

U.S. Court of Appeals for the District of Columbia Circuit, June 14, 2002

The courts of the District of Columbia may assert general jurisdiction over a foreign defendant whose website enables it to form binding contracts with district residents, the U.S. Court of Appeals for the District of Columbia Circuit ruled June 14. In a suit filed by David Gorman doing business as Cashbackrealty.com against Ameritrade Holding Corp. and Freetrade.com Inc. alleging breach of contract, the court held that it could assert general jurisdiction over the defendants because the Ameritrade website enabled the company to enter into binding contracts with district customers constituting the "continuous and systematic" contacts required by the forum's long-arm statute and consistent with constitutional due process. However, even though it ruled that it may assert jurisdiction over a foreign defendant doing business in the District of Columbia via an interactive website, the court affirmed the district court's dismissal of the complaint due to insufficient service of process on the defendant.

Allegedly Breached Deal to Link to Site

Cashbackrealty.com, a real estate broker headquartered in McLean, Va., allegedly had an agreement with on-line securities dealer Freetrade.com to provide a front-page link to its website. In November 1999, Ameritrade, an on-line securities broker-dealer with its principal place of business in Omaha, Neb., acquired Freetrade.com. Gorman claimed that although Ameritrade assumed Freetrade.com's obligation through its acquisition of the company, it refused to provide the link. On June 2, 2000, Gorman filed suit against Ameritrade and Freetrade.com in the U.S. District Court for the District of Columbia, alleging breach of contract. The district court dismissed the suit for lack of personal jurisdiction, stating that a company that seeks to encourage the use of its website by district residents "does not establish the necessary 'minimum contacts' " with the forum through Internet accessibility and does not "operate so continuously and substantially" within the district that it would be fair to allow it to be sued in that forum on any claim, regardless of where the claim arose. *Gorman v. Ameritrade Holding Corp., No. 00-1259 (D.D.C. 2001)*.

Contacts Must Be "Continuous and Systematic"

On appeal, the D.C. Circuit, in an opinion by Judge Merrick B. Garland, said that the district long-arm statute permits the exercise of general jurisdiction over a foreign corporation that does not arise from conduct in the forum if the corporation is "doing business" in the district. Such jurisdiction is permissible only if the business contacts are "continuous and systematic," the court said. In addition, it said that the reach of "doing business" jurisdiction pursuant to D.C. Code §13-334(a) "is co-extensive with the reach of constitutional due process."

Gorman argued that Ameritrade was subject to the general jurisdiction of D.C. courts because it sells securities and provides brokerage services to district residents "on a continuous basis." This constitutes "continuously doing business in the District of Columbia," he claimed. He also argued that at the very least, contrary to the district court's granting of the motion to dismiss without discovery, he was entitled to jurisdictional discovery to uncover further information about Ameritrade's contacts with the district. Meanwhile, Ameritrade contended that the plaintiff was not entitled to jurisdictional discovery. It acknowledged that it derived revenue from electronic transactions with district residents, but claimed that such transactions do not occur in the district. Instead, Ameritrade argued that its business transactions occur "in the borderless environment of cyberspace."

The court rejected Ameritrade's argument, stating that traditional notions of personal jurisdiction have adapted to other changes in the national economy, and,

therefore, they can adapt to changes brought on by the Internet. " 'Cyberspace' ... is not some mystical incantation capable of warding off the jurisdiction of courts built from bricks and mortar," the court said.

Finding no logical reason to distinguish transactions made by mail and telephone, which have served as the basis for the assertion of personal jurisdiction without actual presence in a forum, from transactions conducted via e-mail or an interactive website, the court said it would apply the traditional test of jurisdiction: whether Ameritrade's contacts were "continuous and systematic."

Relying on *GTE New Media Services Inc. v. Bell South Corp., 199 F.3d 1342 (D.C. Cir. 2000),* Ameritrade argued that Internet-based transactions fall outside the jurisdiction of the D.C. courts. The court, however, said that the defendant misread that case.

Website Was Not Passive

In *GTE*, the court held that defendants who operated Internet Yellow Pages Web sites accessible to district residents lacked sufficient contacts for D.C. courts to assert jurisdiction. The D.C. residents, however, did not engage in business transactions with the defendants, rather, they engaged in transactions with businesses found in the Yellow Pages, the court said.

The instant case is distinct from *GTE* because Ameritrade's contact with the district is not limited to an "essentially passive" website that customers merely access for information. "To the contrary, Ameritrade concedes that District residents use its website to engage in electronic transactions with the firm," said the court. "As a result of their electronic interactions, Ameritrade and its District of Columbia customers enter into binding contracts." In addition, such transactions can take place 24 hours a day on Ameritrade's website, the court said, making it possible for the defendant to have "continuous and systematic" contacts "to a degree that traditional foreign corporations can never even approach." D.C. courts, therefore, could have asserted jurisdiction over Ameritrade if service of process on the defendant had been sufficient.

Judges Karen LeCraft Henderson and Stephen F. Williams concurred in the decision.

UNITED STATES

■ NO JURISDICTION OVER OUT-OF-STATE ISP

ALS Scan Inc. v. Digital Service Consultants Inc. (Case No. 01-1812)

U.S. Court of Appeals for the Fourth Circuit, June 14, 2002

A court may not exercise specific jurisdiction over the out-of-state Internet service provider who provided service to an alleged copyright infringer when the ISP's only contact with the state was through its own passive website, the U.S. Court of Appeals for the Fourth Circuit ruled June 14. In a question of first impression in the Fourth Circuit regarding whether electronically transmitting or enabling electronic transmission over the Internet into Maryland could be the basis for an exercise of personal jurisdiction, the court also declined to rule that general jurisdiction over a party may be based only on electronic transmissions into the state.

The plaintiff, ALS Scan Inc. of Columbia, Md., was a producer of adult-oriented photographs which Internet users could view at its website, *www.alsscan.com*. ALS Scan charged that defendants Alternative Products Inc. and Robert Wilkins violated ALS Scan's copyright in hundreds of photographs by placing them on Alternative Products's sites, *www.abpefarc.net* and *www.abpeuarc.com*. The plaintiff also brought suit against Alternative Products's ISP, Digital Service Consultants Inc. of Atlanta, charging that Digital enabled the infringement by the other defendants. First ruling that the Maryland long-arm statute permitted any exercise of jurisdiction that did not violate the U.S. Constitution, Judge Paul V. Niemeyer turned to the analysis under the due process clause.

Minimum Contacts Requirement Not Met

International Shoe Co. v. Washington, 326 U.S. 310 (1945), held that the due process clause requires that any exercise of personal jurisdiction over a foreign defendant comport with traditional notions of fair play and substantial justice. In the case of specific jurisdiction, *Helicopteros Nacionales de Columbia SA v. Hall, 466 U.S. 408 (1984)*, set forth a three-part minimum contacts test:

- the defendant's contacts with the forum state must constitute a purposeful availment of the privilege of conducting business in the forum state;
- the claims must arise out of these contacts; and
- the exercise of jurisdiction must be constitutionally reasonable.

The court applied this test using the sliding scale set forth in *Zippo Manufacturing Co. v. Zippo Dot Com Inc., 952 F. Supp. 1119 (W.D. Pa. 1997),* finding that Digital's electronic transmissions into Maryland were passive and that it did not avail itself of the privilege of operating in Maryland."Digital functioned from Georgia as an ISP, and in that role provided bandwidth to Alternative Products, also located in Georgia, to enable Alternative Products to create a website and send information over the Internet," the court said. "It did not select or knowingly transmit infringing photographs specifically to Maryland with the intent of engaging in business or any other transaction in Maryland." Digital's website itself had no connection with the infringement claim and therefore could not form the basis of an exercise of specific jurisdiction, the court said.

COMMENTARY

POLAND

Poland Gears Up For E-Commerce

By Jerzy Gawel, a doctoral student at Vienna University, and Pawel Litwinski and Marek Swierczynski of Traple, Konarski, Podrecki Law Office, Krakow; e-mail: pawel.litwinski@traple.pl; marek.swierczynski@traple.pl

Poland has recently worked intensively to set legal standards for electronic commerce. Legislation has harmonized European Union requirements and international standards, *i.e.*: the UNCITRAL model law, guidelines prepared by the OECD, WTO and other organizations. On July 14, 2000, the Polish Parliament adopted a resolution establishing parameters for the development of an information society in Poland. According to the resolution, national authorities are obliged to prepare legal regulations concerning electronic commerce, including electronic documents and signatures, information security, cryptography, data protection, electronic contracts and service providers' liability. Generally the changes in Polish law are in accordance with E.U. directives. Laws that bring Poland closer to integration with the European Union are treated by the Polish Parliament with special care and priority and establishing legal standards for electronic commerce is also covered by this special legislation procedure. This guarantees a rapid implementation of new provisions and prevents the adoption of regulations that do not comply with the European standards. However, many model Acts have to be changed subsequently, to be consistent with Polish law and to maintain integrity within the Polish legal system.

Electronic Signatures

The Law on Electronic Signatures enacted on July 27, 2001 will come into force on August 16, 2002. It implements E.U. Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999 on a Community framework for electronic signatures. The purpose of the new Act is to facilitate the use of electronic signatures and to contribute to their legal recognition. It also establishes a legal framework for electronic signatures and certification services. The new law establishes an European principle of equal status for electronic and handwritten signatures. However, the possibility of using the electronic equivalents of documents with the use of electronic signatures is excluded in some cases. Data in electronic form with a secure signature (signatures that fulfil requirements similar to the advanced electronic signature in the E.U. directive), and based on a valid, qualified certificate, have equal legal status with documents with handwritten signatures.

The written form for specific acts in law is required by many provisions of the Polish Civil Code. The most significant is Article 75 of the Code, which states that an act in law, including the disposition of a right or obligation to perform in excess of 2000 PLN (approximately 500 euros) shall be confirmed in writing. Any such act not confirmed in writing is still legally valid, but there are specific limitations of evidence in civil procedure provisions. In the case of contracts exceeding this value, and contracts which are concluded by electronic means without satisfying the aforementioned requirements, parties are limited to proving the existence and conditions of such contract. The contract is still legally valid but it encounters evidence limitations, namely, that proof from witnesses or examination of the parties is not admissible.

The new law will amend Article 60 of the Civil Code to admit expressing the intentions of a person in an electronic way. However, this amendment has been widely criticized. Currently Article 60 states that a declaration of intention is acceptable in any form, if such intent is expressed clearly. Therefore, an electronic form if readable and clear is already included in the provision.

Secure electronic signatures will be applicable in all situations where particular legal provisions require a written form, unless a specific clause states otherwise.

The Polish law on electronic signatures conforms with the E.U. directive. A secure electronic signature (equivalent to an advanced electronic signature as defined by the E.U. directive) is equivalent to a handwritten signature if:

- it is uniquely linked to the signatory;
- it is capable of identifying the signatory;
- it is created using means that the signatory can maintain under his sole control;
- it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;
- it must be based on a qualified certificate;
- it must be created by a secure signature creation device.

Certification Services

The law on electronic signatures will come into force nine months after its publication in the State Gazette. The purpose of a long *vacatio legis* is to ensure the creation of a safe infrastructure for certification services. Until now there are a few companies developing systems of electronic signatures certification. They work in accordance with foreign certification service providers resulting in mutual recognition of certification. At present, because Poland is not an E.U. member, this is the only way to provide a legal recognition of certificates issued in Poland in the E.U. and other countries. The same rule governs the recognition of foreign certificates in Poland.

In principle, no prior authorization is required for the establishment of a Certification Service Provider. The supervisory office is the Ministry of Economy. Under

certain conditions, which are stipulated in the Act, the Ministry has the power to suspend a Certification Service Provider. On the other hand, the National Bank of Poland or its subsidiary company will have influence as to which companies will be allowed to issue qualified certificates. Foreign Certification Service Providers, *i.e*,. those from the European Union, may be interested in establishing branch offices in Poland.

The Act not only gives equal status for electronic and handwritten signatures but also allows the replacement of qualified written form by an advanced electronic signature with time stamp.

Consumer Protection On The Internet

The Law on protection of certain rights of consumers and liability for damage caused by dangerous products was enacted on March 2, 2000, implementing the four E.U. consumer directives: 85/577, 97/7, 93/13 and 85/374, dealing with different aspects of consumer protection, which form the basis for consumer protection law.

The new law came into force on July 2, 2000. The law amends the Polish Civil Code by adding provisions which protect the consumer from abusive clauses in general contract conditions and establish responsibility for dangerous products. On the other hand, provisions protecting the consumer in distance contracts and in contracts concluded outside of business premises remain outside the Polish Civil Code in a separate legal Act. Provisions protecting consumer rights cannot be excluded by a contractual clause or by the choice of a foreign law.

Distance contracts are defined as "business to consumer" contracts. They are concluded without the simultaneous presence of both parties to the contract, using the means of distance communication. It is the act in law that leads directly to the conclusion of the contract that shall be concluded using the means of distance communication. The term "consumer", in contradiction to Directive 97/7, has very extensive scope and means any person who acts in a purpose not directly connected with his business activity. Consequently, it covers not only natural persons but also legal persons.

Sending an offer by certain means of distance communication (fax, e-mail and telephone) is acceptable only after the prior consent of the consumer. This provision protects consumers against receiving unwanted offers and potentially forms the legal basis for claiming damages for the sending of unsolicited commercial e-mail.

Obligations of the parties

The seller in distance contracts is obliged to provide full information to the consumer, which includes informing the consumer about the identity of the supplier, the main characteristics of the goods or services, and the price together with all applicable taxes and duties, etc. He is also obliged to confirm this information in a written form after concluding the contract. The consumer has the right to withdraw from the contract within 10 calendar days from the delivery of the product or from the moment the performance of services has begun, although there are some exceptions to the right of withdrawal. If the seller does not inform the consumer in a written form about his right to withdraw, the term is extended to the period of three calendar months. The law introduces the "first supply, then payment" rule and consequently every contractual provision which obliges the consumer to provide payment prior to the performance of the contract by the seller will be null and void.

The general terms and conditions of the consumer contract bind a consumer if they are provided to him at the moment of or before conclusion of the contract. The standard form must be clear and comprehensible. Any doubts shall be construed in favour of the consumer. It must be mentioned that the recent Article 385 §3 of the Civil Code enumerates 23 abusive/unfair clauses. From the abusive clauses enumerated in the Civil Code, a few have special importance for electronic commerce contracts. The most important of these are:

- the provision prohibiting exclusion or limitation of the consumer's right to take legal action or exercise any other legal remedy, particularly by requiring the consumer to take disputes exclusively to arbitration not covered by legal provisions; and
- the provision which prohibits giving the seller the right to determine whether the goods or services supplied are in conformity with the contract.

Despite the aforementioned regulations, there is still a need to improve the level of consumer protection in other areas including on-line financial services, in accordance with the E.U. directive on distance marketing of consumer financial services.

Electronic Payment Instruments

Drafting of an Act on electronic payment instruments is now the subject of a special parliamentary commission's work as a stage of the legislation process. The Act implements the Commission's recommendation 97/489/EC of July 30, 1997, concerning transactions by electronic payment means. In particular it addresses the relationship between issuer and holder and certain E.U. directives on electronic money. Additionally, it incorporates the provisions of Directive 2000/46/EC and Directive 2000/29/EC on the taking up, pursuit of, and prudential supervision of the business of electronic money institutions.

The means of electronic payment, which enable the holder to effect transactions by electronic means of communication, shall include a payment card, electronic money instrument or any other instrument enabling the electronic identification of the holder. Such means allow direct access to the customer's account, telephone- and home-banking applications. There are exceptions, of which the most significant is that the law does not apply to cheques.

The draft law sets the minimum requirements necessary for an adequate level of consumer protection. It also regulates the process of issuing electronic money, stating that the issuers of electronic payment means can be banks or persons who have concluded an agreement with a bank on performing obligations by electronic money instruments.

The draft law stipulates obligations for the terms, conditions and use of electronic payment means, as well as the liabilities of all the parties taking part in the payment process. According to Article 16 of the draft law, payment performed by payment card is irrevocable. However, the

consumer's liability for the damage as a consequence of instrument theft is limited to 150 EUROS provided there was a proper bank notification. In exchange, the holder is obliged to keep his electronic payment instrument safe.

Liabilities of the parties

The draft law describes in detail the liability rules for the parties to the contract. The cardholder is responsible for losses as a consequence of improper card usage. Again liability is limited to 150 EURO, except in the case of purposeful fraud. The holder is not liable in cases where payment instruments have been used without physical presentation or electronic identification or signature by the holder at the debt document. Use of the identification code in order to identify the holder is not sufficient to establish the holder's liability. However, according to specific rules, the holder is liable for operations completed on the Internet, even though the payment card was not physically presented. This provision is commonly criticized as an obstacle to building consumer confidence on the Internet.

Electronic banking services

The third chapter of the draft law regulates electronic banking services such as home- and telephone-banking systems, which are currently becoming very popular in Poland. The draft includes provisions about obligatory information which has to be provided by the bank and principles of rendering electronic banking services. The holder bears responsibility for all transactions done by himself and by the persons to whom he has disclosed the software for the secret access codes.

The draft also regulates the principles of issuing and using electronic money. The term "electronic money" has recently been defined by an amendment to the banking law. The draft provisions give the same legal status to electronic money as to traditional money. According to the proposal, "electronic money instrument" shall mean an electronic device on which value units are stored electronically, in particular the reloadable stored-value card or hard disk of a personal computer. This special payment means shall include a mechanism which does not allow storage units to exceed 150 EUROS. The draft law regulates the provisions which are the subject of incorporation in the contract between holder and issuer. The issuer of electronic money bears legal responsibility in case of a malfunction of hardware or software provided by him. This liability cannot be limited by the contract between the issuer and the holder.

According to the Act, not only banks are allowed to be issuers of electronic money.

A final provision enables issuers to exchange information, *i.e.*, client's personal data, in cases of a fraudulent use of electronic payment instruments. The draft in its present form was previously rejected by the Polish Parliament because of doubts concerning the banking privileges. However, the future Act will most probably be based on the same rules as presented above.

Electronic Services Under Special Surveillance

The draft Act on rendering services electronically is currently the subject of the legislative procedure in the Polish Parliament. According to distinguished Polish professors of law who are the authors of the draft, it will provide the legal basis for supplying tele-information services and the conduct of electronic commerce.

The Act also regulates the liability of intermediary service providers for unlawful on-line content, differentiating between mere conduit, caching, or hosting services. The Act also regulates the rules of personal data protection and will implement Directive 2000/31/EC concerning legal aspects of information society services, in particular electronic commerce.

New provisions are badly needed because of legal uncertainty with respect to service providers' activity. The law sets out the general framework for these kinds of services, referred to as tele-information services, and covers the scope of economic activities taking place on the Internet.

Tele-information services shall be available to the public. However, a few exceptions exist. The law does not apply to electronic mail or the equivalent means of individual communication, but addresses only business activity.

The service provider is obliged to inform the consumer about his name, address, the supervisory body, number in commercial register, the various steps to conclude the contract, technical means for identification of provider, etc. For particular activities, additional information may be necessary. The information has to be given in a clear, comprehensible way.

According to the new provision a commercial offer has to be identified as such. Additionally, the natural or legal person sending a commercial offer must be clearly identified. Similar rules concern discounts, premiums, gifts, promotional competitions and games.

The draft law chooses the opt-in model, which does not allow the sending of unwanted offers. To ensure compliance with the anti-spam regulation, the draft provides a fine for violation of the presented opt-in model. Consequently, sending unsolicited commercial e-mail will be treated by the draft as a criminal offence.

Data protection

The draft law's personal data protection provisions are based on the German Teleservices Data Protection Act. The choice of the German law as a model for the Polish legislation has widely been criticised, due to the fact that German law does not comply with the project of the Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector. As a consequence of the debate, the personal data protection provisions are likely to be excluded from the Act on rendering services in electronic ways and will be amended in accordance with the proposed Directive.

Advertisements On The Internet

There are no special provisions concerning advertisements on the Web. However, the existence of prohibitions on the advertisement of certain goods such as tobacco, alcohol (with the exception of beer from September 14, 2001) or drugs on prescription, gives lawyers the opportunity of finding loopholes in the existing law. The advertising of other activities like gambling, securities

and financial institutions is also subject to certain legal limitations.

Individual communication on the Internet is not subject to limitations. Specific electronic means of communication such as electronic mail, instant messages and SMS are beyond the scope of the prohibitions. According to the Polish law an advertisement is a public transmission. Consequently, personal communication on the Internet is not considered to be an advertisement.

No Changes On Domains

The Research and Academic Computer Network—NASK (*www.nask.pl/english/*) conducts domain registration in Poland. NASK is the entity managing the domain register in the ***.pl*** domain, some functional domains and regional domains. To register the domain it is necessary to send the electronic Registration Application Form correctly, which is available from NASK's home page. The registration of a ***.pl*** domain is possible only through NASK, with filing of a petition, filling in the application form and enclosing a fee. Registration is based on a "first come, first served" rule but according to Article 4.1 of the NASK internal regulations, NASK refuses registration where there is an identical existing domain. The user may register only such name to which he is entitled. NASK is not able to check names and requires the statement of filing to be correct.

The transfer of domain names is possible. A special form must be prepared. NASK refuses registration of regional names such as *Gdansk.pl* following the German case *Heidelberg.de.* The exclusions from registration involve registered trademarks and the unfair competition practices.

Summary

Polish civil law, in particular contract law, has been firmly established for generations and legislation concerning electronic commerce is being incorporated smoothly. In addition, Polish laws are adapting to E.U. standards and directives. The process at this stage is very advanced and will undoubtedly become a part of the longstanding tradition of Polish legal culture.

■ ITALY

Electronic Money: The New Italian Rules

By Avv. Alessandro del Ninno of the Information and Communication Technology Department of Studio Legale Tonucci, Rome (www.tonucci.it); e-mail: adelninno@tonucci.it

The "EC Law" is a particular legislative technique used by the Italian legislature: it is an annual, comprehensive law which registers the E.U. Directives directly implemented by this Act or to be implemented by successive legislative decrees to be enacted by the Italian Government within one year starting from the entering into force of the EC Law. This Register provided by the EC Law for the year 2001 includes the Electronic Commerce Directive 2000/31/EC, the E.U. Directive 2001/29/EC about certain aspect of Copyright in the Information Society (both to be implemented by a successive Legislative Decree), and the Electronic Money Directives 2000/46/EC and 2000/28/EC.

The "European Community Law for 2001"—recently adopted by the Italian Parliament with the Law of March 1, 2002, No. 39 (published in the Italian *Official Journal* of March 26, 2002 No. 72)—provides (in Articles 55 and 56) the definitive and direct implementation of the Electronic Money Directives 2000/46/EC and 2000/28/EC by amending the Consolidation Act 385/1993, the legislative text which collects all the Italian laws about the credit and banking sector.

New Definitions

According to the new Italian rules, new definitions have been added with regard to those who deal with financial, credit or banking activities. For example, an "electronic money institution" shall mean companies, other than the banks, which issue electronic money. On the other hand, "electronic money" shall mean a monetary value as represented by a claim on the issuer which is:

(i) stored on an electronic device;
(ii) issued on receipt of funds of an amount not less in value than the monetary value issued;
(iii) accepted as means of payment by undertakings other than the issuer.

Banks and electronic money institutions can be the only subjects qualified to issue electronic money. The electronic money institutions can only carry out the activity of issuing electronic money by means of an immediate transformation of the funds received. Within the limits provided by the Italian Central Bank, the electronic money institutions can further carry out activities strictly connected or linked to the electronic money-issuing activity. They can also supply payment services. In any case, such institutions cannot supply, in any form, grating credit activities.

Central Bank to Keep Register

The Italian Central Bank shall insert in a proper Register the Italian electronic money institutions and the secondary branches in Italy of those electronic money institutions with main offices in an E.U. or extra-E.U. member state.

A bearer of electronic money may ask the issuer—according to the specific conditions provided in the related contract—to redeem it at par nominal value of the electronic money in coins and bank notes or by a transfer to an account free of charges other than those strictly necessary to carry out that operation. The contract may stipulate a minimum threshold for redemption. The threshold is provided by the Italian Central Bank in compliance with the Communitary discipline of the sector.

The Italian Central Bank shall authorize the electronic money institutions to carry out the related activities according to the conditions set forth in Article 14, paragraph 1 of the C.A. 385/1993:

(a) they must be a joint-stock company, a joint-stock limited partnership company, a limited liability company or a co-operative company;

(b) their main office and the managing direction must be in the territory of Italy;

(c) their capital stock must be not inferior to the level decided by the Italian Central Bank;

(d) they must present a specific programme related to the initial activity, as well as the Statute and the articles of association;

(e) the capital stock shareholders must have honourability requirements;

(f) the subjects who carry out administrative, direction and control activities must have specific honourability requirements as provided by Article 26 of CA 385/1993.

There is a prohibition on the existence of strict connections between the electronic money institution or the subjects who belong to it and other subjects in order to avoid any kind of evasion of the effective exercise of surveillance activities.

Bank May Refuse Authorization

The Italian Central Bank shall deny authorization to the electronic money institutions if the correct and prudential management of the related activity shall not be guaranteed according to the conditions above-mentioned.

Further, the Italian Central Bank shall regulate the authorization procedure as well as cases of withdrawal of the authorization when the authorized electronic money institution has not started the activity.

In addition, subjects who, by means of controlled companies, carry out relevant entrepreneurial activities in sectors other than the banking or financial field cannot be authorized to acquire quotations or shares so that their participation exceeds 15 percent of the capital of the electronic money institution concerned. The Italian Central Bank shall deny or revoke the authorization in the presence of agreements (of any kind) from which a relevant concentration of powers can derive for the subject above-mentioned. The concentration of powers must regard the power to appoint or revoke the majority of the administrators of the electronic money institution in prejudice of a correct and prudential management of the electronic money institution itself.

Italian electronic money institutions may operate:

- in an E.U. member state, even if a secondary branch is not established there, according to the specific procedures set up by the Italian Central Bank;
- in an non-E.U.member State, even if a secondary branch is not established there. A prior authorization given by the Italian Central Bank is compulsory.

The Italian Central Bank can establish, in the interests of prudence, a maximum limit to the nominal value of the electronic money. Further, the Italian Central Bank shall enact proper provisions to favour the development of electronic money, to promote the regular working of the whole sector and to guarantee the electronic money's reliability.

Exemptions

The Italian Central Bank may exclude electronic money institutions from the application of the rules related to the authorization above when one or more of the following conditions are satisfied:

- the comprehensive amount of electronic money issued by the electronic money institution does not exceed the maximum limit established by the Italian Central Bank in compliance with the E.U. discipline of the sector;
- the electronic money issued by the electronic money institution is accepted in payment exclusively by subjects controlled by the institution who carry out operational functions or any other accessory functions connected with the electronic money issued or distributed by the electronic money institution, by subjects controlling the issuer institution or by other subjects controlled by the same controlling subjects;
- electronic money issued by the electronic money institution is accepted in payment only by a limited number of companies, identified on the basis of their location or on the basis of their strict commercial or financial relationships with the electronic money institution.

To obtain the exemption above mentioned, the contractual agreements must provide a maximum limit to the nominal value of the electronic money at the disposal of each client, that limit not to exceed the maximum limit established by the Italian Central Bank in compliance with the E.U. regulation of the sector.

Electronic money institutions exempted according to the above conditions shall not benefit from the rules related to the "reciprocal recognition" procedures.

Sanctions for Non-Compliance

Finally, with regard to the sanctions to be applied in cases of violation of the legal framework, it must be pointed out that whoever issues electronic money in violation of the above rules or without being included in the Register of electronic money institutions set up by the Italian Central Bank shall be liable to imprisonment for from six months to four years and to a penalty ranging from EUROS 2,066 to EUROS 10,329.

The use of the words "electronic money" (in Italian or in any other foreign language) in any kind of communication to the public or in any distinctive sign is prohibited for subjects others than banks or electronic money institutions. Use of the words "electronic money" or of any other word or phrase is prohibited if aimed at deceiving the public with regard to the entitlement of the subject to issue electronic money.

The Italian Central Bank and the Italian Foreign Exchange Office can report to the competent Public Prosecutor eventual suspect activities carried out by subjects who carry on the activities of savings gathering, banking, financial or issuing of electronic money. Further, it must be pointed out that also that the electronic money institutions are subject to the Italian laws related to prevention of the use of the financial system for the purpose of money-laundering.

■ INTELLECTUAL PROPERTY

Proposed Expansion of WIPO Mandate To Cover Additional Domain Name Disputes

GENEVA—The United States has expressed opposition to a proposal from the World Intellectual Property Organization (WIPO) to expand a global mandate for dealing with disputes over the registration of Internet domain names in order to manage disputes involving country names and the names of international organizations.

Officials who attended a May 21–24, 2002, special session of WIPO's Standing Committee on the Law of Trademarks (SCLT) to discuss the issue said the United States was almost alone in opposing the WIPO secretariat proposal. The SCLT nevertheless agreed to recommend adoption of the proposal at the next annual meeting of WIPO's governing body scheduled to take place from September 23 to October 1.

On September 3, 2001, WIPO's secretariat issued a report proposing that a system for resolving Internet domain name disputes similar to the Uniform Dispute Resolution Policy (UDRP) be considered for disputes involving issues other than trademark infringement. WIPO suggested that the UDRP be modestly expanded to deal with conflicts involving the registration of names for international inter-governmental organizations (IGOs) and that the organization should work with the World Health Organization to establish a mechanism prohibiting the domain name registration of internationally recognized generic medicines.

WIPO said, however, that the diversity of national legal approaches regarding the protection of personal names precluded the extension of the UDRP to such disputes at this stage. It also said the UDRP should not be applied to domain name disputes involving geographic indications and trade names, arguing that the international rules for protecting such names need to be further advanced before such disputes can be tackled in cyberspace. In a special session held November 29–December 4 to discuss the report, the SCLT expressed some reluctance to expand the UDRP to domain names for IGOs. WIPO officials said some members opposed a straightforward UDRP-type system, in which arbitration decisions can be challenged in national courts, because of the immunity IGOs enjoy in national courts.

Widespread Support for Change

The latest special session, however, showed widespread support for a compromise proposal drafted by United Nations legal advisers. Under the compromise, any appeal against a UDRP decision involving an IGO would be handled by a neutral international arbitration panel, thus preserving the immunity of IGOs in the national courts. The United States was the only participant at the special session to voice its opposition to the compromise. U.S. officials had earlier argued that many of the problems encountered by IGOs seem capable of being resolved through informal discussions with domain name registrants and that it was questionable whether the problem was of such a magnitude that it needed to be addressed through the UDRP.

The first SCLT session also revealed general support among participants for the idea of establishing a mechanism to tackle the abusive registration of country names, despite an initial WIPO secretariat recommendation against such a move. The United States, Canada, and New Zealand argued against such protection, citing insufficient evidence of abuse, sufficiency of existing national laws prohibiting the misleading use of country names, the freedom of expression, and the potential impact of the protection on fair use of geographical terms and established trademark rights.

Nevertheless, the SCLT agreed at its latest special session to propose the protection of country names under the UDRP. The committee agreed that protected country names would include the official as well as the short name of the country (*e.g.*, Federal Republic of Germany and Germany). The United States, Canada, and Australia voiced objections, officials said, arguing that country names, like other geographical names, are not intellectual property and thus do not merit special protection.

No Action on Drugs Issue

On other issues, the SCLT maintained its earlier opposition to the WIPO secretariat's call for the immediate creation of a mechanism to protect international non-proprietary names, including generic names of pharmaceutical substances. Officials said that a large number of delegations said there was not enough evidence supporting the need for such protection at this stage. The committee recommended that both WIPO and WHO continue monitoring the situation. A similar outcome emerged in regard to the protection of trade names on the Internet, officials said. No action was taken by the committee in regard to personal names, while on geographical indications delegations continue to be split between "Old World" countries advocating protection for such indications and "New World" countries maintaining their opposition.

NETWORK SECURITY

Information Systems Security Guidelines Being Revised to Be More User-Friendly

Revisions to the 1992 Organization for Economic Cooperation and Development Guidelines for the Security of Information Systems attempting to make the guidelines more user-friendly and accessible to the average computer user are expected to be released by September, members of the group charged with revising the guidelines told an information security workshop at the U.S. Federal Trade Commission May 21, 2002.

According to Orson Swindle III, an FTC Commissioner and head of the U.S. delegation to the OECD Experts Group conducting the review, the reason for revising the guidelines is to get across the point that everyone must be involved in the security of information systems.

Revisions Taking Internet Into Account

Agreeing with Swindle, Sarah Andrews, research director at the Electronic Privacy Information Center, said that the 1992 guidelines need to be updated to recognize the fact that computers are used by average individuals, not just programmers. They also need to focus on network security issues raised by the Internet that did not exist in 1992, Andrews told the FTC's Consumer Information Security Workshop.

Joseph H. Alhadeff, vice president for global public policy and chief privacy officer for Oracle Corp., agreed, saying that the new guidelines are trying to highlight that now—as opposed to ten years ago—you have to have a much larger focus on systems outside your own when dealing with security. He said that the guidelines "are trying to take a holistic approach so that you see yourself as part of the system," not as an island.

Alhadeff also said that the security guidelines attempt to be accessible to all participants from end users to technicians. He noted that security is not a one-size-fits-all solution, but rather solutions need to be tailored to the systems they are trying to secure. However, the guidelines discuss the "formative issues you need to think about," he said.

While it is not presumed that legislation will flow out of the guidelines, Alhadeff said that they were developed so that they could be useful to a wide array of people.

Swindle called the document "the boiling down of ideas" and said that prevalent in this, as always, is the tension between privacy and security. He noted, however, that we are never going to achieve perfect security, but will develop the best solution possible if representatives of government, industry, and the public interest continue to work toward that goal.

Need "Culture of Security"

In addition, "if we're going to have a 'culture of security' we have to start with the generation [that is starting to use computers now and] teach them about security," Swindle added.

The "culture of security" was a concept that Andrews discussed as well. She said that the main issue from EPIC's perspective is that a security solution be developed that is workable in a democratic society that represents other values. The three principles that she was most interested in were:

- raising individuals' awareness about what is involved in protecting security;
- ensuring that the different stakeholders know what their responsibilities are with respect to security; and
- ensuring that this security is protected within the bounds of a democratic society that respects individual rights, including the right to privacy, freedom of movement, and freedom of information.

The 1992 OECD Guidelines for the Security of Information Systems is available on the OECD's website at *www.oecd.org/EN/document/0,,EN-document-43-nodirectorate-no-24-10249-29,00.html.*