CORPORATE COUNSEL'S RECORDS RETENTION REPORT

DECEMBER 2012 | ISSUE 180

LETTER FROM THE EDITOR

Dear Subscribers,

This issue of the CORPORATE COUNSEL'S RECORDS RETENTION REPORT features an excerpt from **Internet Distribution, E-Commerce and Other Computer Related Issues: Current Developments in Liability On-Line, Business Methods Patents and Software Distribution, Licensing and Copyright Protection Questions**, an article written by Mr. Andre R. Jaglom. Mr. Jaglom is a member of the New York City firm of Tannenbaum Helpern Syracuse & Hirschtritt LLP and is a nationally recognized expert in the field of distribution law. We are grateful to Mr. Jaglom for his permission to share his insights on privacy regulation in the European Union.

Sincerely,
Nick J. Vizy
Senior Attorney Editor

IN THIS ISSUE:

PRIVACY UNDER THE EUROPEAN COMMUNITY DIRECTIVE

*By Andre R. Jaglom**

As the use of the Internet has become ubiquitous, companies are gathering more and more information regarding their customers and visitors to their websites. Databases of this information are a powerful business and marketing tool, but also raise a serious threat to the privacy of personal information. Governments around the world are addressing that threat through laws regulating the collection, disclosure and use of

*Mr. Jaglom is a member of the New York City firm of Tannenbaum Helpern Syracuse & Hirschtritt LLP. The assistance of Jason B. Klimpl, an associate at the firm, is gratefully acknowledged.

Mat #41178822

WEST®

personal data. This paper addresses recent developments in this area, focusing on the United States and Europe.

Use of personal data, such as medical information, credit card records, purchasing patterns and the like, by businesses that gather it, whether over the Internet or by other means, has been relatively unregulated in the United States. Except in a few specific areas, the U.S. has adopted a laissez-faire approach to the issue. Use of such data is far more restricted in Europe.[1] The European Community's 1998 Directive on "Transborder Flows of Personal Data"[2] prohibits companies from transmitting data to countries that do not adequately protect it.[3]

The Directive applies to non-European companies with European customers, employees or others from whom personal data is collected. Thus, the collection of personal data by a U.S. company over its website could violate European law, given the lack of formal U.S. protection of such information, particularly if the data is collected through facilities or equipment located in Europe, including the use of cookies placed on European users' computers.[4] Indeed, the EC enacted a new Directive on Privacy in the Electronic Communications Sector (the "E-Privacy Directive") in 2002 that requires consumers to be given clear and precise information about the purposes of the cookies and an opportunity to refuse them before cookies may be used.[5] As amended on December 18, 2009, the E-Privacy Directive requires that consumers *actively* give consent to such cookies.[6] For instance, the EU Article 29 Working Party recently rejected a privacy framework proposed by the Interactive Advertising Bureau (Europe) because, among other things, users could not be considered to have consented to receive cookies where they use an internet browser that allows cookies by default—in the absence of active informed consent, "[i]t cannot be concluded that users who have not objected to being tracked for the purposes of serving behavioural advertising have exercised a real choice."[7] Spyware, web bugs and similar devices, that can store hidden information or trace user activities, are permitted only for legitimate purposes with the user's knowledge.[8]

In response to the 2009 Directive, the United Kingdom enacted new laws on cookies and e-commerce effective in May 2012, which apply to all data collected electronically, whether through cookies or other means, and whether constituting personal information or not.[9] Cookies and similar methods of gathering data may not be used without user consent after having received clear and comprehensive information about what the cookies or other means of data gathering are doing and what information is being stored. Notably, regulatory guidance indicates that consent requires active communication by which the user knowingly indicates acceptance, such as clicking an icon, sending an email or subscribing to a service; the key is that the user understand that the by taking the action, he or she is providing consent. This poses a problem for sites that require a cookie to be set before the web page is displayed; the guidance recommends minimizing such situations and to seek the consent as soon as pos-

CORPORATE COUNSEL'S RECORDS RETENTION REPORT (ISSN 1098-0261) is published monthly by Thomson Reuters, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526. POSTMASTER: send address changes to CORPORATE COUNSEL'S RECORDS RETENTION REPORT, 610 Opperman Drive, P.O. Box 64526, St. Paul, MN 55164-0526.

sible, while being prepared to demonstrate that the site is doing all it can to provide the information and seek consent as promptly as possible.[10]

Canadian law is even more stringent. While the European E-Privacy Directive permits websites to condition access on acceptance of cookies, so long as their purpose is legitimate and the acceptance is well informed, the Canadian Privacy Commission found that an airline's denial of access to users who refused cookies was a violation of the Canadian Protection of Personal Information and Electronic Documents Act.[11] This Canadian law became applicable on January 1, 2004 to all companies—including U.S. companies—that collect, use or disclose personal information about Canadian citizens in the course of commercial activities.[12] India recently enacted strong privacy laws as well. Effective April 11, 2011, India adopted the Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, implementing parts of the 2008 Information Technology Act. These Rules are more restrictive than those contained in the Gramm-Leach-Bliley Act and the EU Privacy Directive and purport to extend to any person so long as a computer or computer network located in India is affected.[13]

The EU Data Protection Directive affects U.S. companies that wish to receive information about its European employees or customers, or respond to government demands for information about Europeans.

This concern was the subject of negotiations between the United States and the European Community. In 2000, the Department of Commerce issued the final version of an intergovernmental agreement[14] creating a "safe harbor" for U.S. companies that voluntarily and publicly agree to adhere to specified principles, including:

(a) *Notice*: Notice to individuals of the purposes for which personal information is collected, the types of third parties to whom it is disclosed, and how individuals may limit such use and disclosure where it is for a purpose other than that for which the information was originally collected or later authorized;[15]

(b) *Choice*: An opportunity for individuals to choose ("opt out") whether and how their personal information is used or disclosed to third parties, where such use is incompatible with the original purpose of collection; for sensitive information (e.g. medical information or information regarding racial or ethnic origin, political opinions, religious beliefs and the like, or information designated as sensitive by the source) individuals must be given an explicit choice ("opt in") before the information is disclosed to a third party or used for a purpose other than that for which it was originally collected;

(c) *Onward Transfer*: A requirement that third parties, who are acting as agents of the a business, to whom personal information may be transferred by that business without Notice and Choice, must provide at least the same level of protection;

(d) *Security*: Use of reasonable measures to protect personal information from loss, misuse, unauthorized access or disclosure, alteration or destruction;

(e) *Data Integrity*: A prohibition on processing personal information in a way that is incompatible with the purposes for which it is collected or subsequently authorized;

(f) *Access*: Giving individuals reasonable access to information about them and the opportunity to correct or delete inaccurate information; and

(g) *Enforcement*: A mechanism for enforcing compliance with these principles.[16]

A comprehensive checklist is available on the Department of Commerce's Safe Harbor website, www.export.gov/safeharbor/index.html.

The EC has recognized the Federal Trade Commission (under § 5 of the FTC Act) and the Department of Transportation (under 49 U.S.C. § 41712, relating to unfair and deceptive practices by air carriers and ticket agents) as government bodies empowered to investigate complaints and obtain relief against unfair or deceptive practices or noncompliance with the safe harbor principles.[17] (Businesses not subject to FTC or DOT jurisdiction such as telecommunications, banking, insurance and nonprofit companies, cannot take advantage of the Safe Harbor program.) The FTC has sued and entered into consent orders with several US companies that have falsely claimed to comply with the safe harbor framework in violation of § 5 of the FTC Act.[18]

Moreover, private damage actions have been filed in U.S. courts for the improper collection, use and transfer of personal information, albeit with little success to date.[19]

United States companies should consider bringing themselves within the safe harbor if they collect personal data from individuals in the EC. This means certifying to the Department of Commerce their adherence to the safe harbor principles and implementing privacy policies that comply with those principles.[20]

A Commission Staff Working Document report analyzing the compliance of participating companies found substantial non-compliance, as a result of failure of companies to have publicly posted privacy policies, or policies that did not fully and clearly comply with the seven privacy principles.[21] The report suggested that European data protection authorities use their power to suspend distributors if they find a substantial likelihood that the principles are being violated. To assist companies in creating compliant, easy to understand privacy policies, the EU has adopted a plan calling for companies to use "very short," "condensed," or "complete" privacy policies in a common format.[22] Major companies are beginning to use the format.[23]

Outside the boundary of the safe harbor, businesses that collect or receive personal data from EU persons risk violation of EC law,[24] although other means of compliance may be elected. One option—perhaps impractical—is obtaining the informed consent of every individual whose information is to be transferred. Another option for such businesses is to choose to use binding contracts that conform to EC Directive requirements with those who provide them with personal data and anyone to whom they transfer such data. To facilitate this, the EC has adopted standard contract forms, under which the data transferred is treated in compliance with EU data protection standards.[25] Note that companies that outsource data processing to third parties remain responsible for breaches of privacy occurring at the third parties' hands.[26] Another option is the development of "binding corporate rules" for internal governance within the organization. Such binding rules must be legally enforceable and subject to audit, and subject to approval by data protection authorities.[27]

European actions indicate that enforcement of privacy rules can be expected. The European Court of Justice found that a website published by a Swedish woman that included names of her colleagues, job descriptions and some telephone numbers and other personal information, constituted the processing of personal data under the Directive.[28]

The EC's investigation, initiated in May 2002, into whether Microsoft's Passport Internet authorization system violates EU rules[29] was settled in 2003 by Microsoft's agreement to make a "radical change" to its.NET Passport system, providing users with more information and choices as to the data they want to provide

and how it will be used by Microsoft and other websites on a site-by-site basis.[30]

In another example of European privacy enforcement, a German state Interior Ministry found that certain Hewlett-Packard printer driver software violated German data protection law by transmitting technical information, including IP addresses and printer model numbers, to a Hewlett-Packard server outside Germany without appropriate user consent.[31] Hewlett-Packard agreed to remedy the problem. However, The High Court of Ireland has held that IP addresses are not always personal data.[32] In upholding a settlement agreement between the nation's largest ISP, Eircom, and four music record companies in connection with Eircom's failure to take action to discourage peer-to-peer copyright infringement on its networks, Eircom agreed to implement a graduated response mechanism with its infringing customers managed by a third party service provider who would get access to the IP addresses of such customers. The Court held that that transfer of IP addresses was not personal information and therefore not in violation of Irish privacy law because the third party service provider would not have the "means" or "motivation" to find out the names or addresses of the persons corresponding to the IP address, the customers consented to Eircom's terms of use, and the graduated response mechanism was implemented in furtherance of a legal contract.[33]

French authorities have warned that sharing of credit and payment histories must conform to French privacy law. While such information may be used for internal and intra-industry purposes, it may not be shared with other industries, and must comply with privacy practices, such as offering a right of redress to the subject of the information.[34] Norway has recently enacted security rules requiring all Norwegian employers subject to Norwegian tax laws to encrypt paycheck stubs sent via e-mail to employees' personal accounts.[35] And in Spain, authorities are charging Google for collecting personal information via Wi-Fi "interceptions" by Google Street View trucks and conveying that information to the United States in violation of the Spanish Information Protection Law.[36]

The United Kingdom's Information Commissioner's Office (the "ICO") announced that where laptops containing unencrypted personal information are lost or stolen, enforcement action may be commenced against even private individuals under the U.K.'s Data Protection Act of 1998 (c. 29) which applies to any person who controls and loses personal data.[37] The announcement is consistent with EC privacy policy, which requires that possessors of data use reasonable measures to protect personal information from loss or unauthorized access. Moreover, as of April 6, 2010, the ICO will have authority to impose monetary penalties up to £ 500,000 on organizations for serious breaches of the Data Protection Act.[38]

The U.S. Sarbanes-Oxley Act's requirement of anonymous corporate whistleblower hotlines has been held to conflict with European data protection laws. Under Sarbanes-Oxley, public companies must provide at least one confidential, anonymous method for employees to submit complaints about questionable accounting matters.[39] French and German decisions have held that such methods may violate European Law.

A German Labor Court held that an anonymous hotline could not be implemented by WalMart without first consulting with the works council, which had a right to participate in "matters relating to the rules of operation of the establishment and conduct of employees."[40] In 2005, the French data protection agency, the Commission Nationale d' Information et des Libertes ("CNIL") found that anonymous hotlines would "reinforce the risk of slanderous denunciations" and "was disproportionate to

the objectives sought."[41] In addition, a French court ordered the French subsidiary of a U.S. company to discontinue a whistleblower hotline, on similar grounds.[42] In December 2009, the French Supreme Court considered the validity of a corporate code of conduct implemented by a company in order to comply with Sarbanes-Oxley. The Court found that the scope of the company's code of conduct was too broad, since not only did it invite employees to report violations relating to more than just finance, accounting and anti-corruption matters, but also intellectual property rights, confidentiality, discrimination, conflicts of interest and harassment outside the scope of the CNIL 2005 decision.[43]

European data protection laws require that individuals have notice of what data is collected about them and that it be processed fairly. Anonymous tips, about which the employee complained about is not informed, and cannot contradict, raise significant data protection and privacy issues under European law. Recognizing the conflict with U.S. law, CNIL issued guidelines in November 2005.[44] The CNIL guidelines, among other things, require that whistleblowing systems be limited in scope: employees should not be required, but merely encouraged to use them: and anonymous reports should be discouraged, and, when received, must be handled with precautions. Critically, the individual who is the subject of the report must be notified promptly.

The EU Article 29 Working Party followed with a preliminary opinion in 2006,[45] which recognized that companies subject to Sarbanes-Oxley "are subject to heavy sanctions and penalties" for failure to comply with the Act's whistleblowing requirements, but face "risks of sanctions from EU data protection authorities if they fail to comply with EU data protection rules." The preliminary report stresses that "whistleblowing schemes must be implemented in compliance with EU data protection rules" and that the individual accused by a whistleblower is entitled to the rights guaranteed by European data protection law. It observed that "whistleblowing schemes entail a very serious risk of stigmatisation and victimisation . . .within the organisation" and that "[t]he person will be exposed to such risks even before the person is aware that he/she has been incriminated and the alleged facts have been investigated."

The report does recognize Sarbanes-Oxley whistleblowing rules as a legitimate initiative to protect the interests of shareholders, so long as adequate safeguards are in place. The report suggests a number of steps that may be taken in this vein:

- Possible limits on the number of persons who may report alleged misconduct.
- Possible limits on the categories of persons who may be incriminated.
- Promotion of identified and confidential reports rather than anonymous reports:
    - The report indicates that anonymous reports are particularly problematic and that only identified reports should be used. Whistleblowers should be informed that their identity will be kept confidential and not disclosed to third parties, including the accused. Only if despite this step, the person making the report wants to remain anonymous should the report be accepted. Anonymous reports should be treated with special caution, and perhaps investigated more quickly because of the risk of misuse.
- Clear definition of the limited types of information to be communicated.
- Compliance with strict data retention periods:
    - Generally data should be deleted

promptly, usually within two months of completion of the investigation, unless legal or disciplinary proceedings are taken.

- Provision of clear and complete information about the whistleblowing scheme.
- Respecting the rights of the accused to be informed of the charges against him as soon as possible, and how to exercise his rights of access and rectification:
    - The report recognizes that where such notice would jeopardize the investigation, it may be delayed, and that the whistleblower's identity should not be disclosed unless the whistleblower is found to have made a malicious false statement.
- Adequate security measures to protect the security and confidentiality of the data.
- Establishment of a specific, separate management structure for the whistleblowing scheme, with data generally remaining in the country in which it is reported.

In addition, whistleblowing schemes need to comply with the requirements of notification to national data protection agencies under the data protection laws of individual EU nations.

U.S. companies caught between the conflicting mandates of Sarbanes-Oxley and the EU data protection laws need to establish hotline programs that comply with these requirements, for example by providing for informing employees accused of improprieties of the details of the complaints and offering them an opportunity to respond, excepting European employees from the program, and treating the complaint's content as personal information of the employee complained about, subject to the applicable privacy rules.

Concerns have also been raised that the EU's data protection Safe Harbor is incompatible with the USA PATRIOT Act. For instance, in 2011 Microsoft announced that, in some circumstances, it may be required to disclose to U.S. authorities the personal data of EU residents, and that such disclosures may be kept secret from EU authorities and data subjects, in accordance with the USA PATRIOT Act. Of course, such disclosures would likely violate the Safe Harbor, which requires that self-certified U.S. companies inform the EU of such requests for personal data. Accordingly, U.S. companies may find themselves with a Hobson's choice of violating either the USA PATRIOT Act or the EU Data Protection Directive.[46]

Even something as routine as an electronic interoffice telephone directory for a multinational company can require significant legal compliance work to avoid violation of European privacy laws. General Motors spent six months on just such a project, working under the rubric of the Safe Harbor Program. This meant mapping where the directory might be used and by whom, notifying employees in Europe that their phone numbers would be exported to other offices and obtaining agreement of hundreds of affiliates around the world not to misuse or disclose the information.[47] Many major U.S. companies are adapting global privacy standards based on the EU model. Proctor & Gamble, Dupont and General Electric are examples.[48] Indeed, a number of corporations, such as P&G and AXA Financial Services, take the approach of complying with the strictest applicable privacy requirements.[49] (In addition to influencing major companies, the EU model has also caused numerous other countries to consider strengthening their online privacy laws.[50])

Finally, the EU's Data Protection Directive[51] has led to a conflict between U.S. discovery obligations and European privacy obligations:

> Both U.S. discovery laws and E.U. data protection laws provide severe sanctions for noncompliance. Accordingly, companies subject to U.S. discovery demands for personal data lo-

cated in the E.U. may find themselves between the proverbial rock and a hard place.[52]

A party's U.S. discovery obligations are found in the Federal Rules of Civil Procedure and similar state provisions that allow a party to request non-privileged information germane to a claim or defense.

Conversely, the Directive places "severe restrictions in the processing of personal data."[53] Specifically, "for documents within the scope [of the EU Directive], compliance with EU law will typically require a basis under EU law for (1) collection; (2) disclosure; and (3) analysis in the EU; a basis for (4) transfer to the U.S.; and a basis for (5) analysis; (6) disclosure; and (7) use in the U.S."[54] Some authors believe that one solution to finding a basis for transferring the information out of the EU into the U.S. may be compliance with the safe harbor procedures described above.[55] But it is unclear if bases exist under EU law to satisfy the other six requirements. For example, EU law would allow disclosure of private data in certain circumstances such as where dissemination is a "necessity."[56] One "necessity" is for compliance with a legal obligation imposed by EU member state law or international law. But it is questionable whether a discovery obligation arising U.S. rules would be sufficient.[57] And other grounds for disclosure under the Directive are unlikely to provide a route for enforcement of the discovery requirements.[58] Accordingly, "it may be quite difficult, and even impossible to comply with both U.S. and E.U. law [in] collecting documents."[59]

If U.S. case law is a guide, courts grappling with a conflict between U.S. discovery rules and foreign privacy laws may engage in a form of interests balancing.[60] However, a U.S. federal district court has held that E.U. requirements to delete user data once it is no longer necessary for legitimate business purposes do not excuse companies from their U.S. electronic evidence preservation obligations.[61]

In the Americas, U.S. litigants seeking to acquire information from a Mexican party will face new hurdles with the recent amendment to Article 16 of the Mexican Constitution concerning privacy protection, which was modeled after the Spanish Data Protection Law promulgated in response to the EU Data Protection Directive.[62] Accordingly, U.S. litigants will likely face similar complications where discovery requires the disclosure of the personal information of Mexican citizens. Uruguay's privacy law, an opinion recently made public by the EU's Article 29 Working Party determined, are on par with the EU Data Protection Directive.[63]

Meanwhile, in 2011 Israel received a determination from the European Commission that Israel's data protections laws are in conformance with the EU Data Protection Directive.[64] Other countries that have received adequacy determinations of privacy include Canada, Switzerland, Isle of Man, Guernsey, Jersey, and the Faroe Islands.[65]

Finally, and as if the foregoing was not enough to consider, the European Commission in early 2012 released onerous draft data protection rules that would entirely repeal and overhaul the 16-year old data protection framework (i.e., the EU Data Protection Directive) currently in place.[66] The proposed rules would include a Regulation to regulate privacy and data protection from the EU level as well as a Directive, in contrast with the current Directive alone, which leaves the task of regulation implementing legislation in individual Member States. The new proposal would increase penalties for violations, allowing fines of up to 1 million or 2% of a company's annual turnover; provide a "right to be forgotten" that would permit individuals to demand the deletion of records about them; impose data breach reporting requirements; and increase regulation of sensitive areas, such as data mining, health end epidemiological data, genetic and biometric

data and closed circuit television video. Moreover, the proposed rules would apply to any company based outside the EU which provides goods and services to EU residents.[67] The Commission's proposal has been sent to the European Parliament and Member States for consideration, and the rules would take effect two years after adoption.[68]

ENDNOTES:

[1]Whether the European approach actually results in greater privacy is open to question. See, e.g., K. Jamal, M. Maier and S. Sunder, "Enforced Standards Versus Evolution by General Acceptance: A Comparative Study of E-Commerce Privacy Disclosure and Practice in the U.S. and the U.K., Working Paper 03-8," AEI—Brookings Joint Center for Regulatory Studies (July 2003, *available at* http://aei.brookings.org/admin/pdffiles/phpWo.pdf; Lettice, "U.S. Full Marks, Europe, Null Points—Study," The Register (July, 28, 2003), http://www.theregister.co.uk/content/6/32018.html.

[2]The Directive is *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:008:0001:0022:EN:PDF.

[3]It is worth observing that, notwithstanding the Directive, the Supreme Court of France ordered France Telecom to provide its list of unlisted telephone numbers to a marketing company, holding that the exclusive use of the lists by France Telecom was an abuse of dominant position and rejecting privacy arguments. *France Telecom v. Lectiel*, Arret No. 2030, Cour de Cassation, Chambre Commerciale (Dec. 4, 2001), *reported* in WORLD DATA PROTECTION ReEP. (BNA) 25 (Jan. 2002).

[4]*See* H. Rowe, "E.U. Data Protection Applies to Personal Data Processing on the Internet by Non-E.U. Based Websites?", WORLD INTERNET L. REP. 26 (Aug. 2002) (discussing May 30, 2002 working document of Working Party established under the Directive).

[5]Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Recitals (24)-(25) and Art. 5, sec. 3, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:EN:HTML. For suggestions on compliance for websites using cookies, see Dr. B. Goldman, "Europe Administers Diet for Cookies," World Internet L. Rep. 26 (Feb. 2004) at 16-24.

[6]*Id*. The 27 EU Member States must enforce these changes by May 25, 2011, which may result in various approaches to implementation and enforcement. As anticipated, "Member States seem to be taking markedly different approaches to implementing the amendment, creating yet another regulatory patchwork' in the EU privacy area." Worlton, "EU Cookies—Where Did the Pieces Fall?", Wiley Rein LLP (July 2011) (noting also that many member states failed to enact implementing rules as of the compliance deadline), *available at* http://www.wileyrein.com/publications.cfm?sp=articles&id=7223. Overall, these changes may have a significant effect on international advertising and referrals. Nabarro LLP, *New European Laws Could Impact the Use of Cookies on Websites from May 2011* (March 5, 2010), *available at* http://www.nabarro.com/Downloads/Commercial-IT-Comms-European-changes-to-laws-on-cookies.pdf.

[7]Massey, Mattina, Schroder, Sheraton and Uphoff, How the cookie crumbles: a clash of cultures on cookie regulation, McDermot Will & Emery (Nov. 3, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=fba09f8d-9408-42d5-b64d-b3117a3a643e. France's Commission National de I'nformatique et des Liberts has established guidelines implementing the E-Privacy Directive that reminds website operators that "browser settings alone are not sufficient to fulfill EU privacy obligations" in the absence of other active consent. "France Still in Search of Perfect Cookie," reported in Steptoe & Johnson LLP E-Commerce Law Week (Issue 684, Nov, 26 2011) *available at* http://www.steptoe.com/publications-7903.html.

[8]*Id.*

[9]"UK Cookies Update: New Laws on Cookies and E-commerce," *Duane Morris Alert* (April 25, 2012) *available at* http://www.duanemorris.com/alerts/UK_cookies_update_new_laws_on_cookies_and_e-commerce_4436.html.

[10]*Id.*

[11]Commissioner's Findings, PIPED Act Case Summary #162, "Customer complains about airline's use of cookies' on its Web Site," (April 16, 2003), case summary *available at* http://www.priv.gc.ca/cf-dc/2003/cf-dc_030416_7_e.cfm, reported *in* "Canada: Airline Violated Privacy Law Using Computer Cookies," WORLD INTERNETL. REP. (BNA) at p.27 (July, 2003).

[12]Guidelines issued in late 2011 by the Canadian Privacy Commission make clear that information collected by companies for online behavioural advertising (OBA) purposes will "generally constitute personal information" under the Canadian Protection of Personal Information and Electronic Documents Act. Consequently, advertisers using OBA must have an OBA policy that is accessible, easy-to-read, and accurate. Moreover, the guidelines provide that individuals must be made aware that information is collected for OBA before it is collected, and opt-ing out must be a simple process. Finally, the guidelines state that websites targeting children should avoid tracking activities. Salzberg, "Privacy Commissioner Releases New Online Behavioural Advertising Guidelines," McCarthy Ttrault LLP (Dec. 21, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=a882d79f-d2dc-49c4-b713-c2aab63bb699.

[13]Hobby, Hollis, Johnson, Miller, Quittmeyer and Dodson, "India adopts new privacy and security rules for person information," Sutherland Asbill & Brennan LLP (Aug. 9, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=9a9b9ec0-e390-45b8-a6f1-4363e29e9af3. Among other things, the Rules require that (i) privacy policies are published on the websites of collectors of personal information; (ii) reasonable steps are taken to inform the individual that his or her information is being collected, the purpose for which it is being collected, the intended recipients of the information, and the name and address

of the entity collecting or retaining the information; (iii) individuals must be provided the right to review and correct inaccuracies in their personal information and a grievance procedure must be established to rectify complaints within one month of their receipt; and (iv) personal information is securely maintained. Moreover, certain additional restrictions apply to "sensitive personal data." *Id*.

[14]For more information on the Safe Harbor Agreement see the Commerce Department's website at http://www.export.gov/build/groups/public/@eg__main/@safeharbor/documents/webcontent/eg__main__018879.pdf.

[15]The notice must be specific. In a ruling dated January 13, 2005, the Spanish Data Protection Authority fined a Peugeot dealer for collecting data without "explicitly, precisely, and unequivocally in form[ing] the data subject about the purpose of collecting the data and the recipients of the information. Statements that data were collected "for commercial purposes" or "to send you offers about our products or services" were found inadequate, as were authorizations by the data subject to disclose "your data to the companies who are members of the Peugeot Group and of the Official Commercial Network." A more specific disclosure of purposes and recipients was required. Similarly, in March 2012 France's Commission Nationale de L'Informatique et des Liberts (CNIL) determined that Google's privacy policy was in violation of the Data Protection Directive because, according to CNIL, the policy "provides only general information about all the services and types of personal data Google process," making it "extremely difficult to know exactly which data is combined between which services for which purposes, even for trained privacy professionals." Halberstam, "The EU objection to Google's combined privacy policy explained—it's not what you do, it's the way that you do it," Kingsley Napley (March 14, 2012), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=f2df543d-6bec-4689-b6a2-faa4a6150c6b.

[16]See www.ita.doc.gov/td/ecom/shprinciplesfinal.htm.

[17]See J. Clausing, *Europe and U.S. Reach Data Privacy Pact*, N.Y. Times, Mar. 15, 2000.

[18]In November 2009 and January 2010, the FTC issued consent orders settling charges that six US companies (World Innovators, ExpatEdge Partners, Onyx Graphics, Directors Desk, Collectify and Progressive Gaitways) falsely claimed to have complied with the Safe Harbor framework in violation of section 5 of the FTC Act. The orders, which each remains in effect for a period of 20 years from the most recent date the U.S. or the FTC files a complaint alleging a violation of such order, require that the companies in question (i) not misrepresent expressly or by implication the extent to which they are a member of, adhere to, comply with, are certified by, are endorsed by or otherwise participate in any privacy, security or other compliance program sponsored by the government or any other third party, (ii) file with the FTC written reports regarding the manner and form of their compliance with the orders and (iii) maintain and upon request make available to the FTC copies of all documents relating to compliance with the orders for 5 years. The companies also could be subject to civil penalties if they engage in any such misrepresentations going forward. Krasnow, Glazer and Bildsten, "U.S. Companies Misrepresenting EU Data Protection Directive Safe Harbor Compliance Risk Federal Trade Commission Enforcement Action" *reported in* Lexology (May 11, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=71ce5496-4d5f-417f-be06-5e776df7d04d.

[19]See, e.g., *Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001) (summary judgment for defendant); *In re Doubleclick Privacy Litigation*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (summary judgment for defendant); *Rivera v. Match Logic, Inc.*, No. 00-K-2289 (D. Colo.) (filed Nov. 20, 2000), *reported in* 79 Antitrust & Trade Reg. Rep. (BNA) 569 (Dec. 15, 2000).

[20]As of January 18, 2005, there were 647 companies on the Department of Commerce's certified list, see http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list. Obviously, statements by companies that they comply must be truthful. In October 2009, the FTC announced that it had settled six enforcement actions with companies that falsely claimed they held current certifications under the EU/U.S. Safe Harbor Framework. *See FTC Settles with Six Companies Claiming to Comply with International Privacy Framework,* FTC Press Release (October 6, 2009), *available at* http://ftc.gov/opa/2009/10/safeharbor.shtm.

[21]Commission Staff Working Document, "The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour Principles and related Frequently Asked Questions issued by the US Department of Commerce," SEC (2004) 1323 (Oct. 20, 2004).

[22]"Opinion on More Harmonised Information Provisions," Article 29 Data Protection Working Party, 11987/04/EN, WP100 (Nov. 25, 2004), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf; "EU Issues Guidance on Privacy Notices," dmNews (Jan. 5, 2005), http://www.dmnews.com/cgi-bin/artprevbot.cgi?article_id=31430.

[23]J. Vijayan, "Companies Simply Data Privacy Notices," ComputerWorld (Jan. 10, 2005), http://www.computerworld.com/s/article/98812/Companies_Simplify_Data_Privacy_Notices.

[24]For example, Directive 95/46/EC of October 24, 1995, prohibits the unauthorized access to or the transfer out of the EU of an individual's personal data without consent. On January 19, 2008, the Working Party published its conclusion that "[s]earch engines fall under the EU Data Protection Directive 95/46/EC if there are controllers collecting users' IP addresses or search history information, and therefore have to comply with relevant provisions." The group concluded that the Directive applies to the search engines of companies who have "an establishment" in a EU member state or that use automated equipment based in a member state for processing personal data. *Press Release of the Article 29 Data Protection Working Party* (Feb. 19, 2008), *available at* http://ec.europa.eu/justice/policies/privacy/news/docs/pr_18_19_02_08_en.pdf.

[25]*See* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/01/851&format=HTML&aged=1&language=%20EN&guiLanguage=en; http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/12&format=HTML&aged=%200&language=EN&guiLanguage=en; "standard contractual clauses for the transfer or personal data to third countries—Frequently asked questions," MEMO/05/3 (Jan. 7, 2005), http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/3&format=HTML&aged=0&laungage=EN. In February 2010, the European Commission approved a new set of model contract clauses for the transfer of

personal data. *See* E-COMMERCE LAW WEEK (February 18, 2010), *available at* www.steptoe.com.

[26]"Outsourced Data Must Be Protected, Says U.K. Privacy Chief", The Register, July 17, 2006), http://www.theregister.co.uk/2006/07/12/outsourced_data_protection/.

[27]M. Watts, "Transferring Personal Data from the E.U.: Are Binding Corporate Rules the Answer?" 4 WORLD DATA PROTECTION REPORT (BNA) No. 3 (March 2004) at 1. Binding corporate rules are submitted for approval to the lead data protection agency—generally in the country where the business has its European headquarters—which then consults with data protection agencies in all affected EU countries before providing comments to the applicant for revision. M.L. Jones, "Data Protection—The E.U./U.S. Data Divide, WORLD TAX and LaAW REP. (BNA INT'L) No. 22 (Sept. 2005). The EU in 2005 set forth procedures for approval in two documents, "Working Documents Establishing a Model Checklist Application for Approval of Binding Corporate Rules," Article 29 Working Party, 05/ENWP/08 (April 14, 2005), *available at* http://www.steptoe.com/publications/352f.pdf; and "Working Document setting forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From Binding Corporate Rules," Article 29 Working Party, 05/EN WP/07 (April 14, 2005) *available at* http://www.steptoe.com/publications/352g.pdf.

[28]*Lindquist*, Case C-101/01 (Eur. Ct. Justice Nov. 6, 2003), *available at* http://curia.eu.int/jurisp/cgi-bin/gettext.pl?lang=en#=79968893C19010101&doc=T&ouvert=T&seance=ARRET.

[29]"Microsoft Faces European Commission Inquiry on Privacy Concerns," N.Y. Times, May 28, 2002, at p. C4.

[30]"European Union Microsoft Passport'—Commission Will Not Impose Sanctions," WORLD INTERNET L. REP NA) at 30 (Feb. 2003).

[31]Hunton & Williams, Privacy and E-Commerce Alert (March 14, 2003).

[32]http://www.hldataprotection.com/2010/04/articles/international-compliance-inclu/irish-court-ip-addresses-not-personal-data/.

[33]*Id.*

[34]"Privacy: French Agency Decries Bad-Credit Blacklist, Citing Sharing of Data Beyond Affected Sector," BANKING DAILY (December 17, 2003).

[35]*See* E-Commerce Law Week (March 20, 2010), *available at* www.steptoe.com/E-CommerceLawWeek.

[36]Baker, "Spanish cases against Google serve as a reminder of the need to take steps to allow data transfers from Europe to the US," reported in Lexology (November 8, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=b863f2b5-669a-4044-ac26-8dc015a87eae.

[37]*See Data Security—Information Commissioner's Office Guidance*, WORLD DATA PROTECTION REP.8 BNA (Jan.2008).

[38]*See* The Data Protection Regulations 2010 No. 31, *available at* http://www.opsi.gov.uk/si/si2010/pdf/uksi_20100031_en.pdf.

[39]Sarbanes Oxley Act of 2002 § 301; SEC Rule 10A-3(b)(3).

[40]Arbeitsgericht Wuppertal, Court order dated June 15, 2005, 5 BV 20/05.

[41]CNIL Decision 2005-110 of May 26, 2005 (Exide Technologies).

[42]CE Bsn Glasspack, Syndicat CGT/Bsn Glasspack, Tribunal de grande instance de Libourne Ordinance de rfr 15 Septembre 2005, *available at* http://www.legalis.net/jurisprudence-decision.php3?ID_article=1497.

[43]While French companies were already required to obtain CNIL approval for whistleblowing that exceeded the scope of the 2005 decision (see footnote 368, above), the French Court's decision helped to clarify exactly when such approval is available; namely, in matters related to accounting, finance, banking, anti-corruption, competition, Section 301(4) of Sarbanes-Oxley and the Japanese Sarbanes-Oxley. Martin, "French Data Protection Agency Restricts the Scope of the Whistleblowing Procedures: Multinational Companies Need to Make Sure They are Compliant," Lexology (December 15, 2010), *available at* http://www.lexology.com/library/detail.aspx?g=1d2fe56a-92c1-4d12-9436-cd9b9e21f26a.

[44]CNIL, "Guideline document adopted by CNIL on 10 November 2005 for the implementation of whistleblowing systems.,"*available at* http://www.cnil.fr/fileadmin/documents/en/CNIL-recommandations-whistleblowing-VA.pdf.

[45]ARTICLE 29 Data Protection Working Party, "Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime," Document 00195/06/EN, WP 117, adopted Feb. 1, 2006, *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

[46]Armstrong, Burnett and Davis, "Storms Gather for Data Protection in the Cloud," CMS Cameron McKenna (Aug. 16, 2011), *reported in* Lexology, *available at* http://www.lexology.com/library/detail.aspx?g=8089feda-5f7f-4a0b-b75d-0f83dba64130.

[47]D. Scheer, "Europe's New High Tech Role: Playing Privacy Cop to the World," WALL STREET JOURNAL (October10.2003) *available at* http://cryptome.org/eu-data-cop.htm.

[48]*Id.*

[49]See L. Conley, "Refusing to Gamble on Privacy," Fast Company, No. 84 (June 2004), http://www.fastcompany.com/magazine/84/essay_es.html; J. Vijayan, "Privacy Potholes," COMPUTERWORLD (March 15,2004), http://www.computerworld.com/printthis/2004/0,4814,91108,00.html).

[50]According to Steptoe & Johnson, *E-Commerce Law Week* (Aug. 28, 2008), new data protection requirements were being considered in Australia, Mexico, Turkey, South Korea, Peru and Vietnam, among other places. Many of these proposed laws would require mandatory notification to individuals affected by data breaches. *Available at* http://www.steptoe.com/publications-5495.html.

[51]Directive 95/46/EC. The Directive governs "processing" and "exporting" of "personal data." "Personal data" is defined broadly under the Directive, i.e., "any info relating to an indentified or identifiable natural person." *Managing the EU-U.S. Discovery Conflict,* "http://www.law360.com/articles/72082/managing-the-eu-us-discovery-conflict" (Oct. 16, 2008).

[52]*U.S. Discovery and E.U. Privacy: Irresistible Force*

vs. Immovable Object?, WORLD DATA PROTECTION REPORT (BNA) 19 (Jan. 2008). *See also* R. Davis, *European Privacy Laws An E-Discovery Stumbling Block*, Law360 (July 23, 2009), *available at* http://www.law360.com/articles/112287.

[53]U.S. Discovery and E.U. Privacy: Irresistible Force vs. Immovable Object?, WORLD DATA PROTECTION REPORT (BNA) 19 (Jan. 2008).

[54]*Id.*

[55]*Id.*

[56]*Id.*

[57]*Id.*

[58]*Id.*

[59]*Id.*

[60]*Id.* at 21, citing *Volkswagen, AG v. Valdez*, 909 S.W.2d 900 (Tex. 1995) (balancing the factors set forth in Section 442 of the Restatement (Third) of Foreign Relations Law); *Société Nationale v. Rogers*, 357 U.S. 197 (1958) (balancing the Congressional intent underlying the Trading with the Enemy Act with more protective Swiss privacy laws); *Richmond v. Timer Falling*, 959 F.2d 1468 (9th Cir. 1992) (balancing the factors set forth in Section 442 and applying the Socit Nationale standard); *Strauss v. Credit Lyonnais*, 242 F.R.D. 199 (E.D.N.Y. May 25, 2007) (balancing the factors set forth in Section 442 and denying the plaintiff's request for bank records as prohibited by French privacy laws). The factors set forth in Section 442 are (1) the importance to the investigation or litigation of the information; (2) the degree of specificity of the request; (3) whether the info originated in the U.S.; (4) the availability of alternative means for securing the info; and (5) the extent noncompliance would undermine foreign interests. Id.

[61]*IO Group Inc., et al. v. GLBT Ltd., et al.*, No. C-10-1282 MMC (DMR), 2011 WL 4974337 (N.D.Cal. 2011) (holding that a British website operator's destruction of e-mails in accordance with the U.K. Data Protection Act of 1998 would not excuse noncompliance with U.S. laws regarding spoliation), *reported in* "EU Privacy Law is No Excuse for Spoliation of Evidence," Steptoe & Johnson LLP E-Commerce Law Week (Issue 683, Nov. 19, 2011), *available at* http://www.steptoe.com/publications-7896.html.

[62]"Mexico's Constitution: for US Litigation Involving Mexican Entities, New Data Protections Could Create New Hurdles," *available at* http://www.dlapiper.com/latinamerica/publications/detail.aspx?pub=4469.

[63]"Uruguay's and Israel's Data Privacy Laws: Good Enough for Europe," reported in Steptoe & Johnson LLP E-Commerce Law Week (Issue 629, Week Ending October 30, 2010) *available at* http://www.steptoe.com/publications-7240.html.

[64]*See Commission Decision*, 2011/61/EU (31 Jan. 2011) (pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data), *available at* http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:EN:PDF.

[65]*Id.*

[66]*See* "Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses," *available at* "http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=EN&guiLanguage=en"; see also Keating, "Draft Regulation Prepared by the European Commission Proposes Fundamental Changes in European Union Privacy and Data Security Standards," Alston Privacy and Security Blog (Dec. 5, 2011), *available at* http://www.alstonprivacy.com/blog.aspx?entry=4485. Among other things, the proposed data rules would clarify the standards for obtaining and using subject data; limit permitted processing of personal data to the minimum amount necessary; contain a new right to be "forgotten" (i.e., have one's personal information erased upon demand); and contain new data breach notification standards. *Id.*

[67]Goetz, "A new world of EU data protection," Faegre Baker Daniels (Feb. 2, 2012) (also reporting that all such non-EU companies would have to appoint a representative in the EU unless it employs fewer than 250 workers), reported in Lexology, *available at* "http://www.lexology.com/library/detail.aspx?g=60b40d08-486a-41a5-8c72-8cf40e1278bb".

[68]"European Commission Issues New Data Protection Proposals," *Duane Morris Alert* (February 16, 2012) *available at* "http://www.duanemorris.com/printPreview?url=http://www.duanemorris.com/alerts/european_commission_issues_new_data_protection_proposals_4347.html".

