International Lawyer

Volume 39
Number 2 *International Legal Developments in Review: 2004*

Article 15

2005

Information Services, Technology, and Data Protection

Michael E. Burke

Demetrios Eleftheriou

Marco Berliri

Giulio Coraggio

Information Services, Technology, and Data Protection

Michael E. Burke, Demetrios Eleftheriou, Marco Berliri, and Giulio Coraggio*

Electronic transactions, data privacy, and dissemination of personal information are hot topics within the information technology community and the international community as a whole. More jurisdictions are putting e-commerce on near equal footing with written transactions. But the use of the Internet has come with a cost as corporations and governments have learned how to track our "electronic footprints." As a result of threats to our privacy from both government and private intrusion, attempts are being made to implement a more cohesive body of privacy law and to establish government policy that addresses the need for more comprehensive protection of privacy rights on the World Wide Web. In the past year, the governments of most developed, and many developing, nations introduced new legislation and regulatory guidelines dealing with a wide variety of Web-based privacy issues. That legislation covered e-commerce transactional information, spyware, emerging web-based telephonic communication, the breadth and scope of disseminated information obtained via the Web, and legal jurisdiction over the Web.

I. Asia: Electronic Information and Transactions—Legislation and Development of Government Policy

A. Hong Kong: Electronic Transactions (Amendment) Ordinance

In late June 2004, Hong Kong's Legislative Council enacted the Electronic Transactions (Amendment) Ordinance. This ordinance amends the *Electronic Transactions Ordinance* (Cap. 553) (the ETO) to enable recognition of forms of electronic signatures other than those generated through Public Key Infrastructure (PKI) technology. Recognition of these other

*Michael E. Burke is an Associate in the firm of Williams Mullen, Washington D.C. He specializes in International Economic Law Issues and Cross-Border Transactions; Demetrios Eleftheriou is an Associate in the firm of Willkie Farr and Gallagher, LLP, Washington D.C. Mr. Eleftheriou specializes in complex domestic and foreign e-commerce issues, including data protection and security matters; Marco Berliri and Giulio Coraggio are lawyers with Lovells in Rome, where they are members of the Technology Media and Telecommunications group.

electronic signatures, which may only be used in transactions that do not involve the Hong Kong government, is subject to conditions such as reliability, appropriateness, and consent of those involved. As such, the ETO is now technology-neutral in its recognition of electronic signatures, a posture consistent with the United Nations Commission on International Trade Law's (UNCITRAL) Model Law on Electronic Commerce.

The Electronic Transactions (Amendment) Ordinance makes other amendments to: (1) enable electronic service of documents on the Commissioner of Rating and Valuation; (2) amend the voluntary registration scheme for Certification Authorities (CAs) by requiring a qualified and independent assessor to assess the certification system's trustworthiness as a prerequisite to CA registration; (3) enable the Director of Information Technology Services to require recognized CA's to furnish an assessment report or statutory declaration of any major changes involving the CA that may occur between two annual assessments; and (4) transfer power to the Permanent Secretary for Commerce, Industry, and Technology (Communications and Technology) for making orders excluding the application of the ETO to electronic records and digital signatures.

B. Japan: Draft Guidelines for the Protection of Personal Data

In November 2004, the Japanese Ministry of Justice released draft guidelines covering entities that handle personal information and operate in the debt collection sector. These guidelines were released to assist such entities in complying with the Personal Information Protection Law, scheduled to come into effect on April 1, 2005. These guidelines require covered entities to: (1) specify the purposes for which personal data will be used; (2) specify whether such data will be provided to a third party; (3) develop adequate and appropriate internal data management systems; (4) obtain a subject's prior written consent before providing personal data to personal credit bureaus; (5) refrain from obtaining such consent through unfair pressure; and (6) not acquire or provide to any third party any "sensitive information" relating to a subject.[1]

C. Australia: Review of the Privacy Act

In October 2004, the Australian Federal Privacy Commissioner requested public input regarding the operation of the private sector provisions in the Australian Privacy Act 1998 (the Act). This public input determines whether the Act has succeeded in: (1) establishing a single comprehensive national scheme that regulates the collection, storage, use, correction, disclosure and transfer of personal information by private sector organisations; and (2) achieving this in a way that (i) meets Australia's international obligations relating to privacy; (ii) recognizes the interests of individuals in protecting their privacy; and (iii) recognises important human rights and social interests that compete with privacy.

Australia's Attorney General requests the public input data by March 31, 2005. Related to this process, in mid-2004, Karen Curtis replaced Malcolm Crompton as Australia's Federal Privacy Commissioner. As reported in the October 2004 edition of BNA's World Data Protection Report, Ms. Curtis has indicated that she may take a softer approach to enforcement under the Act.

1. Privacy Newsletter, *Japanese Government releases draft guidelines for protection of personal data in debt collection sector, at* http://www.bakernet.com/newsletters/article.asp?articleid=5334(Dec. 2004).

D. Taiwan: Tougher Data Protection?

As reported in the October 2004 edition of BNA's World Data Protection Report, the Taiwanese Cabinet has approved a new draft law on data protection that entrusts local governments to implement such regulation. Further amendments to the Computer-Processed Personal Data Protection Law extend that law's coverage to include data held in other locations than on computers, and also increase the penalties for unlawfully releasing personal information for commercial gain.

E. People's Republic of China: Electronic Signatures Law

In late August 2004, China's National People's Congress promulgated the Electronic Signatures Law (E-Signatures Law), which becomes effective on April 1, 2005.[2] The E-Signatures Law, China's first nation wide law addressing this issue, is both consistent with and broadly influenced by UNITRALIS Model Law on Electronic Commerce. The E-Signatures Law covers data messages, which are defined as any information generated, sent, received, or stored by electronic, optical, magnetic, or similar means. Subject to exceptions stated in article 3 of the E-Signatures Law, if parties to a document elect to use data messages, the document will not be invalid or unenforceable solely because of its electronic form. Further, a data message that is capable of tangibly representing its content and is accessible for use and investigation is deemed to be "in writing."[3] Article 14 of the E-Signatures Law provides that, subject to stated exceptions, a data message shall be deemed to be signed when affixed with a reliable electronic signature. Article 13 of the E-Signatures Law provides that an electronic signature is reliable if: (1) at the time the electronic signature creation data is used, it is proprietary to the electronic signatory; (2) at the time of signing, the creation data is controlled solely by the electronic signatory; (3) any change to the electronic signature after signing can be noticed; and (4) any change to the data message's content and form after signing can be noticed. But parties can specify reliability standards by contract that will be enforceable under the E-Signatures Law.

The E-Signatures Law also addresses issues and defines concepts such as (1) retention of data; (2) the admissibility and evidentiary weight of data messages; (3) dispatch of data messages; (4) receipt of data messages; and (5) location of dispatch and receipt of data messages. Importantly, the E-Signatures Law does not require a third certification service provider to independently validate electronic signatures. Under article 16 of the E-Signatures Law, however, an electronic signature certificate issued by a certification service provider, who meets a set of minimum standards as required by law, is deemed sufficiently trustworthy. These minimum standards are defined in article 17 of the E-Signatures Law. China's Ministry of Information Industry is empowered to license certification service providers, as well as promulgate administrative regulations on electronic signature certificates. The E-Signatures Law imposes liability on the certification service provider if a party suffers a loss based on that provider's electronic signature certification services.

2. GCA, *Electronic Signatures Law*, *at* http://gca.nata.gov.tw/eng/eslaw.htm (last visited Apr. 8, 2005).
3. *Id.*

II. United States and State Government Policies Regarding Dissemination of Information in E-Commerce and the World Wide Web

A. Spyware

Generally, spyware is a catchall term describing software that covertly gathers information about a user or a user's computer through an Internet connection, without the user's knowledge. Spyware can be downloaded onto a computer: (1) when a user actively downloads free software, such as games, peer-to-peer file sharing programs, or other programs that change or customize the user's browser; (2) by "drive-by downloads,"[4] such as when a browser's security setting is not set high enough to detect and/or prevent unauthorized downloads; or (3) by clicking on links within pop-up windows or spam. Spyware can cause computers to run slow, malfunction, or crash. Although some existing U.S. federal laws may be used to address the spyware problem, new bills were proposed in 2004 that apply directly to spyware. In October 2004, the House of Representatives passed two bills addressing spyware: the Securely Protect Yourself Against Cyber Trespass Act (SPY Act) and the Internet Spyware Prevention Act (I-SPY Act).[5] The SPY Act prohibits taking control of a computer, disabling antivirus software without authorization, and modifying a computer's settings. The I-SPY Act adds tough criminal penalties and makes it a crime to both intentionally access a computer without consent and to intentionally exceed consent to access a computer. Another bill, the Software Principles Yielding Better Levels of Consumer Knowledge Act (SPY-BLOCK Act), was also introduced in 2004.[6] The SPY-BLOCK Act generally prohibits surreptitious software installation and requires uninstall procedures for authorized software. While efforts to enact these proposals during the final "lame-duck" session of the 108th Congress failed, similar spyware legislation has been introduced in 2005.[7]

B. Phishing and Pharming

"Phishing" is a high-tech scam that uses e-mail or pop-up messages to lure unsuspecting victims into disclosing personal information. Criminals behind phishing attacks, referred to as phishers, send Internet users official-looking e-mails or pop-up messages that claim to have been sent by a familiar entity, such as a particular bank, government entity, or Internet Service Provider. The message usually states that a user needs to update or validate his or her account information by clicking on a particular link in the message. The link directs the user to a fake website with the same look and feel of the entity's website men-

4. Whatis.com, *Drive-by Download*, *at* http://whatis.techtarget.com/definition/0,,sid9gci887624,00.html(last visited Apr. 8, 2005).

5. Securely Protect Yourself Against Cyber Trespass Act, H.R. 2929, 108th Cong. (2004); Internet Spyware Prevention Act of 2004, H.R. 4661, 108th Cong. (2004).

6. Software Principles Yielding Better Levels of Consumer Knowledge Act, S. 2145, 108th Cong. (2004).

7. For updates on current laws or legislation addressing various technologies, including spyware, spam, phishing, pharming, and RFID, please visit the website of the Information Services, Technology, and Data Protection Committee, ABA Section of International Law: http://www.abanet.org/intlaw/committees/industries/information_services_technology/home.shtml [hereinafter Committee].

tioned in the message. At the bogus website, the user is asked to provide his or her personal information (e.g., name, address, social security number, telephone number, credit card number, bank account number, username, or password) in order to update or validate his or her account information. The user's personal information is then used by the phisher for fraudulent purposes.

"Pharming," also referred to as Domain Name System hijacking, is a similar scam. Pharming misdirects users to spoofed websites that mirror the real websites, where thieves harvest large amount of personal information. Even if a user enters the correct website address in the address field of a web browser, malicious software downloaded on the user's computer or hijacked servers send the user to a website that is the exact replica of the real website.

The number of phishing attacks has increased dramatically in 2004, particularly because of the use of "zombie" networks (discussed in more detail below). Existing laws addressing fraud criminalize phishing, but usually only after the damage has been done. In 2004, Congress failed to pass proposed legislation that directly targets phishing, which would have made it illegal to knowingly send fraudulent e-mails linking to fake websites with the intention of committing a crime.[8] Legislation targeting phishing and pharming was introduced in 2005 (the Anti-Phishing Act of 2005). This legislation allows prosecutors to impose fines of up to $250,000 and prison terms of up to five years. The Identity Theft Penalty Enhancement Act, signed into law by President Bush in 2004, increases penalties for identity-theft related crimes, which likely includes phishing and pharming.[9] Initiatives have been formed to fight this criminal activity, including BITS (a consortium of several large financial institutions) and the Phish Report Network (launched by several large companies, including Microsoft and eBay).[10]

C. Spam

The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM), which created the first U.S. federal law regulating commercial e-mail, took effect on January 1, 2004.[11] The definition of commercial e-mail under CAN-SPAM includes any "electronic mail messages with the *primary purpose* of commercial advertisement or promotion of a commercial product or service" (emphasis added).[12] In December 2004, the Federal Trade Commission (FTC) issued a final rule to facilitate the determination of whether the primary purpose of an e-mail is either commercial or non-commercial. The FTC's final rule outlines criteria for determining the primary purpose of various types of e-mails. E-mails are commercial if they contain only the commercial advertisement or promotion of a commercial product or service. For e-mails that have both commercial content

8. Anti-Phishing Act of 2004, S. 2636, 108th Cong. (2004).

9. Identity Theft Penalty Enhancement Act, Pub. L. No. 108-275, 118 Stat. 831 (2004).

10. *See* Committee, *supra* note 7.

11. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2004).

12. Jonathon Storper, Esq. and Billy Chan, Esq., *Controlling the Assault of Non-Solicited Pornography and Marketing (The CAN SPAM Act)*, Hanson, Bridgett, Marcus, Vlahos & Rudy, LLP, *at* http://www.hansonbridgett.com/newsletters/tips/tipsv41ssv41ss1.html(last visited Apr. 8, 2005).

and "transactional or relationship"[13] content (such as contacting users about their accounts, requested products or service, or product upgrades), the primary purpose is commercial if: (1) a recipient reasonably interpreting the subject line of the e-mail would likely conclude that the message is commercial; or (2) the "transactional or relationship" content is not at the beginning of the message. For e-mails that contain commercial, non-commercial, non-transactional, or non-relationship content, the primary purpose of the message is commercial if the recipient, reasonably interpreting the subject line or body of the message, would likely conclude that the message is commercial. Relevant factors include the placement of commercial content at the beginning of the message; the proportion of the message dedicated to the commercial content; and how color, type size, graphics, and style are used to highlight commercial content. E-mails will be deemed to have a "transactional or relationship" primary purpose if they contain only "transactional or relationship" content.

Even in light of CAN-SPAM, it has been reported that spam levels rose in 2004. The use of "zombie" networks has had a significant influence on the rise of spam worldwide. For example, certain malware that has been surreptitiously installed on your computer can convert your computer into a "zombie." Compromised computers are controlled by spammers through remote-control to send millions of unsolicited e-mails, which have contributed to the increasing amount of "phishing" attacks (discussed above).

The FTC published a Notice of Proposed Rulemaking in 2005 seeking comments on definitions and substantive provisions under CAN-SPAM, including: defining the term "person"; modifying the definition of "sender"; and shortening from ten (10) days to three (3) days the time to honor a recipient's opt-out request.[14]

D. Radio Frequency Identification

Although Radio Frequency Identification (RFID) has been around for decades, improvement in the technology has allowed it to proliferate dramatically in the past few years. RFID technology is essentially made up of two components: the actual RFID tag, which consists of an antennae and a microchip containing information about the tagged item, and a reader that activates or detects the antennae's radio signal. RFID tags, which can be as small as a grain of sand, can be used to keep tabs on items, animals or people. For example, RFID tags may be attached to shipping crates to keep track of goods shipped from the manufacturer to the retailer. RFID tags may also be attached to almost anything purchased, including clothes, electronics, and prescription drugs. RFID tags may also be implanted in animals to keep track of their whereabouts or in individuals in order to alert hospital employees of their medical background. For example, an RFID tag may be implanted under a person's skin, or inside a bracelet, to alert paramedics of a person's blood type or medical condition.

RFID technology raises privacy concerns because the technology involves the use of radio waves to share information. Critics of RFID are concerned that widespread application of the technology could potentially lead to misuse. For example, a retailer could track a customer's buying habits and use that information to barrage the customer with advertise-

13. Federal Trade Commission, The CAN-SPAM Act: Requirements for Commercial Emailers, *available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm (last visited Apr. 8, 2005).

14. *See* Committee, *supra* note 7.

ments. In addition, RFID devices implanted in individuals can store sensitive information that could be read by others without the individual's knowledge or consent. The U.S. Food and Drug Administration recently approved the use of RFID devices in humans.

The Opt Out of ID Chips Act, RFID legislation introduced in the House of Representatives in 2004, failed to make its way out of Congress.[15] This legislation would have made it an unfair or deceptive act or practice under the Federal Trade Commission Act to sell at retail a product containing an RFID device, unless: (1) the product has a conspicuous label stating that it contains an RFID capable of tracking the product and transmitting unique information before and after purchase; and (2) the label notifies the customer of the right to remove or permanently disable the RFID at the time of purchase.

Concerns over the use of RFID technology continue to be raised in 2005, some of which are raised in RFID reports issued by the U.S. GAO (Government Accountability Office) and the E.U.'s Article 29 Data Protection Working Party.[16]

E. Affiliate Sharing

The Fair Credit Reporting Act (FCRA) applies to both financial businesses that furnish and use information relating to consumer reports and to businesses that do not necessarily furnish or use such information. The Fair and Accurate Credit Transactions Act (Fact Act), enacted on December 4, 2003, makes significant and substantial changes to the FCRA, including establishing significant consumer protection standards addressing identity theft.[17] The Fact Act also adds an additional restriction with regard to information sharing among affiliates.

There are now *two* notice and opt-out requirements regarding affiliate sharing under the FCRA that run simultaneously, although they are distinct and serve two different purposes. Under the first notice and opt out requirement, the FCRA restricts the sharing of consumer report information among affiliates by requiring an affiliate to provide a consumer with both notice and the right to opt out of having their consumer report information shared with another affiliate. This opt-out requirement is currently in effect.

The second notice and opt out requirement, added by the Fact Act, applies in the context of disclosing information for marketing purposes. The Fact Act provision providing this notice and opt-out requirement will likely become effective sometime in 2005. This requirement covers a substantially broader amount of information, including a company's own transactions and experiences (such as non-consumer report information) with its customers. As a result of the Fact Act, transaction and experience information is deemed the equivalent of consumer report information for purposes of restricting information sharing among affiliates for marketing purposes. For example, before sharing experience, transaction, or consumer report information with affiliates for *marketing solicitation purposes*, consumers must be provided with a notice and a right to opt out of having such information shared with affiliates, absent the application of a Fact Act exception.

15. Opt Out of ID Chips Act, H.R. 4671, 108th Cong. (2004).

16. For more information on RFID and the GAO and Article 29 Data Protection Working Party reports discussing the technology, *see* Committee, *supra* note 7.

17. Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (2003).

F. Appointing a Chief Privacy Officer

President Bush signed a large spending bill, the Consolidated Appropriations Act, 2005 (CAA), into law on December 8, 2004.[18] Among other issues, the CAA requires each federal agency to have a chief privacy officer (CPO) and to hire an independent auditing firm to ensure that U.S. privacy laws are not being violated. The requirement of a CPO is also supported in the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004, which states that agencies with either law enforcement or intelligence functions should designate a privacy and civil liberties officer. The CPO of a federal agency will have primary responsibility for overseeing that agency's privacy policy.

In addition to other requirements, the CPO must assure that: (1) the use of technology sustains privacy protections concerning the collection, use, and disclosure of identifiable information, defined as information that permits the reasonable inference of identity of an individual to whom the information applies (Identifiable Information); (2) technologies used to collect, use, disclose, and store Identifiable Information allow for the continuous auditing of such information; and (3) protects Identifiable Information from unauthorized access, use, disclosure, disruption, modification, or destruction. By December 2005, each federal agency must establish and implement privacy procedures governing the agency's collection, use, disclosure, storage, and security of Identifiable Information. A federal agency must hire an outside consulting firm biennially to evaluate the agency's privacy procedures. Each independent third-party review must also be made available to the public.

III. E-Commerce Law and Case Law in the EU

A. Proposed Directive on the Patentability of Computer-Implemented Inventions

On December 21, 2004, the proposal of Directive on Software Patents[19] was removed from the agenda of the EU Council, which had been expected to finally approve it. After postponement of the final approval, the Directive will be re-examined in early 2005. Since 1999 the European Commission identified the patentability of computer-implemented inventions as one of the main issues to take action on as soon as possible, since the lack of certainty in that area posed a risk of damage to European industry. Under article 52(2)(c) of the European Patent Convention, computer programs cannot be regarded as inventions.[20] However, the Board of Appeal of the European Patents Office (the EPO) has interpreted that exclusion as limited to computer programs. Such interpretation has been directed at impeding only the patentability of computer programs lacking a technical character. The divergence of views between the EPO Board of Appeal and the National Courts[21]

18. Consolidated Appropriations Act, 2005, Pub. L. No. 108-447, 118 Stat. 2809 (2005).

19. Commission Proposal for a Directive of the European Parliament and of the Council 2002/0047 COD on the patentability of computer-implemented inventions, *available at* http://europa.eu.int/eur-lex/en/com/pdf/2002/en_502PC0092.pdf (Feb. 20, 2005).

20. Art. 52(2)(c), European Patent Office, *available at* http://www.european-patent-office.org/legal/epc/e/ar52.html (last modified March 2004).

21. Merrill Lynch's Application, [1989] RPC 561 (Apr. 21, 1989); Raytheon Co's Application, [1993] RPC 427 (Mar. 15, 1993).

required the harmonization of EU Member State legislation. The Commission's approach has been criticised by a number of commentators who maintain that the Directive will lead to the patentability of "all inventions that might reasonably be considered as within the realm of computer science."[22] Some scholars comment that the Directive's goal will damage the European market instead of helping it.

B. Proposed Directive to Prohibit Unfair Commercial Practices

On November 16, 2004 the Council of the European Union approved the Directive on Unfair Business-to-Consumer (B2C) Commercial Practices.[23] This Directive will introduce a new European framework regulating the aggressive and misleading B2C practices carried out both offline and online. The harmonization of EU Member State laws is expected to foster cross-border transactions within the European Union. In contrast, the current divergence among the varying Member State's legislation does not encourage consumers to trade with businesses based in a different Member State. Businesses established in different Member States are subject to laws that they often ignore or that provide them with a lower level of protection than laws in their home state. This issue is especially true for online trading. Moreover, the need to comply with varying Member State legislation also represents an additional cost for businesses.[24]

The Directive will prohibit unfair commercial practices able "to materially distort the economic behavio[u]r of consumers."[25] The proposal lists examples of unfair practices that include misleading and aggressive marketing practices. EU Member States will have to penalize traders involved in such practices with effective and proportionate measures that constitute a deterrent for infringers. The validity of contracts will be preserved. The Directive's purpose is to increase consumer choice, especially online, by persuading consumers, on one hand, to purchase goods from businesses established in different Member States, while on the other hand encouraging small businesses to trade on a cross-border basis.[26] As a result, competition throughout the European market is expected to be substantially enhanced. The European Parliament is expected to approve the Directive's final form in the first months of the 2005.

C. A Step Closer to an EU Discipline of VoIP

In June 2004, the European Commission began a public consultation on the treatment of Voice-over-Internet Protocol (VoIP) under the new regulatory framework set out in

22. Simon Davies, *The Proposed Software Directive: A User's comments*, 2003 J. Info. Law and Tech. 1, *available at* http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2003_1/davies/(July 4, 2003).

23. Commission Proposal for a Directive of the European Parliament and of the Council 2003/0134 COD concerning unfair business-to-consumer commercial practices in the Internal Market and amending directives 84/450/EEC, 97/7/EC and 98/27/EC (The Unfair Commercial Practices Directive), COM (2003) 356, *available at* http://europa.eu.int/eur-lex/en/com/pdf/2003/com2003_0356en01.pdf(June 18, 2003).

24. *Id.* ¶¶ 6-29 of Explanatory Memorandum.

25. *Id.* at 22.

26. Dep't of Trade & Indus., Consultation on a draft EU Directive COM (2003) 356, *available at* http://www.dti.gov.uk/ccp/consultpdf/unfaircon.pdf (July 2003) (containing the results of the Directive coming into effect).

2003's Framework,[27] Access,[28] Authorisation,[29] Universal Service,[30] and Privacy[31] Directives.[32] In early 2005, the Commission is expected to issue non-binding Guidelines that will have an impact on the approaches followed by Member State's national regulatory authorities. In both 1998[33] and 2000,[34] the Commission published notices on the possibility of VoIP as voice telephony, which would make it subject to the old regime's obligations. The Commission held, on that occasion, that VoIP could not be deemed as voice telephony since it was not separately offered to the public, but was merely an additional feature of the already offered browsers. Also, since it faced some delays, VoIP did not allow the transport of speech in real time.

The new regulatory framework aims to introduce a technology-neutral approach based on the distinction between Electronic Communications Service (ECS) and Public Available Telephone Service (PATS). Such a distinction is particularly relevant since it should allow VoIP providers to be considered as PATS. If VoIP providers are considered as PATS, they would be subject to a number of duties and obligations such as directory inquiry services and access to emergency services, including the availability of location information for authorities handling emergencies. The main concern if VoIP providers are PATS is the technical feasibility for VoIP providers to insure the provision of emergency services. To avoid the regulatory constraints that currently hinder further development of VoIP, the EU Commission's Consultation Document suggests removing VoIP from such obligations, instead making customers who use VoIP aware of the lack of availability of some features normally available through traditional voice telephony. This approach has been followed by Ofcom, the British NRA, in its Guidelines. Ofcom stressed the need to enhance competition and protect consumers by informing them of the impossibility of obtaining some services when using VoIP.

27. Council Directive 2002/21/EC of 7 March 2002 on a Common Regulatory Framework for Electronic Communications Networks and Services (Framework Directive), 2002 O.J. (L 108) 33, *available at* http://europa.eu.int/informationsociety/topics/telecoms/regulatory/new_rf/documents/l_10820020424en00330050.pdf (Mar. 7, 2002).

28. Council Directive 2002/19/EC of 7 March 2002 on Access to, and Interconnection of, Electronic Communications Networks and Associated Facilities (Access Directive), 2002 O.J. (L 108) 7, *available at* http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424en00070020.pdf (Mar. 7, 2002).

29. Council Directive 2002/20/EC of 7 March 2002 on the Authorisation of Electronic Communications Networks and Services (Authorisation Directive), 2002 O.J. (L 108) 21, *available at* http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424en00210032.pdf(Mar. 7, 2002).

30. Council Directive 2002/22/EC of 7 March 2002 on Universal Service and Users' Rights Relating to Electronic Communications Networks and Services (Universal Service Directive) 2002 O.J. (L 108) 51, *available at* http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/l_10820020424en00510077.pdf (Mar. 7, 2002).

31. Council Directive 2002/58/EC of 12 July 2002 concerning the Processing of Personal Data and the Protections of Privacy In the Electronic Communications Sector, 2002 O.J. (L 201) 37, *available at* http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/documents/l_20120020731en00370047.pdf (July 12, 2002).

32. Commission Staff Working Document on the Treatment of Voice Over Internet Protocol (VoIP) under the EU Regulatory Framework, *available at* http://europa.eu.int/information_society/topics/ecomm/doc/useful_information/library/commiss_serv_doc/406_14_voip_consult_paper_v2_1.pdf(June 14, 2004).

33. Status of Voice Communications on Internet under Community Law and, In Particular, Pursuant to Directive 90/388/ECC, 1998 O.J. (C 6) 4.

34. Status of Voice on the Internet under Community Law, and In Particular, under Directive 90/388/EEC, 2000 OJ (C 369) 3.

D. Consultation on the Application of the E-money Directive to Mobile Operators

On May 2004, the EU Commission launched a consultation paper[35] relating to the treatment of mobile operators with respect to the EU Directive on Electronic Money.[36] The problem arose when mobile operators started using pre-paid cards as a means for customers to purchase not only air time, but also other products such as videos, games, ring tones, and small value goods. By March 2003, the EU Banking Advisory Committee had already held that "the conditions for application of the E-Money Directive are met if a mobile user purchases third party products or services and pays for them with the electronic value stored on his pre paid card."[37] The consultation's goals are to define when the Directive applies to mobile operators; what regulatory and economic consequences its application will have on the parties involved; what solutions can better meet the need of fostering the development of such services; and which appropriate legal framework and safeguards should be adopted.

Currently, the E-Money Directive sets up burdensome constraints on e-money issuers who must ensure the redeemability of e-money. These issues are subject to minimum capital requirements and anti-money laundering obligations; they also cannot be involved in activities other than the issue of e-money.[38] Such obligations might be disproportionate to the small number of transactions carried out via pre-paid cards. Therefore, the EU Commission hopes to define, through the consultation process, the best approach for the short term, while also considering a possible future revision of the Directive to better suit the needs of these E-Money issuers. In 2005, the Commission is expected to prepare a Report on the application of the E-Money Directive in this context.

IV. Recent Case Law in the EU

A. English Courts and Online Defamation

In October 2004, the English courts issued two decisions regarding defamatory statements published on the Web. The first case, *Lennox Lewis v. Don King*, concerned two texts stored on websites based in California accusing boxing promoter Don King of anti-Semitic behaviour.[39] Under English law, the tort of libel is committed where the publication takes place, and each publication generates a separate cause of action. The Court of Appeal held that England was the forum conveniens in the case of material published on the web since it was the place where the material had been downloaded. The court stressed that the publisher should be aware of the "ubiquitous character of the medium" when he posts something on the web.[40] But the court added that this approach did not "propose a free-

35. Commission Directorate General of Internal Market Consultation Paper, Application of the E-money Directive to Mobile Operators, *available at* http://europa.eu.int/comm/internal_market/bank/docs/e-money/2004-05-consultation_en.pdf (last visited Jan. 11, 2005).

36. Council Directive 2000/46/EC on the Taking up, Pursuit of and Prudential Supervision of the Business of Electronic Money Institutions, 2002 O.J. (L 275) 39, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_275/l_27520001027en00390043.pdf (last visited on Apr. 7, 2005).

37. Commission Directorate General, *supra* note 35.

38. Council Directive 2000/46/EC, *supra* note 36.

39. Lennox Lewis v. Don King, [2004] E.W.C.A. Civ. 1329.

40. *Id.* at ¶ 31.

for-all for claimants libelled on the Internet" as courts will still have to consider the parties' connections with the forum.[41]

Richardson v. Schwarzenegger considers both the connections of parties to the forum and also sufficient connections based on the claimant's reputation in England.[42] The judge held that the court had jurisdiction over statements released by one of Schwarzenegger's spokespersons during his gubernatorial campaign and subsequently published such statements on the Los Angeles Times and on the Web. The mere forseeability of the statement being downloaded in England was sufficient to obtain English jurisdiction. These cases continue to leave uncertainty for website owners, increasing the possibility of multiple forums claiming jurisdiction.

B. Sui Generis Database Right, First Decisions by the ECJ

On November 9, 2004, the European Court of Justice (ECJ) issued its first four rulings[43] on the new database *sui generis* right introduced through the Directive 96/9/EC.[44] According to the ECJ, a database is any collection of works or data separable from one another without affecting the value (informative, literary, artistic, musical etcetera.) of their contents. The Directive distinguishes between databases showing creativity in their arrangement and selection and *sui generis* rights that article 7 grants to makers "of a database which shows there has been qualitatively and/or quantitatively a substantial investment in either obtaining, verification or presentation of the contents to prevent extraction and/or reutilisation of the whole or of a substantial part, evaluated qualitatively and/or quantitatively."[45]

The ECJ held that the investments in obtaining and verifying the contents of a database refers to the resources used to select, collect, and ensure the reliability of existing materials, not to the resources used for the creation of the contents of a database.[46] The ECJ also stated that in article 7 the expressions of "extraction" and "re-utilisation" had to be interpreted as referring to "any unauthorised act of appropriation and distribution to the public of the whole or part of the contents of a database."[47] As to what can be deemed to be a substantial part of a database "evaluated qualitatively and/or quantitatively"[48] whose extraction and/or re-utilisation amounts to an infringement, the court held that the former term refers to the investment in the obtaining, verification, or presentation of the database's illegally extracted and/or re-utilised contents, whereas the latter term concerns the volume of data extracted from the database and/or re-utilised. Finally, the court interpreted article 7(5), which prohibits "[t]he repeated systematic extraction and/or re-utilisation of insub-

41. *Id.*

42. Richardson v. Schwarzenegger, [2004] EWHC 2422 (QB).

43. The British Horseracing Board Ltd v. William Hill Org. Ltd, C-203/02 (2004); Fixtures Mktg. Ltd v. OY Veikkaus Ab, C-46/02 (2004); Fixtures Mktg. Ltd v. Organismos Prognostikon Agonon Podosfairou, C-444/02 (2004); Fixtures Mktg. Ltd v. AB Svenska Spel C-338/02 (2004) *available at* http://www.curia.eu.int/en/content/juris/index.htm (last visited Apr. 8, 2005).

44. Council Directive 96/9/EC of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 077) 20, *available at* http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31996L0009&model=guichett (Mar. 27, 1996).

45. *Id.*

46. The British Horseracing Board, *supra* note 43, at ¶¶ 23-42.

47. *Id.*

48. *Id.*

stantial parts of the contents of the database,"[49] as referring to acts whose cumulative effect is to reconstitute and/or make available to the public the whole or substantial part of the contents of the database.

C. Applicability of the Distance Selling Directive to Online Auctions in Germany

On November 3, 2004, Germany's Supreme Court[50] stated that eBay's German site is subject to the provisions of the Distance Selling Directive (DSD).[51] As implemented in Germany, the DSD recognises the consumer's right to withdraw from the contract without penalty and without giving any reason within fourteen days, if the item was purchased from a commercial seller. In this case, a jeweller had sold a diamond bracelet through eBay's German site to a customer who subsequently rejected the good since it did not meet his expectations. The customer asserted that he was entitled to return the bracelet under EU consumer protection rules. While the DSD does not apply to auctions, the Court held that eBay's internet auctions cannot be deemed pure auctions because of the peculiar role of the auctioneer, who does not have possession or control over the auctioned item. Indeed, on eBay the "the contract was concluded through the binding offer to sell made by the plaintiff and the acceptance of said offer by means of the highest bid made by the defendant."[52] Hence, there was no necessity for the auctioneer to take any action. Therefore the DSD, particularly the right to return goods, is applicable to B2C transactions carried out through eBay.

D. U.K. High Court Orders ISPs to Reveal the Identity of Twenty-Eight File Sharers to BPI

The U.K. High Court ordered a number of Internet Service Providers to disclose the identity of twenty-eight file sharers to the British Phonographic Industry (BPI).[53] BPI alleges that these "major filesharers"[54] are infringing the copyright of some of BPI's members by uploading and sharing music on peer-to-peer networks including KaZaA, Imesh, Grokster, Bearshare and WinMX. Particularly, BPI asserted the infringement of sections 16 and 20 of the Copyright, Designs and Patents Act of 1988. These sections reserve to copyright owners the exclusive rights to copy and disseminate their works to the public. In addition, section 20, enacted in 2003, implements the Directive 2001/29/EC, which har-

49. *Id.*

50. Robert W. Smith, *Germany's Federal Supreme Court Grants a Right to Revocation Regarding eBay-auctions*, Heise Online, *at* http://www.heise.de/english/newsticker/news52867 (Nov. 3, 2004). *See also* Statement by the Court (in German) *at* http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=pm&Datum=2004&Sort=3&nr=30710&pos=0&anz=126.

51. Council Directive 97/7/EC of 20 May 1997 on the Protection of Consumers In Respect of Distance Contracts, 1997 O.J. (L 144) 19, *available at* http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0007&model=guichett (June 4, 1997).

52. Smith, *supra* note 50.

53. British Pornographic Industry, *BPI to Sue "Major Filesharers"*, *at* http://www.bpi.co.uk/news/bizinfo/news_content_file_846.shtml.

54. *Id.*

monizes certain aspects of copyright and related rights in the information society.[55] This Directive considers as part of the right to communicate works to the public "the making available to the public of the work by electronic transmission in such a way that it may be accessed in a place and at a time individually chosen by the user."[56] According to some commentators, this language would catch "the actions of peer-to-peer music websites where the work is made available for members of the public to download at their convenience."[57] BPI's legal action is part of a rolling program of legal actions against major file sharers.[58] BPI believes that 15 percent of users are responsible for 75 percent of files shared on peer-to-peer networks. Through this program, BPI hopes to reduce the number of illegally shared music files.

55. Council Directive 2001/29/EC of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights In the Information Society, 2001 O.J. (L167) 10, *available at* http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_167/l_16720010622en00100019.pdf(May 22, 2001).

56. David Rose, *BPI wins right to know identities of UK file sharers*, World eBusiness Law Rep. (Nov. 4, 2004), *available at* http://www.worldcopyrightlawreport.com.

57. *Id.*

58. *Id.*