International Lawyer

Volume 40
Number 2 *International Legal Developments in Review: 2005*

Article 16

2006

Data Protection and E-Commerce in the United States and the European Union

Demetrios Eleftheriou

Marco Berliri

Giulio Coraggio

INDUSTRIES

Data Protection and E-Commerce in the United States and the European Union

DEMETRIOS ELEFTHERIOU, MARCO BERLIRI, AND GIULIO CORAGGIO*

I. In the United States

A. DATA INSECURITY

The past year was plagued by dozens of reported high-profile breaches in data security, resulting in over fifty million compromised personal data files. The most notable security breach instance involved ChoicePoint, one of the largest consumer data brokers in the United States. ChoicePoint initially reported that it allowed criminals posing as legitimate businesses access to personal data of around 145,000 individuals; this number later increased to 162,000.[1] ChoicePoint notified affected individuals of the data security breach, which was prompted in large part by a pioneering California law requiring consumer notification in the event of a breach in data security.[2] A more recent case involves CardSystems Solutions (a payments processor), which informed the public of stolen information affecting forty million accounts.[3] The CardSystems data security breach is the largest yet reported, compared to similar reports from financial institutions, retailers, academic institutions, and other entities. ChoicePoint settled with the Federal Trade Commission (FTC) in January 2006 for $15 million ($10 million in civil penalties and $5 million in consumer redress). CardSystems also settled with the FTC shortly thereafter. Both companies are required to implement a comprehensive information security plan and obtain audits by an outside third-party security professional every two years for twenty years.

The data insecurity instances of 2005 have triggered state and federal legislation addressing data privacy and security matters, including requiring entities to notify individuals in

*Demetrios Eleftheriou is a lawyer with Willkie Farr & Gallagher LLP in the firm's Washington, DC office and co-chair of the Information Services, Technology and Data Protection Committee of the American Bar Association Section of International Law. Marco Berliri and Giulio Coraggio are lawyers with Lovells in Rome, and are members of the Technology Media and Telecommunications group.

1. *See* ABC News, *Choice Point Warns Customers About Fraud*, Nov. 8, 2005, http://abcnews.go.com/Business/FinancialSecurity/wireStory?id=1293938.

2. *See* CAL. CIV. CODE § 1798.29 (West 2003).

3. *See* Jonathan Krim & Michael Barbaro, *40 Million Credit Card Numbers Hacked*, THE WASH. POST, June 18, 2005, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/06/17/AR2005061701031.html.

the event a breach in data security compromises their personal data. Many states have actually passed legislation that follow California's security breach notification law. In 2005, at least thirty-five states introduced security breach notification legislation and at least twenty-two states passed such legislation.[4] At the federal level, several bills addressing data security breach notification have been introduced in Congress, but none have become law.

Earlier in 2005, the Office of Thrift Supervision, Comptroller of the Currency, Federal Reserve System, and Federal Deposit Insurance Corporation jointly issued "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice."[5] The guidance document describes the appropriate elements of a response program, including customer notification procedures.

As reports of data security problems and identity theft continue to increase, data security practices and policies will likely be subject to increased scrutiny. Thus, businesses must ensure that they have appropriate security policies in place that protect their customers' personal data. Businesses that collect personal data should reevaluate the way they secure such data and ensure that they have implemented a comprehensive and well-articulated written data security policy. Procedures should be in place to regularly maintain, monitor, test, and update data security practices, including documenting and maintaining records of any unauthorized activity, and performing periodic penetration tests. A security policy should cover a broad array of applications and devices, including networks servers, workstations, switches, routers and web applications. In addition, firewall, encryption (to safeguard data while in storage and in transit), anti-virus, anti-spyware, intrusion-detection, and other similar security software and mechanisms should be in place and up to date. Moreover, clear security management procedures should be in place to effectively and efficiently respond to an actual breach in network security.[6]

B. Data Disposal

Businesses that collect consumer reports or any information derived from such reports must comply with the Fair Credit Reporting Act's (FCRA) Disposal Rule,[7] which was added to the FCRA by the Fair and Accurate Credit Transactions Act of 2003.[8] The Disposal Rule requires the proper disposal of consumer report information to protect against any "unauthorized access to or use of the information."[9] The standard for proper disposal is flexible,

4. *See* National Conference of State Legislatures, 2006 Breach of Information Legislation, http://www.ncsl.org/programs/lis/cip/priv/breach.htm.

5. *See, e.g.*, Joint Press Release, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, & Office of Thrift Supervision, Federal Bank and Thrift Regulatory Agencies Jointly Issue Interagency Guidance on Response Programs for Security Breaches (March 23, 2005), *available at* http://www.federalreserve.gov/boarddocs/press/bcreg/2005/20050323/default.htm.

6. A group of credit card companies, including American Express, MasterCard International, and Visa International, require certain security standards for businesses that work with credit card companies. *See* Steven Marlin, *More Customer Data Missing*, Info. Week, April 25, 2005, http://www.informationweek.com/story/showArticle.jhtml?articleID=161500879.

7. *See* Federal Trade Commission for the Consumer, Disposing of Consumer Report Information? New Rule Tells How (2005), http://www.ftc.gov/bcp/conline/pubs/alerts/disposalalrt.htm [hereinafter FTC New Rule].

8. Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. § 602 (2005).

9. FTC New Rule, *supra* note 7.

allowing businesses to determine what measures are reasonable based on the type of information collected, changes in technology, and costs and benefits of different disposal practices. Reasonable measures could include burning, pulverizing, or shredding documents containing consumer report information; erasing or destroying electronic files containing consumer report information; or hiring a document destruction service (after conducting due diligence, of course) to dispose of the consumer report information. Businesses should ensure that the destroyed information cannot be read or reconstructed. Importantly, although the Disposal Rule applies to consumer report information, the FTC encourages businesses who dispose of personal data to take similar measures to protect such information.

C. Spyware

Generally, spyware is a catchall term that is used to describe software that covertly gathers information about a user or a user's computer through an Internet connection without the user's knowledge, typically for advertising purposes. The Anti-Spyware Coalition, a group of software companies, consumers, and academics,[10] has defined "Spyware and Other Potentially Unwanted Technologies" as

> [t]echnologies deployed without appropriate user consent and/or implemented in ways that impair user control over: Material changes that affect their user experience, privacy, or system security; Use of their system resources, including what programs are installed on their computers; and/or Collection, use, and distribution of their personal or other sensitive information.[11]

Spyware is often downloaded onto a computer in three circumstances: (1) when a user actively downloads free software, like games, peer-to-peer file sharing programs, or other programs that change or customize the user's browser; (2) by drive-by downloads, such as when a browser's security setting is not set high enough to detect and/or prevent unauthorized downloads; or (3) clicking on links within pop-up windows or spam. Spyware may cause computers to run slow, malfunction, or even crash. The 108th Congress has failed to pass legislation specifically addressing spyware, and it is unlikely that the 109th Congress will pass such legislation anytime soon. Note, however, that certain states have enacted spyware legislation.[12]

D. RFID

Although Radio Frequency Identification (RFID) has been around for quite some time, the improvement in the technology has allowed it to proliferate dramatically in the past few years. An RFID tag consists of an antenna that gives off a radio signal that can be activated or detected by a reader, and a microchip containing data about a tagged item. RFID tags may be passive (i.e., they are not self-powered) or active (i.e., they are self-powered). RFID has wide-ranging applications, but raises significant privacy implications for consumers and businesses alike. RFID may be used to keep tabs on items, animals, or

10. *See* Anti-Spyware Coalition, Anti-Spyware Coalition Definitions and Supporting Documents, http://www.antispywarecoalition.org/documents/definitions.htm (last visited Feb.15, 2006).

11. *Id.*

12. For information on state legislation regarding spyware, *see* Benjamin Edelman, Spyware Research, Legislation, and Suits, http://www.benedelman.org/spyware/legislation/ (indexing and summarizing proposed state anti-spyware legislation) (last updated Feb. 12, 2006).

even people, among other applications. RFID tags may be attached to shipping crates, for example, to keep track of goods being shipped from the manufacturer to the retailer. Tracking items for inventory purposes may not raise significant privacy issues, but could cause other headaches. For example, RFID tags could be reprogrammed by hackers in order to change the price of an item.

RFID technology has raised privacy concerns as a result of its ability to use radio waves to share information. Critics of RFID are concerned that widespread use of the technology could lead to misuse. For example, a retailer could track a customer's buying habits and use that information to barrage the customer with advertisements. In addition, RFID devices implanted in individuals can store sensitive personal data that could be read by others without the individuals' knowledge or consent. According to a recent U.S. Government Accountability Office report, without effective security controls, "data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users."[13]

The European Union's (EU) Article 29 Working Party, the European Commission's advisory board on data protection, issued a working document providing guidance to users of RFID under relevant EU Directives,[14] and to manufacturers of the technology (e.g., tags, readers, and applications), as well as to RFID standardization bodies with regard to adopting privacy compliant technology. The working document states that the EU Data Protection Directive applies to RFID technology to the extent it involves the processing of personal data.[15] In addressing the issue of data protection, the working document states the following:

> On the data protection front, Working Party 29 . . . is concerned about the possibility for some applications of RFID technology to violate human dignity as well as data protection rights. In particular, concerns arise about the possibility of businesses and governments to use RFID technology to pry into the privacy sphere of individuals. The ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns. The problem is aggravated by the fact that, due to its relative low cost, this technology will not only be available to major actors but also to smaller players and individual citizens.[16]

E. Spam

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM) is the federal law regulating commercial electronic mail messages.[17] CAN-

13. U.S. Government Accounting Office, Information Security: Radio Frequency Identification Technology in the Federal Government, GAO-05-551 (May 2005), *available at* http://www.gao.gov.new.items/d05551.pdf.

14. Article 29 Data Protection Working Party, *Working Document on Data Protection Issues Related to RFID Technology*, 10107/05/EN WP 105 (Jan.19, 2005), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf.

15. *Id.* at 2.

16. *Id.*

17. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM Act"), 16 C.F.R. § 316 (2005).

SPAM largely preempts state laws and thus provides a national uniform regulatory approach. In May 2005, the FTC opened a new proceeding seeking public comment on certain definitions and substantive provisions under CAN-SPAM. The FTC also launched a campaign—Operation Spam Zombies—to encourage Internet service providers (ISPs) to crack down on zombie computers.

Spam may be used to install malware on unprotected computers that can convert computers into zombies. Spammers control zombie networks through remote-control to send millions of unsolicited e-mails, which has contributed to the increasing amount of phishing attacks, as discussed below. Remote-controlled zombie networks are becoming a serious problem that has drawn the attention of the FTC and several of its foreign counterparts. Other spam by-products that can create problems are spim, or spam over instant messaging, and spit, or spam over Internet telephony (Voice over Internet Protocol), which is a relatively new phenomenon. New and developing spam-related technologies will need to be taken into account when creating and implementing anti-spam measures.

F. Phishing and Pharming

Phishing is a high-tech scam that uses official-looking e-mail and pop-up messages as bait to lure unsuspecting victims into divulging personal data at fake websites. Generally, criminals behind these phishing attacks, referred to as phishers, simultaneously send Internet users hundreds of thousands of 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 ISP. The message can say that a user needs to update or validate 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 mentioned in the message. At the bogus site, the user is required to provide her personal information (e.g., name, address, social security number, telephone number, credit card number, bank account number, username, or password) to update or validate her account information. The personal data submitted by the user, however, is used by the phisher for fraudulent purposes. Phishing attacks are becoming ever-more sophisticated, foregoing the traditional mass-targeting approach in favor of targeting consumers on an individual basis, or spear phishing.[18]

Phishers are difficult to catch because they are a moving target. Their fraudulent e-mail accounts and/or websites may last from a few hours to several days. The increased use of zombie networks, discussed above, by criminals has been a major contributor to the increase in phishing attacks because such networks send out massive numbers of fraudulent e-mails. The FTC has brought a few enforcement actions against phishers over the past couple of years.

Pharming is a similar scam that misdirects users to spoofed websites that mirror the real site, where criminals harvest large amounts of personal data. Even if a user types in the correct address of a particular Web site, malicious software downloaded on the user's computer or hijacked servers will send the user to a site that is the exact replica of the real site. Although phishers and pharmers could be prosecuted under existing laws (e.g., fraud statutes), these prosecutions typically take place after someone has been the victim of a crime,

18. *See* Timothy O'Brien, *Online Scammers Go Spear-Phishin*, N.Y. Times, Dec. 4, 2005, *available at* http://news.com.com/Online+scammers+go+spear-phishin/2100-1029_3-5981917.html.

which makes them insufficient to tackle the phishing and pharming problems. In March 2005, the Anti-Phishing Act of 2005 was introduced in the Senate.[19] Under this federal legislation, prosecutors could impose fines of up to $250,000 and prison terms of up to five years against phishers. The legislation also covers pharming.

Increased consumer awareness of these fraudulent practices is another way of battling this problem. Companies should post anti-phishing/pharming information on their websites to inform their customers on how to protect themselves. Also, several private sector efforts have been undertaken to fight this criminal activity, including BITS (formed by several large banks) and the Phish Report Network, launched by several large companies, including Microsoft and eBay.[20]

II. Privacy and E-Commerce Law in the European Union

A. New Developments on Data Retention in Italy and the European Union

As a consequence of the recent terrorist attacks, France, Ireland, Sweden, and the United Kingdom have submitted to the EU a proposal for a Framework Decision[21] on the retention of communication traffic data (with the exclusion of their content) for a minimum of twelve months and a maximum of thirty-six months across all EU Member States to prevent, detect, investigate, and prosecute crimes and criminal offenses. This area is currently regulated in the EU by the Directive 2002/58/EC on Privacy and Electronic Communications.[22] The Directive prescribes the deletion of traffic data once they are no longer required for the transmission of the communication, except for data necessary for billing or interconnection payments. Article 15 of the same Directive, however, states that such provisions can be derogated when further processing of traffic data is justified by the need to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offenses.

The Article 29 Data Protection Working Party, in its opinion[23] on the Draft Framework Decision maintained that the new proposed measures were in contrast with article 8 of the European Convention on Human Rights (ECHR)[24] because they made surveillance the rule, when instead it should only be allowed in exceptional cases. This opinion was supported by the European Parliament that rejected the Draft Framework Decision in April 2005.[25]

19. Anti-phishing Act of 2005, S. 472, 109th Cong. (2005).

20. Phish Report Network, http://www.phishreport.net/ (last visited Feb. 15, 2006); BITS Financial Services Roundtable, http://www.bitsinfo.org/index.html (last visited Feb. 15, 2006).

21. Draft Framework Decision No. 8958/04 (EC), (Apr. 28, 2004), *available at* http://www.europarl.eu.int/meetdocs/2004_2009/documents/cls/cons_cons(2004)08958_/cons_cons(2004)08958_en.pdf.

22. Directive 2002/58/EC of the European Parliament and of the Council, 2004 O.J. (L 201) (EC), *available at* http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32002L0058&model=guichett.

23. *Opinion 9/2004 of the Article 29 Data Protection Working Party*, 11885/04/EN, Nov. 9, 2004, *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2004/wp99_en.pdf.

24. Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221, *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf.

25. European Parliament, Draft Report on the Retention of Data Processed, Eur. Parl. Doc. 2004/0813(CNS) (Apr. 8, 2004), (*prepared by* Alexander Nuno Alvaro), *available at* http://www.statewatch.org/news/2005/may/ep-data-ret-alvaro-report.pdf.

In September 2005, the European Commission again adopted a proposal[26] for a Directive on the retention of communications traffic data, with the exclusion of their content. The new proposal provides for an EU-wide harmonization of the obligations on providers of publicly available electronic communications or a public telecommunications network. They must retain data related to mobile and fixed telephone services for a period of one year, and Internet communication data for six months for the purpose of the prevention, investigation, detection, and prosecution of serious criminal offences, terrorism, and organized crime. Interestingly, the proposal also prescribes that service or network providers will be reimbursed for the additional costs incurred by storing such data. The European Data Protection Supervisor, in its opinion of September 26, 2005,[27] did stress that even if this proposal is more liberal than the Draft Framework Decision, it must still be amended in accordance with the ECHR to ensure that adequate safeguards to protect individuals' privacy rights are implemented.

Ultimately on October 21, 2005, the Article 29 Data Protection Working Party issued an opinion[28] on such proposal, in which it expressed its concerns on the effectiveness of data retention as a useful tool for investigations. A justification for compulsory and general data retention should be demonstrated and backed up with evidence. This evidence should be reviewed periodically, taking into account that introducing general surveillance of citizens might encourage terrorist organizations to modify their strategies to avoid using certain means, and thereby obliging investigation authorities to find more effective methods of surveillance. In particular, the Article 29 Working Party suggested that methods like the quick-freeze procedure might be more effective and would harm to a lesser extent the privacy of the citizens. The law enforcement authorities would consult the companies and request the storage of certain data when an investigation is in course.

On November 24, 2005, the European Parliament's Civil Liberties Committee voted thirty-three to eight in favor of such proposal, subject to some amendments. Members of the committee, among others, stressed the need to allow the usage of data for the detection, investigation and prosecution only of terrorism and organized crime, rather than any kind of crime, to avoid abuses by national authorities. Moreover, the Committee added a provision requiring effective, proportionate and dissuasive criminal sanctions for companies that fail to store data or misuse the retained information. Finally, it was specified that access to data retained should be granted to third countries, and particularly the United States, only by means of an international agreement.

The EU Ministers of the Justice and Home Affairs Council gave their final seal of approval to the proposal on Febraury 21, by adopting the Directive with a qualified majority. Notwithstanding the recent approval of the Directive, some national governments have already issued regulations regarding the storage of traffic data. The Italian government, for

26. *Commission Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed*, COM (2005) 438 final (Sept. 9, 2005), *available at* http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/communic_reports/data_retention/retention_proposal_en_com_2005_0438.pdf.

27. *Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed*, (Sept. 26, 2005), *available at* http://www.edps.eu.int/legislation/Opinions_A/05-09-26_Opinion_data_retention_EN.pdf.

28. *Opinion/2005 of the Article 29 Data Protection Working Party on the Proposal for a Directive of the European Parliament and of the Council*, 1868/05 WP 113 (Oct. 21, 2005), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp113_en.pdf.

instance, has recently enacted anti-terrorism legislation in the form of Law Decree No. 144 of July 27, 2005,[29] which provides in part that all communications service providers shall store traffic data, including Internet traffic communications, until December 31, 2007. Until such date, all traffic data currently held shall be retained and must not be deleted, regardless of when the data was collected. The new Italian law supersedes the application of all current data retention provisions. From January 1, 2008, Italian service providers will be obliged to store traffic data connected with telephone calls for a period of twenty-four months,[30] and traffic data relating to Internet communications for a period of six months.[31]

Communication operators have complained of the high financial costs that they will incur as a consequence of the Italian Law Decree, such as the costs associated with the storage of such enormous quantities of data and that such costs might dissuade companies from investing in Italy. Commentators, including Professor Rodotà, the former Chairman of the Italian Privacy Authority, have stressed that such provisions excessively constrain the privacy rights of individuals and their effectiveness to prevent terrorist attacks is doubtful. It will be interesting to see how possible inconsistencies between local legislation and EU regulation will be reconciled.

B. The Saga on Transfer of Flight Passengers from the European Union to the United States

Following the terrorist attacks of September 11, 2001, the United States adopted legislation requiring airlines carrying passengers to, from, or across United States territory to give U.S. authorities electronic access to the passengers' data contained in their systems for controlling and monitoring departures. In light of possible conflict between such a measure and European privacy laws, the European Commission started negotiations with U.S. authorities. Under article 25 of the Directive 95/46/EU,[32] the transfer of personal data to countries outside the EU can take place only if such receiving countries ensure an adequate level of protection. According to the Article 29 Working Party,[33] as of December 2005, the United States was not deemed to provide the level of adequate protection required by EU standards. But on May 14,[34] and 17,[35] 2004, the European Commission and the European Council respectively have adopted two decisions holding that the United States Bureau of

29. The law decree has subsequently been implemented (without amendments) by Italian Anti-Terror Law Decree, Gazz. Uff. no. 155 (July 31, 2005), *available at* http://www.parlamento.it/parlam/leggi/051551.htm.

30. There is an additional twenty-four months for the investigation and prosecution of serious crimes. *Id.*

31. There is an additional six months for the investigation and prosecution of serious crimes. *Id.*

32. Directive 95/46/EC of the European Parliament and of the Council, 1995 O.J. (L 281) (EC), *available at* http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett.

33. *Opinion 1/99 of the Article 29 Data Protection Working Party Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government*, 5092/98 WP 15 (Jan. 26, 1999), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/1999/wp15en.pdf.

34. Commission Decision on the Adequate Protection of Personal Data Contained in the Passenger Name Record, 2004 O.J. (L 235) 11, *available at* http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_235/l_23520040706en00110022.pdf.

35. Council Decision on the Conclusion of an Agreement between the European Community and the United States of America, 2004 O.J. (L 183) 83 (EC), *available at* http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_183/l_18320040520en00830083.pdf.

Customs and Border Protection (CBP) offered an adequate level of protection for personal data transferred from the European Community and, therefore, approved the transfer of European passengers' data by airlines established in the territory of EU Member States to the CBP. The European Parliament requested that the Court of Justice of the European Communities (ECJ) annul the European Commission and the European Council decisions. The European Advocate General, in his opinion of November 22, 2005, to the ECJ stressed that the Directive 95/46/EU, which is designed to remove obstacles to the free movement of personal data by making the level of protection of the rights and freedoms in relation to those data equivalent in the EU Member States, is not applicable to matters concerning public security since it falls outside the scope of community law. Therefore, both the European Commission and the European Council did not have the power and authority to adopt the above decisions of May 14th and 17th. The opinion of the Advocate General is not binding on the ECJ as it will independently decide on the issue.

C. Launch of ".eu" Top-Level Domains

EURid,[36] the official registry for ".eu", announced that from December 7, 2005, it is possible to register domain names with the Top Level Domain ".eu". ".Eu" is the first and unique cross border domain name available to 376 million people and twenty million enterprises. It will not replace existing domain names, but some commentators stressed the relevance it will have for the development of e-commerce in Europe. The launch of ".eu", however, will pass through a so-called sunrise period. Until February 7, 2006, only holders of prior rights recognized or established by national and/or community law and public bodies were eligible to apply for domain names. Prior rights were deemed to be only registered national and community trademarks, geographical indications, or designations of origin. Such rights had to be valid no later than the date on which the application is received by EURid. After February 7, 2006, holders of unregistered trademarks, trade names, business identifiers, company names, family names, and distinctive titles of protected literary and artistic works will be entitled to register domain names with the Top-Level Domain ".eu." Finally, after April 7, 2006, open registrations will begin on a first come, first served basis.

Applications for ".eu" domain names may only be submitted by accredited registrars in the order received. EURid will then register the first application for a particular domain name received, subject to validation of the prior rights claimed. This means that is highly relevant for brand owners to submit their application to registrars as soon as possible. The following categories of companies, organizations and individuals will be able to register an ".eu" domain: (i) undertakings having their registered office, central administration, or principal place of business within the European Community; (ii) organizations established within the European Community without prejudice to the application of national law; and (iii) natural persons resident within the European Community. It is possible, however, for entities based outside the EU to license their trademark to entities having the required presence in the EU. The domain name will be registered in the name of the licensee.

36. EurID: The European Registry of Internet Domain Names, http://www.eurid.eu/en/general/ (last visited Feb. 15, 2006).

D. Websites' Terms and Conditions Challenged in Europe

A number of interesting decisions have been issued recently by European national courts regarding the validity of websites' terms and conditions and their applicability to consumers.

Two decisions have been issued by French courts in June 2004[37] and April 2005[38] in cases brought by French consumer associations against America Online (AOL) and the European ISP Tiscali, respectively. In the first case, the French court held that thirty-one clauses in the standard contractual terms used by AOL in France in its online subscriber contract were not in compliance with consumer protection regulations.[39] The list of provisions deemed as illegal included: contract acceptance by performance, modifications, discontinuance of service, late payments, disclaimers of liability, third party content, service performance, and termination.

In both decisions the courts awarded the plaintiff a monetary compensation in damages and required the removal of the unfair clauses within one month, with a further fine in case of noncompliance. Moreover, the French courts ordered the publication of substantial parts of the decisions in three major French daily newspapers and on the homepage of the defendants' websites. Tiscali was also obliged to send via e-mail the ruling of the judgment to all its subscribers under the penalty of 1000 Euro per day for failure to do so. The two decisions were based on the application of the law implementing in France the Directive 93/13/EU on unfair terms in consumer contracts.[40]

The Hague Court of Appeal in the Netherlands in 2005 has set aside Dell's general conditions.[41] The case was started by an association of computer users who claimed that many of the provisions in Dell's general conditions were unreasonably onerous for consumers. The Court of Appeal found that the provisions in Dell's general conditions excluding its own liability with respect to products or components of third parties were unreasonably onerous and prohibited their use in contracting with consumers. The court also held that incorporation by reference to other documents or third-party general conditions was against mandatory statutory rules protecting consumers. These decisions highlight the importance for foreign companies doing business in the EU to draft their general terms and conditions in compliance with national requirements in each jurisdiction where they seek to do business.

37. Tribunal de Grande Instance de Nanterre, *UFC Que Choisir/AOL Bertelsmann Online France* (June 2, 2004), *available at* http://www.legalis.net/jurisprudence-decision.php3?id_article=1211.

38. Tribunal de Grande Instance de Paris, *UFC Que Choisir/Tiscali* (Apr. 5, 2005), *available at* http://www.lauremarino.com/tgipar05042005.htm.

39. *UFC Que Choisir/AOL Bertelsmann Online France*, *supra* note 37.

40. Council Directive 91/13, 1993 O.J. (L 095) 29-34 (EC), *available at* http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31993L0013&model=guichett.

41. *HCC/Dell Computer BV*, Gerechtshof [Hof] [The Court of Appeals of the Hague], Mar. 22, 2005, Case no. 03/1463 LJ AT1762 (Neth.).