Privacy Regulation

Spring 2003

Table of Contents

Consumer Protection Committee
Computer and Internet Committee
Section of Antitrust Law
American Bar Association

Privacy Regulation

Spring 2003

Privacy Regulation is published two times a year by the American Bar Association Section of Antitrust Law Consumer Protection and Computer and Internet Committees. The views expressed in the Newsletter are the authors' only and not necessarily those of the American Bar Association, the Section of Antitrust Law, or the Consumer Protection and Computer and Internet Committees (or their subcommittees).

If you wish to comment on the contents of the Newsletter, please write to the American Bar Association, Section of Antitrust Law, 750 North Lake Shore Drive, Chicago, IL 60611.

From the Editor

The Consumer Protection and Computer & Internet Committees of the ABA Antitrust Section are pleased to present the second issue of Privacy Regulation Newsletter.

Each issue of this publication, which is delivered by e-mail semiannually to members of both committees who have registered for their respective Committee's Listservs, focuses on a specific, timely privacy issue. This issue is focused on developing, implementing, and managing a globally-compliant privacy policy. We are fortunate to have contributions from regulators and practitioners from around the world. Commissioner Mozelle W. Thompson and his Attorney Advisor, Peder Magee, lead with a discussion of the US-EU Safe Harbor agreement, including not only a summary of the Safe Harbor Principles and the benefits of certification, but also some insight into how the FTC may enforce Section 5 of the FTC Act against Safe Harbor participants.

Lynda Marshall and Mary Ellen Callahan of Hogan & Hartson follow with a piece discussing the various ways a multinational company may make cross-boarder transfers of personal information in compliance with the EU Directive, including the use of model contract clauses, obtaining the data subject's consent, and through Safe Harbor certification.

Gayle Hill of Freehills in Australia offers a thoughtful article on how multinational organizations can comply with international data protection laws when exchanging information among affiliated entities within a multinational organization.

We complete our treatment of European privacy issues with an article by Mike McNeely and Patrick O'Connor of Gray Cary on the differences in the way European and US regulators approached privacy issues associated with Microsoft's .NET Passport service.

Articles on privacy law in Canada (by Ariane Siegel and Brenda Pritchard of Gowlings in Toronto), and Australia (by Philippa Hore of Clayton Utz in Melbourne), and a piece on Privacy and Video Surveillance (by Lanise Hayes and Olimpia Policella of Studio Legale Imperiali) round out our issue.

I would like to thank members of the Editorial Board – David Evans of Arent Fox, Peder Magee, Attorney Advisor to FTC Commissioner Mozelle Thompson, and John Villafranco and Elisa Nemiroff, both of Collier Shannon, for their work to make sure that the articles we publish are accurate, complete and, most importantly, focused on assisting privacy law practitioners in their day-to-day work.

We hope that you will find this newsletter useful in your practice. If you have any questions, comments, or suggestions for improvement of this newsletter, please let me know.

D. Reed Freeman, Jr.
Collier Shannon Scott PLLC
Washington, DC
rfreeman@colliershannon.com

Privacy Regulation
Spring 2003

US/EU Safe Harbor Agreement: What It Is and What It Says About the Future of Cross Border Data Protection

The Honorable Mozelle W. Thompson[1]
Commissioner
Federal Trade Commission
Washington, DC

Peder van Wagonen Magee[1]
Federal Trade Commission
Washington, DC
pmagee@ftc.gov

In February 1999, the staffs of the United States Department of Commerce ("Commerce") and the Federal Trade Commission ("FTC" or "Commission") huddled together in an FTC conference room to discuss the European Union's ("EU") soon-to-be-implemented directive governing the collection and dissemination of personal data gathered from the citizens of its 15 member states.[2] At the time, America was in the middle of the "dot-com bubble" as consumers began to engage in e-commerce and companies found newer and more sophisticated ways to collect information about their cyber visitors. Both agencies were heavily involved with issues raised by the newly emerging global electronic marketplace: Commerce, with such issues as encryption, digital signatures and domain name registration; and the FTC with online marketing and consumer protection. It took little more than a cursory glance at the EU's new "Privacy Directive" to recognize that it could potentially block trans-Atlantic data flows. This bottleneck threatened not only to seriously hamper traditional international trade, but also to cause e-commerce to wither on the vine.

The Privacy Directive was one by-product of the European Commission's attempt at harmonizing the maze of 15 countries' laws and regulations governing a wide range of subjects -- including the gathering and dissemination of citizens' personal information. The Privacy Directive required member states to pass laws and take steps to protect the privacy of their citizens' personal data. Even more importantly, from a global perspective, the Privacy Directive also directed EU member States to prohibit transmissions of personal data to any entity that did not agree to provide similar protections.[3] This requirement created the potential for serious conflict with the United States ("US"), a country with no generally applicable law governing data protection.[4] Absent some agreement between

the US and the EU, the Privacy Directive threatened to disrupt trans-Atlantic commerce by blocking the ability of European organizations to transfer employee records, customer records and other types of personal data to companies in the United States. Neither the EU nor the US thought this was a desirable result.

The Privacy Directive's extraterritorial effect became a focus of Commerce and the FTC's attention. After several months of complex negotiations the US and the EU agreed upon an innovative framework that would act as a bridge for sharing data between the two continents, while preserving the basic policy principles of both. By establishing a self-certification process that incorporated seven required privacy policy elements, this "safe harbor" agreement allowed the data of European citizens to continue to flow to certain American companies.

This article provides a glimpse of the circumstances that surrounded the US and European safe harbor negotiations, summarizes how the safe harbor operates today, and provides guidance concerning future US action in the privacy area.

US Goals In The Safe Harbor Negotiations

In negotiating the substance of the US/EU Safe Harbor Principles, the US sought to advance certain policy goals. After examining the EU Privacy Directive and recognizing its potential impact on trans-Atlantic trade, Commerce and the FTC began to explore how to address the EU's data protection concerns while at the same time, respecting the sectoral approach of US data protection laws. Both agencies already believed that encouraging industry self-regulatory efforts in the online privacy area was good for consumers and good for e-commerce. Indeed, the US had already agreed to the 1988 Organization of Economic Cooperation and Development's ("OECD") Privacy Principles, and many US companies had already adopted some form of these nonbinding principles through participation in several self-regulatory bodies. (See e.g., The Online Privacy Alliance, Trust-E and BBB Online). Moreover, the FTC's authority under Section 5 of the Federal Trade Commission Act ("FTCA") to take action against unfair or deceptive trade practices, as well as the agency's strong enforcement background, provided a clear statutory and historical backdrop to bolster industry self regulation.

Accordingly, Commerce and the FTC sought to negotiate a safe harbor based on the following goals:

- Voluntary participation of American companies that received European data.
- Compliance standards that the US through the Department of Commerce (and not the EU) certified.
- Existing US law enforced by the FTC.

After some 17 months of discussions, in July 2000, the US and the European Union agreed upon a framework with a set of Safe Harbor Principles that satisfied each of these goals.[5]

Safe Harbor Requirements for US Companies

The safe harbor framework, including how companies can participate and certify their compliance, is set forth in detail on the Commerce and the FTC websites.[6] To summarize, the agreement allows most US corporations to certify to Commerce that the company has joined a self-regulatory organization that adheres to the following seven Safe Harbor Principles or has implemented its own privacy policies that conform with these principles. A self-certifying organization must do the following:

- Notify individuals about the purposes for which information is collected and used;
- Give individuals the choice of whether their information can be disclosed to a third party;
- Ensure that if it transfers personal information to a third party, that the third party also provides the same level of privacy protection;
- Allow individuals access to their personal information;
- Take reasonable security precautions to protect collected data from loss, misuse or disclosure;
- Take reasonable steps to ensure the integrity of the data collected; and
- Have in place an adequate enforcement mechanism.

Since the creation of the Safe Harbor Principles, Commerce has certified over 300 companies as qualifying for the safe harbor. That figure includes over 6% of the Fortune 500 companies. Jay Cline, Safe Harbor: A Success, Computerworld (Feb. 19, 2003).

The Safe Harbor and FTC Enforcement Actions

It is well-settled that the FTC has authority to sue a company that makes public representations which it fails to fulfill. See e.g., Deception Policy Statement, Cliffdale Associates, Inc., 103 F.T.C. 110, 176 (1984). The Commission has also determined that this authority extends to a company's violation of its privacy policy or other misrepresentations concerning its information practices. See Toysmart.com,, Civil Action No. 00-11341 (D.MA. July 21, 2000); GeoCities, Docket No. C-3849 (Final Order Feb 12, 1999). This same statutory jurisdiction will serve as the primary basis for government action against a US company that obtains safe harbor certification but fails to comply with the Safe Harbor Principles.[7] To date, Commerce and the FTC have not received any complaints about privacy breaches committed by any of the registered American companies. Notwithstanding this lack of complaints, however, the FTC has increased its privacy enforcement activities, and two recent actions illustrate how the Commission might pursue safe harbor enforcement.

Microsoft Passport

In August of 2002, Microsoft settled FTC allegations that the company had made deceptive claims about the security of its Passport Internet service and about the types of customer information it collected in connection with the service. Microsoft Corp., Docket No. C-4069 (Final Order Aug. 8, 2002). Microsoft's Passport system collects and maintains consumers' personal information and allows consumers to use the stored data in making online purchases through participating web sites. Following an investigation, the FTC concluded that Microsoft had falsely claimed that "it maintained a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information" of its Passport consumers. Microsoft Corp., Docket No. C-4069, Complaint at para. 6. Additionally, the FTC asserted, Microsoft had deceived consumers by failing to disclose that it collected personally-identifiable, sign-in history data from its Passport customers.

In analyzing whether the Microsoft Passport security measures were reasonable and appropriate, the Commission looked closely at the nature of the underlying data. Although Microsoft did have some security measures in place to protect its customer data, because of the sensitive nature of such data -- including consumers' credit card information -- the Commission determined that Microsoft's security was insufficient. Similarly, even though Microsoft collected and retained the customer sign-in history data for only a limited time, the sensitivity of those data made the failure to disclose its collection a deceptive omission, in violation of Section 5.

The FTC settled its allegations against Microsoft when the company agreed to an order that enjoined it from misrepresenting its information practices and required it to implement and maintain a comprehensive information security program that is subject to the review and certification of an independent third-party review organization.[8] This remedy is significant because it represents the first time that a private corporation has agreed to regular, independent third party review of its privacy and information security practices in the context of a Commission order.

Eli Lilly

A second matter involving allegations of privacy violations and inadequate data security, involved the pharmaceutical company Eli Lilly ("Lilly"). Eli Lilly and Co., Docket No. 4047, (Final Order May 8, 2002). Through its Prozac.com Web site, Lilly collected personal data and offered customers its "Medi-messenger" service which sent consumers personal e-mail reminders to take or refill their medication prescriptions. Privacy policies that Lilly posted on its website stated that the company took the necessary steps to maintain and protect the privacy and confidentiality of its customers' personal information.

The Commission challenged Lilly's privacy and security claims as deceptive under Section 5 after a Lilly employee unintentionally distributed an e-mail that disclosed the identities of some 700 of Lilly's prosac.com subscribers. Despite the unintentional nature of the disclosure, the FTC determined that Lilly's internal privacy and security measures were inadequate given the highly sensitive nature of the data at issue and the express representations the company had made regarding the security of that information. The Commission further found that Lilly had failed to provide "appropriate training for its employees regarding consumer privacy and information security" and had failed to "implement appropriate checks and controls" over the prozac e-mail program. Eli Lilly and Co., Docket No. 4047, Complaint at para. 7.

The FTC's settlement with Lilly bars the company from making misrepresentations about the privacy or security of the company's consumer information. The settlement also requires Lilly to establish a four-stage information security program that identifies "reasonably foreseeable internal and external risks to security, confidentiality, and integrity of personal information." Decision and Order at para. II.

Lessons Learned from Microsoft Passport and Eli Lilly

Microsoft and Eli Lilly are both American companies that market to consumers worldwide. Both companies made public representations about the use and security of the personal information they collected and both were alleged to have violated their own public representations. Although neither action was specifically characterized as a safe harbor case,[9] they both provide insight into how the Commission might approach enforcement of the Safe Harbor Principles.

It is evident through these cases that the FTC will evaluate whether a company has taken "reasonable precautions" to protect the security of its consumer data, based on the sensitivity of the data at issue. This "sliding scale" — as opposed to an inflexible, a one-size-fits all approach – can apply to other Safe Harbor Principles as well. The level of choice a company must offer its customers concerning data collection (opt-out versus opt-in) depends upon the sensitivity of the data being sought. Similarly, the judgment about the sufficiency of a company's data access program requires consideration of the type of data collected weighed against the burden and the risk to the company.

Each case will obviously be driven by its specific facts; however, it is likely that judgments about reasonableness will differ where the data involved is financial, medical, or some other type of highly sensitive information. Therefore, these questions could form the basis for future actions where there is a claim of breach of the Safe Harbor Principles.

Conclusion

With this background in mind we can provide some advice for those who are counseling organizations that collect, receive, or otherwise use consumer information. First, they should advise their clients to identify whether the client collects or receives personal information from consumers and, if so, what kind of information it is.[10] Second, they should advise organizations that collect or receive data from EU citizens to strongly consider applying for safe harbor certification. While certification requires that the organization take some responsibility for how it collects and uses personal data, this exposure is likely to be far less serious than the risk of facing legal actions brought by each of the 15 EU Data Commissioners.[11] Finally, an organization should take steps to ensure that it is fulfilling its privacy policies, whether or not it is certified through the safe harbor. This last point is important not only because of the risk of FTC enforcement, but also because it makes good business sense.

(Endnotes)

1 Mozelle W. Thompson is a Commissioner at the United States Federal Trade Commission. He participated in the negotiations leading to the US/EU Safe Harbor Principles and agreement as head of the United States Delegation to the Organization for Economic Cooperation and Development Consumer Policy Committee. Commissioner Thompson now serves as Chairman of the Committee. Peder Magee is Attorney Advisor to Commissioner Thompson, working on various consumer protection and competition matters with specific emphasis on online privacy, global e-commerce, and high technology matters. The views expressed in this article are those of the authors, and do not necessarily reflect the views of the Federal Trade Commission or any other individual Commissioner or Commission employee.

2 The EU members include Austria, Belgium, Denmark, Finland, France, Germany, Greece, Italy, Ireland, Luxembourg, The Netherlands, Portugal, Sweden, Spain, and the United Kingdom.

3 "Member States shall provide that the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection." Council Directive 95/46/EC, 1995 O.J. (L 281) 31, Article 25.

4 Unlike Europe's "top-down" regulatory approach to privacy protection, historically the US has taken a "sectoral" approach mixing self-regulation with certain discrete legislation pertaining to specific industries. See, e.g., Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act. Some would argue that these differences create the perception that European privacy protections focus more on legal principles, while America's privacy protections are more focused on enforcement.

5 It is important to keep in mind that the US and the EU are continuing to negotiate the safe harbor with respect to certain issues such as financial institutions. The current safe harbor does not apply to financial institutions and there is a de facto moratorium by the EU on pursuing financial institutions that transfer personal information to organizations in the US. The extent to which the Gramm-Leach-Bliley Act is sufficient for purposes of the Privacy Directive is an unresolved issue to which US companies and their counsel should pay close attention.

6 See United States Department of Commerce, Export Portal, http://www.export.gov/safeharbor/sh_overview.html. Financial and insurance organizations, telecommunications companies and not-for-profits are ineligible for safe harbor certification.

7 The Department of Commerce publishes a list on its website containing the names of each organization that obtains safe harbor certification (http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list). The FTC views this publication as an affirmative representation which is actionable if violated. Letter from Robert Pitofsky, Chairman, Fed. Trade Comm'n, to John Mogg, Director, DG XV, European Comm'n (July 14, 2000), available at http://www.export.gov/safeharbor/FTCLETTERFINAL.htm.

8 It is important to note that the Passport investigation did not arise from specific consumer complaints, but was instead prompted by a request from a coalition of public interest groups. Consequently, there was no provision for consumer redress.

9 Microsoft is a certified safe harbor company and the EU has looked at its Passport system; however, the Commission's allegations did not specifically concern the safe harbor.

10 Companies that collect data online from children under 13, for example, must comply with COPPA.

11 These actions can stem from violations of each country's laws governing the collection and use of personal information.

Privacy
Regulation
Spring 2003

The European Union Data Directive: Implications for United States and Multinational Companies

Lynda K. Marshall[1]
Hogan & Hartson LLP
Washington, DC
lkmarshall@hhlaw.com

Mary Ellen Callahan[1]
Hogan & Hartson LLP
Washington, DC
mecallahan@ftc.gov

Over the past few years, United States companies have faced several challenges in implementing the EU Directive on Data Protection (the "Directive"),[2] as applied through national law of the EU Member States. One of the most difficult of these challenges has been the Directive's mandate that transfers of personal data[3] outside the EU are possible only if the country to which the data being transferred has "adequate protections." The Directive's definition of adequate protections is less than clear; it states only that the adequacy of the level of protection should be assessed in light of all circumstances surrounding the transfer, giving particular consideration to "the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law. . . and the professional rules and security measures which are complied with in that country."[4] What is clear, however, is that the laws of very few countries meet this standard. The privacy laws of the United States do not. Consequently, the transfer of personal data from the EU to the US, without any additional precautions, is contrary to the Directive and Member State laws implementing the Directive.

This portion of the Directive has significant repercussions for US companies with operations in the EU. US businesses move unknown quantities of personal data between the US and the EU daily; all types of data from employee records to customer names to proxy mailing lists are exchanged in electronic form. These transfers, even if they may be intra-company transfers, have the potential to violate the Directive.

Fortunately, both the EU and the US governments recognized this potential and took steps to avert it. There are mechanisms through which a US entity can legally transfer personal data from the EU to the US – it can join Safe Harbor, enter into a Model Contract, or obtain the data subject's[5] individual consent to the transfer. Each of these options can

create "adequate protections" in accord with the Directive. None of these options, however, are "one size fits all" solutions for the legal transfer of personal data between the EU and the US.

The simplest solution to the transfer prohibition often may be to obtain the data subject's consent to the transfer. This consent must be "unambiguous," which in certain Member States means that the data subject must be told in writing that her data are being transferred outside the EU to a country "without adequate data protections." It also may be necessary to specify in the consent the exact destination of the personal data, citing the receiving entity and listing its contact information. The information that must be specified in the consent may vary from Member State to Member State, but because the scope of the allowable export will be defined by the scope of the consent, it is important in every Member State that the consent be clear and exact.

Consent is not always the appropriate solution, however. First, consent must be obtained for each type of transfer. If disclosure that personal data "X" would be transferred was not included in the original consent, the entity proposing to transfer personal data "X" must go back to the data subject and obtain a new consent for the transfer of those specific data. Additionally, the data protection authorities of some Member States question the legitimacy of using consent in certain circumstances. For example, in France the use of consent for processing employee data is highly controversial and therefore not always advisable. In Belgium, consent for the transfer of health-related data is invalid if the data subject is employed by the data controller (the entity directing the transfer) or is otherwise dependent on the data controller. Belgian law does not consider consent to be freely given in those circumstances. Recent discussion within the EU seems to indicate that the situations in which consent can be "unambiguous" may become more limited in the future.

A second option for the transfer of data is to join the Safe Harbor program. This option is available only to entities subject to the jurisdiction of the United States Federal Trade Commission ("FTC") and the United States Department of Transportation ("DOT") because, as of today, the FTC and DOT are the only US governmental agencies that have committed to use their authority to prohibit unfair and deceptive acts to enforce Safe Harbor. In a nutshell, by agreeing to adhere to Safe Harbor's seven basic principles – notice, choice, onward transfer obligations, security, data integrity, access, and enforcement – a Safe Harbor member agrees to treat data from the EU in a manner very similar to that required by the Directive. Moreover, the enforcement principle and FTC/DOT oversight are designed to ensure that violations of the Safe Harbor have similar consequences as do violations of the Directive. The program is somewhat flexible, however, in that Safe Harbor Members specify the scope of their Safe Harbor membership by specifying the types of personal data to be covered. Note, however, that a narrow declaration may mean the entity could be in compliance with the Directive in some areas of its busi-

ness, but not in others.

Like consent, the Safe Harbor is not a complete solution. Most notably, it does not cover certain entities, such as financial institutions, telecommunications carriers, and non-profit organizations, because these entities are not always subject to FTC or DOT jurisdiction. Furthermore, the Safe Harbor will only cover information transferred to the United States. For a multinational company that ships personal data all over the world, joining the Safe Harbor only solves one part of the EU data export problem. Finally, once a party joins the Safe Harbor (and publicly proclaims its membership), the data exported during the time the entity was under the Safe Harbor must be treated according to the Safe Harbor principles forever, even if the entity later drops out of the Safe Harbor program.

The third solution to the issue of legally exporting data outside of the EU is to enter into the EU Model Contract. Like the Safe Harbor, the Model Contract is a way of imposing the rights and obligations set out in the Directive on an entity outside of the Directive's jurisdiction. Through the contract, the party receiving the data agrees to certain notice, choice, access, integrity, and security principles. The contract, which is governed by the law of the data exporter's Member State, sets out the scope of the allowable transfer and designates the data subject as a third party beneficiary of the contract. The parties are jointly and severally liable for damages suffered by the data subject, with mutual indemnification unless they prove neither of them is responsible for the breach.

As with the previously outlined export solutions, the Model Contract has drawbacks. First, altering the terms of the contract may invalidate it; individualized contracts that deviate from the EU Model Contract must be approved by the Member State Data Protection Authorities. Because the Directive has not yet been implemented in France, the unwritten practice is for parties to submit even the standard Model Contract for approval by the French data protection authority. Second, in order to ensure the legal export of data, an entity may have to enter multiple contracts – each receiving entity and all exported data must be covered by a contract. This means that a parent organization may have contracts with subsidiaries and affiliates that vary in terms and that are governed by different Member State laws. Furthermore, it is not clear if an entity, by contracting with a non-US office that is not a separate legal entity, would be contracting with itself and, if so, whether this creates a binding contract.

In the face of the various pros and cons associated with the legal obligations involved in exporting data from the EU, many US companies have chosen to disregard the Directive's requirements and continue "business as usual." The price associated with this course of conduct can be high. The EU Member States do enforce the data export restrictions and the consequences for failure to comply with the law can range from civil fines and criminal convictions to prohibitions on certain data processing ac-

tivities. Just going through an investigation alone can be time consuming and expensive. Examples of companies that have done so include Microsoft, which in 2001 paid a fine of approximately US $58,000 to the Spanish data protection agency for exporting data to the US, and eBay, which ran afoul of the Dutch data protection authority when, as part of merger integration activities, it attempted to transfer to the US customer information from the newly-acquired iBazar, a company operating auction websites in Europe. Microsoft has since joined the Safe Harbor.

In addition to raising complex compliance obligations, the EU export restrictions also have interesting implications for US privacy. Whether a company chooses to conform with export restrictions of the Directive, as implemented by Member State laws, through consent, the Safe Harbor, or the Model Contract, only the information transferred from the EU and specified in one of these options is covered by the "adequate protections." Therefore, according to the commitments made by the company to the EU and, in the case of the Safe Harbor, to the FTC or the DOT, only specified information must be treated with that high standard of care. The company, however, might also be under an obligation to handle other data according to the relevant US laws such as the financial privacy Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act. These multiple obligations with varying requirements make a difficult patchwork for multinational companies.

There might be an additional pitfall for multinational companies that decide to abide by the Directive with the Safe Harbor, which requires a public proclamation. Although there is no specific US legislation on personally identifiable information of adults other than those listed above, companies must store and use information in a manner consistent with its public statements (such as in a privacy policy), or else they could be found in violation of Section 5 of the FTC Act for deceptive acts or material mispresentations. An issue that has not yet been addressed is whether an organization that has announced its compliance with the Safe Harbor (published on the US Department of Commerce's website) has made a public statement with regard to public expectations about how US-based data will be handled. Such unclear relationships between EU and US obligations further cloud an already difficult implementation structure for multinational companies managing personal data from around the world.

In sum, the export restrictions of the Directive, particularly when combined with any US privacy obligations, raise significant implementation challenges for US and multinational companies operating in Europe. These challenges have the potential to affect not only the European operations of a company, but its US operations as well. How companies choose to meet these challenges will have an important impact on the evolution of data protection law both at home and abroad.

(Endnotes)

1 Lynda K. Marshall is a partner, and Mary Ellen Callahan is an associate, in Hogan & Hartson's Antitrust, Competition and Consumer Protection practice group in Washington D.C. Ms. Marshall has extensive experience working with in the EU Directive, while Ms. Callahan focuses primarily on U.S. privacy issues.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data, 1995 O.J. (L281) 31 – 50 ("EU Directive on Data Protection" or "EU Directive").

3 Personal data as defined by the Directive means any information relating to an identified or identifiable natural person. See Article 2(a) of the Directive.

4 Directive, Art. 25.

5 The data subject is the individual whom the information concerns.

Privacy
Regulation
Spring 2003

Harmony or Discord? Using Intra-Group Contracts to Address International Data Protection Standards

Gayle Hill[1]
Freehils
Melbourne
gayle.hill@freehills.com

Multinational corporate groups seeking to reap the benefits of globalization must inevitably grapple with the vexed and seemingly intractable challenge of complying with multiple data protection and privacy regimes.

At the heart of the issue lies the requirement under the European Data Protection Directive[2] ("Data Protection Directive") with respect to international data transfers. The export of personal data from any European Union ("EU") member state or from any European Economic Area member country to a third country is restricted unless the recipient country ensures an "adequate level of protection"[3] for that personal data. Because a number of non-European countries have now legislated to protect personal data, transfers of such data from those countries will be restricted by any transborder data flow ("TBDF") provisions that are imposed under the law of the exporting country.

Accordingly, multinational corporates ("MNCs") are likely to find that the countries in which they operate include any or all of the following classifications:

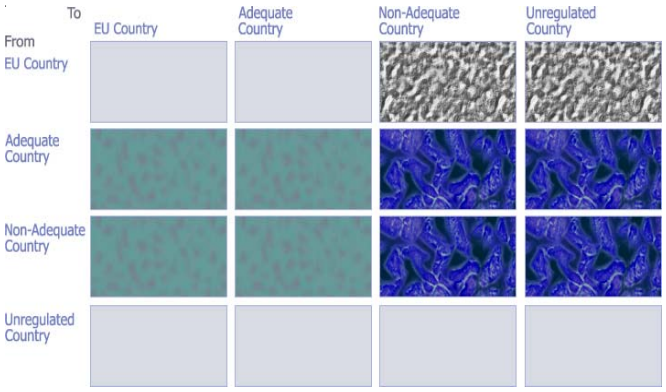
- EU countries — European countries having laws that mirror the Data Protection Directive restrictions on TBDFs (e.g., Great Britain).
- Adequate countries — countries with data protection laws or schemes that have been assessed as "adequate" for the purposes of the Data Protection Directive (e.g., Switzerland, Hungary, Canada and, in those situations where the relevant company participates in the "Safe Harbor" scheme, the United States[4]).

- Non-adequate countries — countries with data protection laws that either have not been conclusively assessed or have been assessed as "non-adequate" for the purposes of the Data Protection Directive (e.g., Australia).
- Unregulated countries — countries in which personal data is not protected (e.g., India).

Transferring personal data within the MNC but across national territorial boundaries requires that the entity exporting the data adhere to its own domestic laws (if any) that govern TBDFs. Further, the recipient entity in the corporate group might be required by the exporter to adhere to standards established under the laws of that exporting country.

A simple diagram to explain the resultant web of personal data protection restrictions that potentially apply to TBDFs within the MNC is set forth below. The complexity of the situation is further exacerbated when a recipient company in the MNC seeks to transfer personal data to another country.

International Transfers of Data



No restriciton on international transfer of personal data.[5]

Exporter must ensure data protection standards are imposed in accordance with the law in the exporter's country.

Depends on the details of the law in the exporter's country but it is likely that the international transfer is not inhibited because the personal data are protected under the laws or scheme of the importer's country to standards that are acceptable under the law of the exporter's country.

Depends on the details of the law in the exporter's country but it is likely that restrictions on the international transfer must be imposed by the exporter in accordance with the law in the exporter's country because data are not protected at all or are protected to standards that are unacceptable under the law of the exporter's country.

In this complex international regulatory environment, isolated and infrequent international data transfers, while presenting obvious complications, can be addressed under specific arrangements between the exporter and the importer of the personal data. Such arrangements are cumbersome but nevertheless achievable.

Global organizations are increasingly unlikely, however, to operate in such a simplistic capacity. To take advantage of globalization, MNCs strive to gain efficiencies out of streamlining their operations and reducing duplication of processes. MNCs may seek to warehouse greater volumes of the data that they hold in fewer locations or in common databases accessible by entities in various locations around the world. As a result, the entities in their groups will need to transfer personal data internationally and receive data from other countries. MNCs often structure the processes within their group with the goal of ensuring that the flow of information between the members can occur as quickly and as freely as possible to and from multiple points in the MNC at any time.

Whatever the internal mechanics adopted by the MNC, it is a considerable impediment to competitive efficiency if the multinational fails or is unable to implement a system that harmonizes the various data protection and privacy standards attached to personal data transferred across national borders. Nevertheless, it is imperative for the group to do so if it is to achieve compliance with data protection and privacy regulation.

Although the "adequacy" process under the Data Protection Directive offers some assistance at a macro level, the table above clearly illustrates that MNCs having European operations will be disadvantaged if any of the other countries in which they operate have laws that do not meet the standards required to be deemed as "adequate." Whether or not a country has legislation that is "adequate" for the purposes of the Data Protection Directive is essentially in the hands of the domestic legislature and is not an outcome that the MNC can guarantee.

Assuming that the TBDFs do not fall within the specific derogations in the Data Protection Directive,[6] which is highly unlikely when vast amounts of data are being transferred regularly for varying purposes by different entities in the group, alternative arrangements must be implemented. Other means by which MNCs can seek to resolve the dilemma of harmonizing multiple data protection standards at a micro level include the following arrangements:

- Use of the standard contractual terms that have been approved by the European Commission ("EC") for those purposes; and
- Development of a non-standard intra-group agreement to govern TBDFs within the group.

The EU Model (or Standard) Contracts

Under Article 26(4) of the Data Protection Directive, the EC has the power to decide whether certain standard contractual clauses offer sufficient safeguards to ensure adequate protection for personal data transferred internationally from the EU. Pursuant to this power, the EC promulgated standard contractual clauses to facilitate the transfer of personal data to non-EU countries. The two versions of the clauses respectively address the TBDF:

- To an importer that is to be a controller of the data[7]; and
- To an importer that is merely to undertake processing of the data on behalf of the exporter.[8]

A data controller exporting personal data from an EU country on the terms contained in the model contracts does not need to seek the prior approval of that country's data protection regulator, thereby alleviating an onerous administrative burden. The model contracts are intended to expedite TBDFs between organizations operating in different jurisdictions and under different data protection standards, including MNCs.

However, the model clauses themselves may not offer an attractive option to many global organizations. The clauses have been criticised as flawed and inflexible; unable to accommodate different types of organizations, recipient countries, and personal data; imposing a "one size fits all" approach; and, arguably, requiring separate terms for each of the EU countries.[9]

Although global organizations may be prepared to live with some difficulties in effecting TBDFs, it is the model clauses themselves that present the greatest obstacle. The roadblock potentially arises when the model terms are reviewed by lawyers practicing in any of the Non-adequate or Unregulated countries in which the multinational operates. For example, the entity's local legal counsel may advise that the model clauses~

- Are very onerous;
- Require observance of the exporting entity's laws when the importer is in no position to know or ascertain those laws;
- Go well beyond what would otherwise be required under the importing entity's local laws;
- Incorporate concepts that are not recognized under that country's laws, particularly the purported granting of rights to enforce the terms and bring an action in a court even though privity of contract principles preclude such third party rights; and
- Include a reverse onus of proof with respect to establishing an entitlement to compensation for violation of the terms.

As a result, prudent local counsel is likely to advise against agreeing to the standard contractual terms and disapprove contracts incorporating those terms.

Non-Standard Intra-Group TBDF Agreements

Another potential solution for MNCs is the use of an intra-group TBDF agreement that does not adopt the model clauses; in other words, is a non-standard contract. This approach involves the various group entities entering into an agreement governing their TBDFs. The terms must address deficiencies in levels of protection in recipient countries by raising the standards of protection whenever those standards fall below what is regarded as "adequate."

For situations in which data may be transferred within the MNC, an entity that is exporting data from an EU country would face the onerous task of attempting to determine whether all other likely recipients are subject to laws that are "adequate."[10] Such an analysis requires an assessment of the data protection standards applicable in the recipient countries and the means by which their application is ensured.[11]

Exporting entities will often not be in a position to assess the adequacy of the laws of other countries. The intra-group TBDF agreement could set out basic data protection standards. Data recipients would be required to handle any internationally transferred personal data in accordance with the data protection laws of the recipient's country. In the absence of such local laws or to the extent that the basic standards in the agreement are higher than those of the local laws, recipients must handle the data in accordance with those basic standards. The recipients would be required to comply with instructions of the exporter when handling the data as a mere processor (as opposed to a controller).

This approach means that the data exporter is not obliged to determine adequacy for any TBDF because adequacy is assured under the agreement. The basic standards set out in the intra-group TBDF agreement could be modeled on the mandatory data protection principles in the standard contractual clauses for the transfer of personal data to third countries.[12]

However, to guarantee a minimum level of protection, the intra-group TBDF agreement must include enforcement mechanisms. The third party beneficiary clauses typically used by EU countries pose the same problems under privity of contract principles that exist for the EU model contracts. A possible solution might be for the exporter to be obliged to enforce the obligations of the recipient entity for the benefit of data subjects adversely affected by a recipient's mishandling of personal data. Such a provision would apply only where third party beneficiary rights purported to be granted to data subjects are not recognized by local law.

There remains a problem, however, if the exporter fails to bring the recipient to account. A safety net could be provided by ensuring that, if the data subject is denied redress under local laws, the agreement is governed by the laws of a country that does enable the third party rights to be enforced (e.g., the laws of England and Wales). Practically, though, a data subject not resident in that country would still face problems.

Non-standard intra-group TBDF agreements may also prove to be administratively burdensome where exporters are obliged under local laws to obtain the approval of the local data protection regulator prior to any TBDFs. Under the Data Protection Act 1998 (United Kingdom), such approval is not required. The UK Data Protection Commissioner has sensibly taken the view that the data exporter must determine how it ensures compliance with the legislation and should be able to defend its actions should it be called to account subsequently.[13]

If the approval of numerous regulators is required, an alternative might be to seek the endorsement of the EC itself under the same process followed for the EU model clauses. If that occurred, European data protection authorities would be obliged to recognize that TBDFs under an approved intra-group agreement would enjoy adequate protection, even if those authorities still require notification of the agreement under their own local laws. Background information that accompanied Decision 2002/16/EC stated:

> *The Commission has declared its readiness to examine and if appropriate approve other sets of standard contractual clauses submitted by business organizations or other interested parties.*[14]

It is not clear from the above if an intra-group TBDF agreement would be regarded by the EC as a "set of standard contractual clauses," or if the EC would limit itself to approving standard clauses submitted on behalf of industry sectors.

Clearly, however, the global business community will continue to struggle with TBDF compliance and with harmonizing international data protection standards until more streamlined and simplified ways of addressing the regulatory requirements can be achieved. The need for a common EU-wide approval process to facilitate intra-group TBDF arrangements is self-evident and must be one of the next challenges to resolve in this area.

(Endnotes)

1 Gayle Hill is a special counsel in the Melbourne office of Freehills, one of Australia's major commercial law firms, and advises in the area of privacy law and practice. She is the national co-ordinator of Freehills privacy law team. Before joining Freehills in 1996, Gayle was a senior in-house counsel at Australia's major telecommunications corporation where she had corporate legal responsibility for privacy. Gayle was assisted in the preparation of this article by Steven Powell who until recently was a privacy adviser at Freehills who has held various positions as a privacy manager and adviser during more than 15 years working in this area of the law.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995.

3 Id. Article 25(1).

4 Details of the Safe Harbor scheme are available at: http://www.export.gov/safeharbor/sh_documents.html.

5 For present purposes, disparities in the way in which different EU countries have implemented the Data Protection Directive have not been canvassed. For a discussion on the need for a consistent European-wide data protection law, see "95/46: The Case for Proper Reform" by Tim Pullen, World Data Protection Report Volume 2 Issue 12 Dec. 2002 (BNA International Inc) p. 14.

6 Article 26(1) of the Data Protection Directive permits TBDFs to a Non-adequate country in limited specified circumstances.

7 European Commission Decision 2001/497/EC (15 June 2001).

8 European Commission Decision 2002/16/EC (27 Dec. 2001).

9 Tim Pullen at 17.

10 For guidance on assessing "adequacy" see: European Commission WP 12 (5025/98) Working document: "Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive", adopted on 24 July 1998 by the Working Party on the Protection of Individuals with regard to the Processing of Personal Data; and UK Data Protection Commissioner "The Eighth Data Protection Principle and Transborder Dataflows" July 1999, which is a preliminary view of the Data Protection Commissioner on assessing adequacy including consideration of the issue of contractual solutions and is available at: http://www.dataprotection.gov.uk/dpr/dpdoc.nsf.

11 European WP 12 (5025/98) at p. 5.

12 European Commission Decision 2001/497/EC, ibid, Appendix 2.

13 UK Data Protection Commissioner "International Transfers of Personal Data: Advice on compliance with the 8th data protection principle" para 9.5. Available at: http://www.dataprotection.gov.uk/dpr/dpdoc.nsf.

14 Background documentation dated 22 Jan. 2002 accompanying European Commission Decision 2002/16/EC (27 December 2001). Available at: http://europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-102.htm.

Privacy
Regulation
Spring 2003

Privacy Regulation on Both Sides of the Pond: Lessons from Microsoft .NET Passport

Mike McNeely
Gray Cary Ware & Freidenrich LLP
Washington, DC
mmcneely@graycary.com

Patrick O'Connor
Gray Cary Ware & Freidenrich LLP
Washington, DC
poconnor@graycary.com

Companies using the Internet to deal with consumers in more than one country may face a complex task in complying with those countries' regulations protecting privacy. Two recent agreements between Microsoft and privacy regulators in the United States and the European Union illustrate the differences between privacy regulation in the United States and the EU, and at the same time suggest practical approaches to compliance in both jurisdictions.[1]

Microsoft .NET Passport

The subject of these agreements is .NET Passport, Microsoft's digital identity authentication service.[2] Its users create a single sign-in name and password for use in accessing and interacting with .NET Passport's participating sites and services, eliminating the need for users to remember and manage multiple website identifiers and passwords. .NET Passport account creation requires at least an email address and password, and additional user information may include the user's name, address information, language, time zone, gender, birth date, and occupation.[3]

Evidently recognizing the sensitivity of the information it was collecting for .Net Passport, Microsoft's web site made a variety of claims extolling the security associated with the service. Microsoft claimed, for example, that ".Net Passport achieves a high level of Web Security," and promised "safer online purchases" with the system.[4]

Federal Trade Commission Consent Order

Acting on the complaints of several consumer advocacy organizations,[5] the United States Federal Trade Commission ("FTC") investigated .NET Passport. Based on this investigation, the Commission found reason to believe that Microsoft had violated the FTC Act's prohibition on unfair

or deceptive acts or practices,[6] and Microsoft agreed to a Consent Order.[7] The Commission examined Microsoft's performance in preventing unauthorized access to the .NET Passport system, detecting such unauthorized access, monitoring the .NET Passport system for potential vulnerabilities, and retaining information sufficient to permit system audits.[8] According to the FTC complaint accompanying the Consent Order, in light of Microsoft's actual performance, its statements describing the privacy and security of .NET Passport information were false or misleading and thus a violation of the FTC Act.[9] For example, Microsoft's failure to prevent unauthorized access to the .NET Passport system made its claim that ".NET Passport is protected by powerful online security technology and a strict privacy policy"[10] deceptive.

The Consent Order must require that Microsoft cease and desist from any misrepresentation of the information practices associated with Microsoft .NET Passport.[11] In addition, Microsoft must develop and maintain a comprehensive security program. As part of this program, Microsoft must (1) designate an employee responsible for information security compliance, (2) establish a risk assessment program for the security, confidentiality, and integrity of customer information, (3) design and implement controls to protect against the risks identified, and (4) revise the security program in light of the risks identified in the risk assessment.[12] The Consent Order also requires biannual assessments by an accredited and independent third-party to ensure that the security program complies with the Order's requirements.[13]

One notable aspect of the Consent Order is its requirement that Microsoft significantly improve its programs for safeguarding user data. By requiring that Microsoft revamp its information security system, the FTC has identified particular practices for protecting information that Microsoft must adopt to ensure that its representations about those practices will not be deceptive and illegal under the FTC Act. If a firm wishes to claim, as Microsoft did, that its privacy protections are particularly strict or secure, it can help ensure its compliance with U.S. privacy requirements by modeling its privacy program on the order's requirements, which include the following:

- Notifying users of the need for and intended uses of collected personal data prior to data entry;
- Providing reasonable, industry standard privacy protection in the collection, processing, use and disclosure of personal user data;
- Employing secure facilities when data is vulnerable to unauthorized access;
- Disclosing personal data only where prior notification of potential disclosure has been made to data subjects;
- Ensuring that any stated privacy policy or claims related to privacy protections are realistic; and
- Instituting internal mechanisms for ensuring compliance with the stated privacy policy.

European Union Agreement

In discussions beginning in the latter half of 2002 and continuing into early 2003, Microsoft agreed to further changes to the .Net Password service to bring it into compliance with European Commission privacy regulations. This agreement, however, was the result of regulation that differed significantly – in both substance and procedure – from the FTC's approach in the United States. The fundamental regulation underlying the agreement is the EU's Data Protection Directive, which requires that entities handling personal data meet a host of broadly stated requirements, many of which are subject to exceptions and qualifications.[14] These requirements cover such areas as the handling of personally identifiable data,[15] as well as highly personal data like race, religion, or health information and the information to be given to a person when his or her data are collected.[16] In addition, the Directive gives data subjects broad rights to receive notice when their personal data is to be disclosed to others, to gain access to their data, and to object to disclosure or other processing of that data.[17] The Directive also imposes various notification, consent, and confidentiality requirements on entities handling data.[18] EU member states were required to make their national privacy regimes compliant with the Data Protection Directive by October 24, 1998.[19]

The Microsoft-EU agreement was the product of negotiations between Microsoft and the EU's Working Party on the Protection of Individuals with Regard to the Processing of Personal Data ("Working Party"). The Working Party was established in the Data Protection Directive and includes representatives of the EU and its member states.[20] It provides advice and recommendations concerning the enforcement and substance of the Directive. As part of its mission, the Working Party prepared a "Working Document on online authentication services," which it released on January 29, 2003.[21] Microsoft .NET Passport was used as a case study in the Working Document, which described and discussed at length the agreement concerning changes to .Net Passport. The Working Document commented favorably on these changes, but indicated that the Working Party would continue to study a few of them and generally reserved the right to monitor compliance with and the effect of the agreement.[22]

The Working Party identified a number of privacy and security concerns with Microsoft .NET Passport.[23] These included, among other things, (1) a lack of information given to users when the service collected personal data, processed it, or transferred it to a third-party, (2) the uncertainty of whether participating websites would comply with the Data Protection Directive, (3) the use of a persistent unique identifier, which third parties might use to correlate and assemble data about particular users, (4) the inability of users to exercise their rights under the Data Protection Directive, and (5) security risks associated with .NET Passport operations that might lead to unauthorized disclosure of personal data.[24]

To address these concerns, Microsoft agreed to significant changes in .Net Passport. Microsoft will recode the .NET Passport service so that the creation of a .NET Passport account will be separate and apart from the storing of information in the .NET Passport profile.[25] This will enable the user, on an opt-in basis, to choose whether to store information disclosed to a registering site in the .NET Passport profile. Additionally, users will be able to alter or delete information stored in their .NET Passport profiles on a field-by-field basis before communicating profile information to a participating website.[26] The Working Party also required Microsoft to post significant user notifications related to both privacy law and options for .NET Passport account creation.[27] Finally, Microsoft will provide users access to their unique user identifiers upon request.[28]

Coping with Multi-National Privacy Regulation

It might appear that in the United States a company could achieve compliance with the FTC's privacy requirements simply by accurately describing the company's relevant policies and procedures, while compliance in the EU would involve interpreting and applying a detailed set of prescriptive regulations. The FTC's treatment of .Net Passport, however, signals that the FTC may use its Section 5 jurisdiction not only to require that a company accurately describes its privacy practices, but to impose affirmative obligations on companies to ensure that they protect privacy online. Even with a more prescriptive approach to online privacy by the FTC, if the Microsoft agreements are any guide, we can expect the requirements imposed by the EU to be far more detailed and demanding in most respects. The only exception to this may be the FTC's insistence on the establishment of internal mechanisms to ensure continued compliance. The lesson of the Microsoft actions, then, is that a company can minimize its risks of non-compliance by adopting privacy policies that generally follow the lead of the Microsoft-EU agreement and add internal compliance mechanisms. The following approaches will help in that endeavor:

- Collect, process and disclose data only after the data subject has given unambiguous and informed consent;
- Collect data for legitimate purposes that are disclosed to the data subject, and use the data accordingly;
- Ensure that data collected is relevant and not excessive in relation to the purpose for which it is processed;
- Collect, use, or disclose sensitive data (such as data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sexual preference) only in very specific circumstances for clearly defensible purposes;
- Ensure that data is and remains accurate and current;
- Provide data subjects with reasonable means to rectify, delete or block dissemination of incorrect data about them;

SAFE HARBOR FOR
UNITED STATES COMPANIES

Although not directly involved in the .Net Passport matter, the "Safe Harbor" program for companies collecting or processing personal data in the EU is an important consideration. The EU's Data Protection Directive prohibits the transfer of personal data to countries that do not meet EU privacy protection standards. Because of the differences between privacy regulation in the United States and the EU, this prohibition could hamper the trans-Atlantic operations of U.S. companies. To address this, the United States Commerce Department and the EU jointly developed a program under which U.S. companies may certify that their privacy protections meet a set of prescribed standards. Compliance with this Safe Harbor is evidence of the adequacy of a company's privacy practices under EU requirements. To qualify for the Safe Harbor, companies must undertake to provide:

- Notice of the company's data related procedures,
- A choice to opt-out or opt-in to a transfer of data (depending on the nature of the data and its subsequent use),
- Assurance that any third party who receives data will adequately protect it,
- Access to data by the data subject,
- Reasonable measures to ensure that data is accurate and complete,
- Reasonable security to protect data, and
- A suitable recourse mechanism and remedies for breach of the company's privacy promises.

- Keep personal data only as longer as necessary;
- Adopt internal mechanisms to ensure that privacy practices are working as intended;
- Ensure that descriptions of privacy practices are not overblown or deceptive; and
- Adopt and comply with the Safe Harbor. (See sidebar)

SAFE HARBOR FOR UNITED STATES COMPANIES (con't)

A company may join the Safe Harbor by publicly declaring compliance with these principles and annually self-certifying continued compliance. The Safe Harbor will be enforced in the United States, primarily through what the agreeing parties call "private sector self regulation and enforcement." Private sector efforts will be backed up by government enforcement of federal and state statutes governing unfair and deceptive acts and practices, with the FTC having a primary role in that effort.

(Endnotes)

1 This article compares only FTC and EU enforcement. While these are unquestionably important regulatory schemes that are central to privacy law compliance, there are other provisions that companies must consider. In the United States, for example, the Health Information Portability and Accountability Act, 42 U.S.C. § 1320d-2; Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501 et seq.; Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, 6821-6827; Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521, 2701-2711, 3121-3127; Federal Wiretap Act, 18 U.S.C. § 1343; Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.; Telecommunications Act, 47 U.S.C. § 222; state and federal constitutions; and state laws also address privacy. In Europe, enactments such as E.U. Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector and the specific privacy requirements of member states must be taken into account.

2 See Microsoft Corp., ".NET Passport Overview," http://www.microsoft.com/netservices/passport/overview.asp.

3 Microsoft Corp., ".NET Passport Privacy Statement," http://www.passport.net/Consumer/PrivacyPolicy.asp.

4 Microsoft Corp., Complaint, File No. 012 3240 (2002) ¶¶ 3, 9 ("FTC Complaint"). (FTC Aug. 8, 2002).

5 Lydia Adetunji, "Microsoft to Tighten Security: 'Passport' Settlement with FTC Over Data Protection Charges, Financial Times, p. 7 (Aug. 9, 2002).

6 15 U.S.C. §44.

7 Microsoft Corp., Agreement Containing Consent Order, File No. 012 3240 (FTC Aug. 8, 2002) ("Consent Order"). As in the case of all FTC consent agreements, the agency released this order for public comment pursuant to 15 U.S.C. §16(b). The public comment period ended on September 9, 2002, but the FTC has not yet issued a final order.

8 FTC Complaint ¶ 7.

9 Id.

10 Id. ¶¶ 4-7.

11 Consent Order § I.

12 Id. § II.

13 Id. § III.

14 EC Directive 95/46/EC (adopted July 25, 1995) ("Directive"). Microsoft has also taken steps to be covered by another, important EU-related provision, the Safe Harbor that has been established so that protected information that is collected in the EU may be transferred to the United States. Its provisions are summarized in the sidebar. Safe Harbor compliance is evidence of compliance with the EU's privacy rules generally.

15 Id. Art. 6.

16 Id. Art. 8.

17 Id. Art. 10-12.

18 Id.

19 Republic of Lithuania State Data Protection Inspectorate, "Data Protection in the European Union" at 4, available at http://www.ada.lt/en/docs/Data_protection_in_the_EU.pdf.

20 Directive Art. 29.

21 Article 29 Data Protection Working Party, Working Document on online authentication services, 10054/03/EN, WP 68 (adopted Jan. 29, 2003) ("Working Document").

22 Working Document § 5.

23 Article 29 Data Protection Working Party, Working Document: First orientations of the Article 29 Working Party concerning online authentication services, 11203/02/EN/final, WP 60 (adopted July 2, 2002).

24 Id. at 3.

25 Working Document § 2.2.3.

26 Id. § 2.2.3.

27 Id.

28 Id. § 2.2.5.

Privacy
Regulation
Spring 2003

The Impact of New Canadian Privacy Rules on U.S. Businesses

Arian Siegel
Growling Lafleur Henderson, LLP
Toronto
arian.siegel@gowlings.com

Brenda Pritchard
Growling Lafleur Henderson, LLP
Toronto
brenda.pritchard@gowlings.com

Subject to any legislative changes, by January 1, 2004, almost all organizations doing business in Canada will be required to comply with federal privacy legislation, specifically the Personal Information Protection and Electronic Documents Act ("PIPEDA"). The implications of privacy legislation for U.S. businesses operating in Canada and collecting personal information about Canadians are significant both from a corporate marketing and corporate governance perspective. The legislation will impact how organizations can collect, use, and disclose an individual's personal information in the course of their activities. Depending on the nature of an organization's activities and the use made of personal information, compliance can be as simple as preparing privacy policies or can involve complex processes including comprehensive audits, training of staff, modifications to information storage systems, databases to enhance security, and revision of corporate contracts and forms.

This article will provide a brief overview of privacy requirements for the private sector in Canada and the potential impact for U.S. businesses operating in Canada.

While the steps taken by a U.S. corporation to adhere to privacy principles under the U.S. Safe Harbour Agreement are likely to be consistent with the steps required to ensure compliance with the requirements of Canadian privacy law, including PIPEDA, these steps may not satisfy all such requirements. As a result, U.S. corporations wishing to receive personal information from Canadian corporations (including Canadian subsidiaries of U.S. parent corporations), should determine whether Canadian privacy requirements are applicable to their circumstances.

Canadian Federal and Provincial Privacy Legislation

Canadian Federal Legislation - PIPEDA is being implemented in three stages. As of January 1, 2001, PIPEDA applied to the federally regulated private sector (i.e., airlines, banks, etc.). PIPEDA currently also applies to all organizations disclosing personal information for consideration across provincial boundaries or outside of Canada. As of January 1, 2002, PIPEDA applied to federal organizations that collect, use, or disclose personal health information. By January 1, 2004, all organizations (including associations, partnerships, persons, and trade unions) that collect, use, or disclose personal information in the course of commercial activity in Canada will have to comply with PIPEDA. However, PIPEDA provides that if a province enacts privacy legislation substantially similar to PIPEDA on or before that date, an exemption may be available under PIPEDA in connection with such activities conducted in that province. As a result, by January 1, 2004, almost all organizations engaging in commercial activities in Canada will be required to comply with some form of privacy legislation. To date, only the Province of Quebec has comprehensive private sector privacy legislation in place. British Columbia and Alberta will likely introduce similar legislation shortly.

Quebec Legislation - Quebec's comprehensive privacy legislation governing the private sector is called an Act Respecting the Protection of Personal Information in the Private Sector. Quebec's legislation contains requirements similar to those in PIPEDA with respect to obtaining consent for the use and disclosure of personal information. However, somewhat different obligations are imposed with respect to the collection process. Similarly, there are slight variations on access rules.

Draft Ontario Legislation - On February 4, 2002, the government of Ontario made public its draft privacy legislation, the Privacy of Personal Information Act, 2002 (the "PPIA"), to govern how the Ontario private, not-for-profit, and health care sectors collect, use, and disclose personal information. As currently drafted, the PPIA is intended to apply to all activities and organizations that are not federally regulated and not already covered by provincial public sector privacy legislation, even if the organization collected the information before the day on which the PPIA comes into force. After public consultations, the government indicated its intention to make substantial changes to the draft legislation. New legislation has yet to be tabled in the Legislature. Until such time that new legislation is introduced, it is likely that organizations that collect personal information in Ontario in the course of commercial activities will be required to comply with PIPEDA.

Sectoral-Specific Privacy Legislation - There are other laws at both the federal and provincial levels that contain provisions that provide sectoral-specific privacy protection to Canadians. For example, there are privacy requirements in legislation dealing with credit reporting, banking, insurance, securities, telemarketing, and employment standards. Additionally, vari-

ous consumer protection laws at federal and provincial levels offer limited protections and remedies against business practices that may constitute an infringement of privacy.

What is PIPEDA All About?

The federal government states that the purpose of PIPEDA is to establish, rules to govern the collection, use, and disclosure of personal information in a manner that balances the right of privacy of individuals with the need of organizations to collect, use, or disclose personal information for a reasonable purpose.

Personal information is defined as "information about an identifiable individual." It does not include the name, title, business address, or telephone number of an employee of an organization. It includes such information as race, ethnic origin, colour, age, marital status, religion, education, medical, criminal, employment or financial history, address and telephone number, numerical identifiers such as the Social Insurance Number, fingerprints, blood type, tissue or biological sample, and views or personal opinions that are linked to an individual.

PIPEDA is divided into six Parts. For purposes of this review, the most important part is Part I (Protection of Personal Information in the Private Sector). Incorporated into the legislation as a Schedule is the Canadian Standards Association Model Code for the Protection of Personal Information ("Model Code"). The Model Code ten principles that have been adopted by various industries and organizations in protecting personal information. Some of the principles create clear obligations and prohibitions, while others are set out as recommendations (using the word "should") and do not necessarily impose an obligation. The legal impact of these recommendations is uncertain.

The Model Code's 10 principles are outlined below.

1. *Accountability*: An organization is responsible for personal information under its control and shall designate an individual or individuals who is/are accountable for the organization's compliance with the following principles.

2. *Identifying Purposes*: The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

3. *Consent*: The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except when inappropriate.

Commentary: The most important principle set out in PIPEDA is the requirement for companies to obtain an individual's consent when they collect, use or disclose the individual's personal information. PIPEDA also requires that personal information be used or disclosed only for purposes for which it was collected. Except for limited circumstance, if an organization plans to use or disclose this information for purposes other than those initially disclosed, additional consent must be obtained. PIPEDA does not specify whether minors can give informed consent. The Canadian Marketing Association has implemented voluntary guidelines for collection of personal information from children and teenagers which should be followed.

4. *Limiting Collection*: The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5. *Limiting Use, Disclosure, and Retention*: Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Personal information shall be retained only as long as necessary for fulfilment of those purposes.

6. *Accuracy*: Personal information shall be accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. *Safeguards*: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. *Openness*: An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. *Individual Access*: Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. *Challenging Compliance*: An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

What are the Implications of Canadian Privacy Legislation for Your Organization?

Compliance with Canadian privacy requirements could involve the preparation of new, or the revision of existing, policies and procedures relating to the following:

- Privacy (as it relates to both customers and employees);
- Internet Terms of Use;
- Information storage and security (including structure and access rights of databases); and
- Audit (to assess compliance with new polices).

Organizations will then have to put internal and sometimes external systems in place that conform with the above policies.

All organizations will be required to designate an individual responsible for privacy compliance. PIPEDA requires organizations to provide indi-

viduals with information regarding the collection, use, and disclosure of their personal information and to obtain consent for collection, use, and disclosure of this information in most circumstances.

American businesses that have Canadian operations will need to comply with a number of requirements regarding the retention, accuracy, security, and destruction of records; the means by which consent is obtained for collection, use and disclosure of personal information; and the means by which rights of access to, and correction of, personal information are provided. Companies that regularly collect personal information either online, through the mail, or on the telephone for purposes of marketing, rewards programs, or consumer research should be especially vigilant about complying with the consent requirements of PIPEDA. While neither PIPEDA nor the Code provide specific direction on how consent should be obtained, in recent decisions stemming from individual complaints, the Federal Privacy Commissioner has taken a hard line in favour of express consent requirements, particularly when dealing with sensitive personal information.

What are the Risks if an Organization Does Not Comply?

PIPEDA establishes a redress mechanism that allows individuals to complain about any aspect of an organization's compliance with provisions relating to the protection of personal information. PIPEDA provides the federal Privacy Commissioner with general powers to receive and investigate complaints and to attempt dispute resolution. The Privacy Commissioner also has the right to initiate a complaint and must file with the organization a notice of the complaint.

The Privacy Commissioner has the power to summon and enforce the appearance of persons before the Commissioner to testify, receive any evidence, enter any premises (other then a dwelling-house), interview persons on the premises, and examine records on the premises. The Commissioner then prepares a report within one year after the day that the complaint is filed.

Following an audit, the Commissioner may make public any information relating to an organization's personal information management practices if the Commissioner considers it in the public interest to do so. Either (a) the Privacy Commissioner, or (b) the individual if not satisfied with the Commissioner's report, may apply to the Federal Court for~

- Damages (a monetary award); and/or
- An order compelling the organization to correct its practices; and/or
- An order compelling the organization to publish a notice of any action taken or proposed to correct its practices.

PIPEDA also creates offenses for the following activities:

- Obstructing an investigation or audit;
- Destroying personal information that is the subject of an access request; or
- Disciplining a whistleblower.

An organization that engages in these activities can be fined up to $10,000 for a summary conviction or $100,000 for an indictable offence.

Privacy
Regulation
Spring 2003

Privacy and Business in Australia

Philippa Hore[1]
Clayton Utz
Melbourne
phore@claytonutz.com

Information privacy is protected in Australia by a range of legislation at the Federal, State and Territory levels.[2] This article focuses on the recently adopted private sector privacy regime and considers some of its practical implications for businesses operating in Australia.

Background

Australia's new private sector privacy regime came into effect on 21 December 2001. The Commonwealth government implemented the privacy regime through amendments to the existing Federal Privacy Act (Cth) 1988 (the Privacy Act). The Office of the Federal Privacy Commissioner administers the regime.

The New Privacy Regime Marks a Significant Change to Australian Privacy Regulation

Previously, the Privacy Act applied mainly to the Commonwealth and Australian Capital Territory public sector, with the exception of some specific provisions relating to private sector credit providers, credit reporting agencies and tax file number recipients.[3] Privacy in Australia's private sector was subject to ad hoc privacy regulation through a mixed bag of statutory restrictions for certain business sectors[4] and voluntary codes of conduct in other industries.[5] Now all private sector businesses in Australia are required to comply with the Privacy Act unless they fall within one of the exemptions contained in the Act.

The New Regime's Key Features

The new regime is based on 10 National Privacy Principles (NPPs), that set out minimum standards that private sector organisations must comply with when they handle personal information. The NPPs also regulate the transfer of personal information outside Australia and restrict the adoption of government-agency identifiers by organisations as their own identifiers. The 10 NPPs are as follows:[6]

- Collection
- Use and Disclosure
- Data Quality
- Data Security
- Openness
- Access and Correction
- Identifiers
- Anonymity
- Transborder Data Flows
- Sensitive Information

Delayed Application of Some NPPs

The NPPs applying to collection, use and disclosure, data quality (insofar as it relates to the collection of personal information), anonymity, and sensitive information do not apply to information collected by an organisation before 21 December 2001.

The NPPs applying to data quality (insofar as it relates to personal information used or disclosed), data security, openness, unique identifiers, and transborder data flows applies to information collected before 21 December 2001.

NPP 6, which applies to access and correction, applies to information collected by an organisation before 21 December 2001 and used or disclosed after that date, except to the extent that compliance would place an unreasonable burden on the organisation, or cause it unreasonable expense.

Approved Privacy Codes

Organisations regulated by the Act are bound by the NPPs unless they have their own privacy code that the Privacy Commissioner has approved. The Privacy Commissioner may only approve a code if it provides at least the same standard of privacy protection as the NPPs. To date, most organisations have chosen to be directly regulated by the NPPs. Only two privacy codes have been approved by the Privacy Commissioner and three codes are awaiting approval.[7]

What sort of information is protected?

The Privacy Act regulates the manner in which private sector businesses handle "personal information." This is defined as "information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." "Sensitive information"

-- including "health information" (itself a defined term) and information about a person's race, ethnic origin, political opinions, membership of a political, professional or trade association, religious or philosophical beliefs, sexual preferences, and criminal history -- is subject to more restrictive obligations.

Which Entities are Covered?

The Privacy Act applies to the acts and practices of "organisations." This includes bodies corporate, unincorporated associations, partnerships, trusts and individuals such as sole traders or consultants when operating in a business capacity. However, a number of organisations are exempt from the Act in certain circumstances, including the following:

- Small business operators with an annual turnover in the preceding financial year of AUD$3M or less, provided that they meet certain criteria (for example, small businesses will not be exempt from the Act if they engage in acts or practices that pose a particular risk to the privacy of individuals, if they provide a health service, if they are related to a business that is not a small business or if they are contracted to provide a service to the Commonwealth);[8]
- Media organisations (but only in relation to acts and practices engaged in during the course of journalism and provided that the media organisation has publicly committed to observing published privacy standards);
- Registered political parties and political representatives (but the latter only in relation to acts and practices engaged in for purposes connected with participation in the political process, for example in relation to elections and referenda); and
- Commonwealth agencies, State and Territory authorities and prescribed instrumentalities (which in many cases are also subject to their own, specific privacy legislation).

Activities Excluded from the Operation of the Act

In addition, certain activities by covered organisations are excluded from the Act's requirements, including:

- The passing of personal information (but not sensitive information) between related bodies corporate (subject to certain restrictions);[9]
- Non-business personal, family, and household activities of individuals that involve the collection of personal information; and
- Some acts or practices by current or former employers of an individual in relation to "employee records" (this exemption is considered further below).

What if an NPP is Breached?

If an NPP (or an approved privacy code) is breached, the affected individual can complain to either the Federal Privacy Commissioner or to the relevant code adjudicator (if a complaints resolution process has been established under the approved privacy code). Following the completion of an investigation or complaint, the Privacy Commissioner or code adjudicator may make a determination that the respondent:

- Has interfered with privacy and should not repeat or continue conduct;
- Should perform any reasonable act to redress loss or damage; and
- Should pay the applicant an award of compensation for loss or damage (including injury to feelings or humiliation).

The complaint handling body may also determine that it is inappropriate to take further action. Determinations are reviewable by the Privacy Commissioner (in the case of a determination of a code adjudicator) or by the Administrative Appeals Tribunal (in the case of a determination by the Privacy Commissioner).

The Office of the Federal Privacy Commissioner reports that, from 21 December 2001 (when the private sector regime came into force) to February 2003, it received over 27,000 calls to its hotline, over 1,200 written complaints and over 2,000 written enquiries. The main issue that people were concerned about was the improper disclosure of personal information (this was the subject of 207 written complaints and over 4,000 enquiries).

The Privacy Act requires the Commissioner to endeavour to resolve complaints by conciliation, and the vast majority of complaints that he deals with are closed on the grounds that the respondent has adequately dealt with the privacy issue (for example, by revising procedures, rewriting product terms and conditions and privacy statements, taking disciplinary action against staff involved in an interference with privacy, and conducting staff privacy training). The Privacy Commissioner publishes de-identified case notes of finalised complaints that will be of interest to the general public (for example, because they involve a new interpretation of the Privacy Act or because they illustrate systemic issues).[10]

The Privacy Commissioner has only issued two formal determinations since the Privacy Act commenced in 1989 (both were issued in 1993 and relate to complaints about the public sector).

Acts and Practices Outside Australia - Extra-territorial Operation of the NPPs

The NPPs will apply to acts done or practices engaged in by an organisation outside Australia where the act or practice relates to personal information about an Australian citizen or permanent resident,[11] provided either:

- The organisation was created, formed or incorporated in Australia; or
- The organisation carries on business in Australia and the personal information was collected or held by it in Australia, either at or before the time of the relevant act or practice.

The extra-territorial provisions are designed to ensure that, as far as practicable and appropriate, the legislation applies in an environment where organisations operate across national boundaries and may move personal information overseas to process it. It is also designed to prevent organisations from avoiding the effect of the NPPs by simply moving personal information overseas.[12] The Privacy Commissioner is specifically empowered to take action overseas to investigate complaints in circumstances where the Act applies extra-territorially.

Practical Implications of Australia's New Private Sector Privacy Regime

Collecting Personal Information

One of the most significant practical impacts of the new legislation arises out of the requirement in NPP 1 regulating the collection of personal information) that organisations take reasonable steps to ensure that the individuals, about whom they are collecting personal information, are informed of certain details about that collection. This obligation applies whether the information is collected directly from the individual, or from a third party.[13]

Specifically, the collecting organisation must disclose the following:

- The identity of the collecting organisation and how to contact it;
- That the individual is able to gain access to the information;
- The purposes for which the information is collected;
- The organisations (or types of organisations) to which the collecting organisation usually discloses information of that kind;
- Any law that requires the information to be collected; and
- The consequences for the individual (if any) if the information is not provided.

To ensure compliance with the disclosure requirement, organisations have had to carefully consider how they collect personal information, and then incorporate the provision of these details into the collection process. Privacy collection statements are now included in a wide range of corporate communication material, including standard customer contracts, call centre scripts, employment application forms, prospectuses and conditions of entry for trade promotions. Where third parties collect personal information on behalf of an organisation, steps have had to be taken to contractually oblige the third party to provide individuals with these details on the organisation's behalf.

Transferring Personal Information Out of Australia

NPP 9 provides that an organisation may not transfer personal information outside Australia to a person (other than the organisation or the individual) unless one of six conditions applies. These include where the individual consents to the transfer, or where the organisation reasonably believes that the recipient is subject to a law, binding scheme, or contract containing requirements substantially similar to those imposed by the NPPs in relation to the protection of personal information. The principle is modelled on the restrictions placed on international transfers of data by the European Union Directive 95/46.[14]

There is some uncertainty as to whether an Australian body corporate transferring personal (non-sensitive) information overseas to a related body corporate would be required to comply with NPP 9. On one hand, the Privacy Commissioner has indicated that the Australian body corporate would need to comply with NPP 9 in these circumstances.[15] On the other hand, the wording of the provision that allows the sharing of non-sensitive, personal information between related bodies corporate suggests that such sharing would not interfere with privacy, even where the related body corporate is located offshore. This uncertainty may be addressed when the Privacy Commissioner conducts his review of the private sector provisions of the Privacy Act (which is scheduled to take place in December 2003).

In the meantime, if an organisation wants to transfer an individual's personal information outside of Australia (for example, because data processing occurs offshore), it can use the privacy collection statement (required by NPP 1 - discussed under the previous heading), to obtain consent from that individual.

The Scope of the Employee Records Exemption

The Privacy Act exempts employers from complying with the NPPs when collecting and handling personal information about current or former employees. However, this exemption applies only where the acts or practices of the current or former employer are directly related to a current or former employment relationship between the organisation and the indi-

vidual and directly related to an "employee record"[16] held by the organisation and relating to the individual.

This direct link to the employment relationship ensures that employers cannot seek the protection of the exemption if they use or disclose employment records for commercial purposes unrelated to the employment context.

The existence, as well as the scope of the employee records exemption, has generated a great deal of debate and some criticism. For example, because there is no employer/employee relationship between a contractor and an organisation, contractor personal information does not fall within the exemption. The practical effect of this distinction is that organisations have to collect and handle personal information about contractors (which is regulated by the Privacy Act) quite differently than personal information about employees (which generally is not). The differing application of the NPPs to employees and contractors in this context is viewed by some as arbitrary and unnecessary, particularly where contractors are performing very similar roles to employees (for example, temporary secretarial staff).

The exemption has also created practical difficulties for employers that outsource employment-related functions to third parties such as recruitment organisations, travel booking services and information technology service providers. Because these third parties do not have an employment relationship with the employees of the outsourcing organisation, the exemption does not apply. In practice, this can mean that employers must provide their employees with privacy collection statements on behalf of the organisations performing outsourced functions, which places an administrative burden on large employers (particularly where a number of activities are outsourced at different times).

The application of the employee records exemption to due diligence activities has also caused some concerns. Questions were initially raised as to whether making employee information available to a range of prospective purchasers of the employer organisation in a data room would be an act "directly related" to the employment relationship between the target company and its employees. This uncertainty has prompted the Privacy Commissioner to release an Information Sheet, which attempts to clarify how the NPPs will operate in a due diligence scenario,[17] both from the perspective of the target company and the prospective purchasers.

It is likely that the existence and scope of the employee records exemption will attract a great deal of scrutiny when the Privacy Commissioner undertakes his review of the Privacy Act in December 2003.

Health Information - Some Complications

Some Australian States and Territories have enacted specific health privacy legislation that regulates the handling of health information by the public and, in some cases, the private sectors.[18] Organisations that collect or handle health information in Australia need to consider whether this specific legislation affects them, as it may require them to observe a higher standard of privacy than is required by the NPPs.

For example, the Victorian Health Records Act 2001 requires public and private sector organisations to comply with 11 Health Privacy Principles when they collect and handle health information in that State. Because this Act does not contain an exemption for employee records, employers in Victoria must take steps to protect the privacy of employee health information despite that employee records are generally exempt from the NPPs. Although this apparent inconsistency may raise an issue as to the constitutional validity of the Victorian legislation, as yet, this issue has not been tested in the Courts. The Victorian Health Privacy Principles also impose specific obligations on health service providers in relation to the transfer or closure of their practices and making health information available to other health service providers. These matters are not dealt with specifically in the Federal Privacy Act.

The problems created by different privacy standards applying across jurisdictions and across public and private sector boundaries, has prompted the development of a draft National Health Privacy Code. Commonwealth, State, and Territory health authorities collaboratively developed the Code in order to establish a nationally consistent privacy standard for health information.[19] Once the Code is finalised, Australia's Federal, State, and Territory governments will need to consider whether to make legislative or administrative changes to ensure that the one uniform set of rules can apply to the privacy of health information across the public and private sectors throughout Australia.

Contracting with the Public Sector

Organisations contracting with Federal, State, or Territory public sector agencies in Australia should be aware that they may be required to comply with the public sector privacy principles applicable to the relevant agency. These organisations should keep in mind that they will continue to be subject to the NPPs to the extent that the NPPs are not inconsistent with the obligations imposed by the agreement with the public sector agency. Care needs to be taken to ensure that the implications of such dual regulation are considered and understood.

Additional Obligations for Credit Providers, Credit Reporting Agencies and Tax File Number Recipients

Specific privacy obligations apply to credit providers and credit reporting agencies. Part IIIA of the Privacy Act, which was already in force when the private sector amendments to the Act became operative, imposes these obligations. Private sector credit providers and credit reporting agencies must now comply with both the specific obligations in Part IIIA and the NPPs. The Privacy Act also contains provisions dealing with the collection and handling of tax file numbers (which again pre-dated the NPPs). Organisations must observe these if collecting tax file numbers in Australia.

Conclusion

The introduction of the new private sector privacy legislation in Australia has compelled businesses operating within (and, in some cases, outside) Australia to review and adapt their information collection and handling practices. For organisations that collect and handle a great deal of personal information, this has been a significant task. Some practical difficulties have arisen since the commencement of the new regime, particularly in relation to the scope of some of the exemptions. These issues are likely to be addressed in the Privacy Commissioner's review of the Act, which is scheduled to take place at the end of this year.

(Endnotes)

1 Philippa's profile is available at http://www.claytonutz.com/people/controller.asp?pid=322.

2 Australian legislation is typically couched in terms of "information" and "privacy" rather than "data protection."

3 These specific obligations still apply in addition to the new private sector privacy requirements and are considered later in this article.

4 For example, Part 13 of the Telecommunications Act (Cth) 1997.

5 Examples include the Codes of Practice of the Insurance Council of Australia, the Australian Direct Marketing Association and the Australian Bankers' Association.

6 The full text of the NPPs is available on the website of the Office of the Federal Privacy Commissioner, at www.privacy.gov.au/publications/npps01.html.

7 Codes have been approved for the insurance industry and for the Queensland Clubs Industry. Codes under consideration are for the market and social research industry, the Australian Casino Association and the Internet Industry Association.

8 Although there is a mechanism by which small businesses can "opt in" to complying with the Act if they choose to.

9 For example, the related body corporate that receives the information must only use that information consistently with the primary purpose for which the information was originally collected.

10 The case notes are available at http://www.privacy.gov.au/act/casenotes/index.html.

11 The limitation on the extra-territorial operation of the NPPs to personal information about Australian citizens and legal residents has been the subject of criticism by the European Commission and is one of a number of reasons why Australia's private sector privacy regime has been found to fall short of the adequacy test for European Union data protection standards. See the report of the Article 29 Data Protection Working Party of the European Commission (Opinion 3.2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000, adopted on 26 Jan. 2001, available at http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp40en.htm).

12 Explanatory Memorandum for the Privacy Amendment (Private Sector) Bill 2000, page 12.

13 NPP 1.3 and NPP 1.5.

14 The European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data.

15 Guidelines to the National Privacy Principles, Office of the Federal Privacy Commissioner, Sept. 2001, page 43.

16 "Employee record" means a record of personal information relating to the employment of the employee. Examples provided in the Privacy Act include health information about an employee and personal information relating to the employee's engagement, training, performance, disciplining, resignation, termination, terms and conditions of employment, taxation, banking or superannuation affairs, sick leave, and other leave.

17 This Information Sheet is available at http://www.privacy.gov.au/publications/is16_02.doc. It also considers the collection and disclosure of personal information about customers and trading partners in the due diligence scenario.

18 For example, the Health Records Act (Victoria) 2001 (public and private sector application; the Health Records (Privacy and Access) Act (Australian Capital Territory) 1997 (public and private sector application); the Privacy and Personal Information Protection Act (New South Wales) 1998 (public sector application) and the Health Records and Information Privacy Act (New South Wales) 2002 (public and private sector application). The Northern Territory is developing similar legislation, which is intended to have public and private sector application.

19 The Consultation Paper was released in December 2002 and can be accessed at http://www.health.gov.au/pubs/nhpcode.htm.

Privacy
Regulation
Spring 2003

Privacy and Video Surveillance: A European Vision

Lanise Hayes[1]
Studio Legale Imperiali
Naples
LaniseHayes@hotmail.com

Olimpia Policella[2]
Studio Legale Imperiali
Naples
Olimpiaoli@hotmail.com

Driven by governmental and commercial needs, video surveillance is steadily advancing into all aspects of our daily lives. But with its advancement, public concern is growing. Lawmakers are reacting to the tension by trying to balance the need of public and private enterprises to carry out surveillance for legitimate reasons while ensuring the privacy rights of citizens.

The European Response to Video Surveillance

Europe has various legal instruments that safeguard privacy with respect to video surveillance. Directive 95/46 sets out basic principles for the protection of personal information and is best known. These principles, however, were first introduced in the earlier Strasbourg Convention 108 of 1981, and have since been expanded by the adoption of diverse Recommendations and Working Party documents. In October 2002, the specific principles for correct video surveillance activities were established by the Council of Europe.

The Basic Data Protection Principles

Generally speaking, personal information collected through the use of video surveillance devices falls within the ambit of the Strasbourg Convention.[3] The Strasbourg Convention protects an individual's privacy with respect to the automated processing of personal data and recognizes privacy as a right and fundamental freedom.

Under the Convention, lawful processing means that the quality of the personal information and the security of this information are ensured. To ensure these goals, the information must be collected and processed fairly and must only be used for the purposes that were specified at the time of collection. The data collection should be adequate, relevant, and not excessive, as well as accurate and up-to-date. Personal information

must also be stored in such a way as to prohibit identification of the data subject. Data subjects also have a right of access to the personal data. Data subjects may request correction or cancellation of the data or seek remedy when processing operations have been carried out in violation of the individual's privacy rights. Right to access is directly connected to the principle of transparency. Transparency entails providing clear information about surveillance activities and the location of the cameras. In some European countries, the nature of the place – public or private – in which surveillance is carried out may be determinative.[4] Generally speaking, public spaces are those where access is allowed to everyone, such as parks, streets, stores, and banks. Private spaces are offices, homes, and work areas where access is limited to authorized persons only.

Consumer Data Protection Principles for Video Surveillance and Application of the Basic Data Protection Principles to Surveillance Activities

Many publicly accessible spaces are equipped with video surveillance devices for security and commercial purposes. Banks, gas stations, and some stores have relied on surveillance cameras as a security measure against theft and robbery. More and more, however, merchants are implementing surveillance systems for commercial reasons. Video registration of consumer shopping habits, for example, has allowed merchants to determine peak-hour shopping times and create more stimulating "shopping routes" that might push consumers into spending more. Video surveillance has also found its way into other consumer areas.

Video surveillance must comply with the data protection principles. In addition, video surveillance must be allowed by law and must serve a specific and legitimate purpose.[5] Data Controllers must also ensure that less intrusive systems cannot be implemented.

The data quality and access rights principles have particular significance in video surveillance. Because personal information must be relevant and not excessive, a number of restrictions must be placed on video registration activities. More specifically, the visual field should be limited in relation to the purposes or the areas that actually require surveillance. Where possible, close-up shots should be avoided to eliminate the risk of taking in details and physical traits that have no bearing on the purposes. Because individuals must be guaranteed a reasonable expectation of privacy, even in public places, data Controllers should register only those images that are indispensable for the purposes that the data Controller has declared to the relevant Data Protection Authority.

Data Controllers have often invoked Art. 9 of the Strasbourg Convention to refuse access rights to individuals because it would reveal data pertaining to another person. In light of new technological advances,

France proposed adding a twelfth principle[6] regarding access to the Guiding Principles that were adopted provisionally in October 2002. This principle stipulates that adequate technical and organizational means should be used so as to allow individuals to access personal data without obtaining information concerning others. If adopted, data Controllers would be required to carry out surveillance operations in such a way as to ensure the right to access.

Some other legal instruments offer additional safeguards to privacy in different sectors where surveillance or monitoring activities are concerned. Recommendation No. R(87)15 regulates the use of personal information in the police sector. Under this Recommendation, eight principles are set out confirming those found in the Strasbourg Convention 108, especially regarding automated processing, and confine data collection by law enforcement agencies to that which is necessary for the prevention of a "real danger" or the suppression of a "specific criminal offence." Information sharing, storage periods, publicity of data collection activities, access and rectification rights, as well as the role of the Data Protection Authority are further dealt with in this instrument.

Recommendation No. R(95)4 protects data with respect to automated processing in the telecommunications sector. Service providers and network operators are required, according to this Recommendation, to respect users' right to secrecy of correspondence and freedom of communication. In particular, subscriber lists containing personal information may only be disclosed to third parties if one of four conditions are satisfied: the subscriber has expressly consented to the data-sharing in writing; the subscriber has been informed of the intended disclosure and has not objected; disclosure has been authorized by the Data Protection Authority; or, disclosure is provided for under domestic law. Video communications are also regulated under R(95)4 requiring the use of anonymous systems for accessing networks. As well, subscribers and those called must not be subject to positioning or locating techniques when the call is made. Recommendation No. (89)2 concerns personal data used in the employment sector. This Recommendation applies not only to data undergoing automated processing, but to all other employee data used or kept by employers, from recruitment through to termination of employment. What's more, involvement by trade unions in determining the suitability or as a means of informing employees of the intended use of automated processing methods is expressly provided for under this document.

In situations where more than just images are collected, like biometric data, or where the data is subject to automated operations that allow for profiling, facial recognition, indexing, decision-making or that use intervention systems or are aimed at provoking specific behaviour,[7] the prudent data Controller should also consider additional protections for individuals and more comprehensive controls.

Video Surveillance in the Workplace

Today, the line between our private and professional lives has almost disappeared. Most of our waking hours are spent in the office or shopping, and the relationships we develop in those places are not always limited to our professional life. In response, Recommendation No. R(89)2[8] attempts to protect workers' privacy and dignity in their social and professional relations. Correct business practices would have the employer inform employees of the use of surveillance devices, or of any intention to introduce devices that permit movements or productivity to be monitored. Where desirable, trade union representatives should also be consulted.[9]

The eleventh Principle in the Guiding Principles[10] requires employers to refrain from using video surveillance as a means of controlling performance quality and quantity. In addition to the necessity of informing employees as to surveillance activities, trade union agreement is also a condition if the surveillance is carried out for organizational or management purposes or for work safety reasons. Furthermore, employees may use the recorded images in case of legal actions or disputes.

Most countries consider the workplace a private space, providing different guidelines for monitoring in public or publicly accessible places. France and Italy, for example, have legislated the use of video surveillance devices in the workplace. These dispositions are part of particular labour laws that relate to all aspects of the employee-employer relationship, however, and not specifically a unique privacy regulation. Other dispositions prohibit distance controlling of work-related activities and may require that trade union representatives are involved before installing video cameras. The United Kingdom is still struggling to pass its Employment Code of Practice, which has a specific section dealing with monitoring activities and, specifically, workplace video surveillance. Section 6.4 of the Draft Code recognizes the pertinence of the provisions of the CCTV Code of Practice.[11] The Draft Code underlines the intrusive nature of monitoring activities and the need to respect workers' privacy as much as possible. Generally, the privacy impact of surveillance should be evaluated beforehand by both the employer and trade unions. Covert monitoring, which is contrary to the principle of transparency or openness, may only be justified in light of specific criminal activities. Finally, employers must respect employees' reasonable expectation of privacy in certain areas, avoid installing cameras or other devices in these places[12] and ensure that the public is made aware of the monitoring when entering spaces under surveillance.

Video Surveillance

One of the principal concerns that the public has is that video surveillance activities will influence our behaviour, possibly limiting our freedom of movement and informational self-determination. A greater risk is that this data may be collected on the basis of pre-determined criteria, such as ethnic origin, belief, political opinions or sex life, leading to discriminatory practices. On the other hand, consumers may benefit from increased knowledge about their demand. The EU recognizes both the concern and need, and is trying to balance the two. And so is the public.

(Endnotes)

1 Lanise Hayes is a member of the Quebec Bar and collaborates with Studio Legale Imperiali, an Italian law firm specialising in privacy and Information Technology, insurance, banking and credit management. She prepares press releases and articles on privacy and IT matters for the firm's service site and for publication on external legal web sites. This article reflects the personal views of the authors.

2 Eulalia Olimpia Policella, a member of the Italian Bar in Isernia, is an Italian attorney and collaborator, in charge of the privacy - IT sector, with Studio Legale Imperiali. She writes numerous articles which are published in newspapers and specialised law reviews on Privacy, IP, IT, telecommunications and data security issues for legal web sites.

3 The Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data, ETS no.: 108, 1981. An exception to this general rule might be where the surveillance merely captures without actually recording the images or in digital recording without further purposes or means for retrieval of the images.

4 In Italy, for example, the Presidential decree no. 250/1999 has set out the conditions for lawful video surveillance for the purpose of regulating access of vehicles to restricted areas in city centres, requiring cities to obtain authorisation from the Ministry of Public Works and the Department of traffic and road safety. In Belgium, the Data Protection Authority emitted Opinion 3/2000 of 10 January 2000, regarding the use of video surveillance systems in the entrance halls of apartment buildings. Thus, specific legislation may set out additional obligations on the Data Controller or may authorize surveillance activities without performance of the usual formalities, like notification; though, generally, data subjects' rights are maintained regardless of the nature of the place under surveillance.

5 Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance, prepared by Mr. Giovanni Buttarelli (Secretary General of the Data Protection Authority of Italy).

6 This proposal was submitted to the European Committee on Legal Co-operation in April 2003.

7 As G. Buttarelli pointed out in his report, which can be found on the Council of Europe web site, that surveillance activities implemented for prevention purposes might "tend to replace or supplement control with the incitement to self-control". Hence, individuals' normal impulses would be repressed by the knowledge that their actions are being monitored. An example might be in the case of surveillance of areas in which youth are known to gather. Self-consciousness brought on by the awareness of video cameras will surely lead them to behave differently. Big Brother is probably another example of people changing their regular behavioural patterns because of continuous monitoring.

8 Recommendation No. R(89)2 of the Committee of Ministers to Member States on the Protection of Personal Data Used for Employment Purposes, 1989.

9 This specific requirement can be found in different national laws regarding data protection in the employment sector. France, Belgium and Italy, to name only a few, have provided for the involvement of trade union representatives before introducing or modifying automated data processing systems including monitoring. Likewise, national legislation or trade agreements have also stipulated the purposes for which video surveillance may be authorized.

10 Id.

11 The CCTV Code of Practice applies to surveillance activities in publicly-accessible spaces in compliance with the Data Protection Act 1998.

12 The examples given by the British Data Protection Commissioner are cloakrooms, vehicles and individual offices where one may expect a certain degree of autonomy of action.

Consumer Protection Committee

Robert M. Langer
Chair
Wiggin & Dana LLP
Hartford, CT
rlanger@wiggin.com

Julie Brill
Vice-Chair
Office of the Attorney General
of the State of Vermont
Montpelier, VT
jbrill@atg.state.vt.us

Lesley A. Fair
Vice-Chair
Federal Trade Commission
Washington, DC
lfair@ftc.gov

August Horvath
Vice-Chair
Weil, Gotshal & Manges LLP
New York, NY
august.horvath@weil.com

John Villafranco
Vice-Chair
Collier Shannon Scott PLLC
Washington, DC
jvillafranco@colliershannon.com

Computer and Internet Committee

David H. Evans
Co-Chair
Arent Fox Kintner Plotkin & Kahn, PLLC
Washington, DC
evans.david@arentfox.com

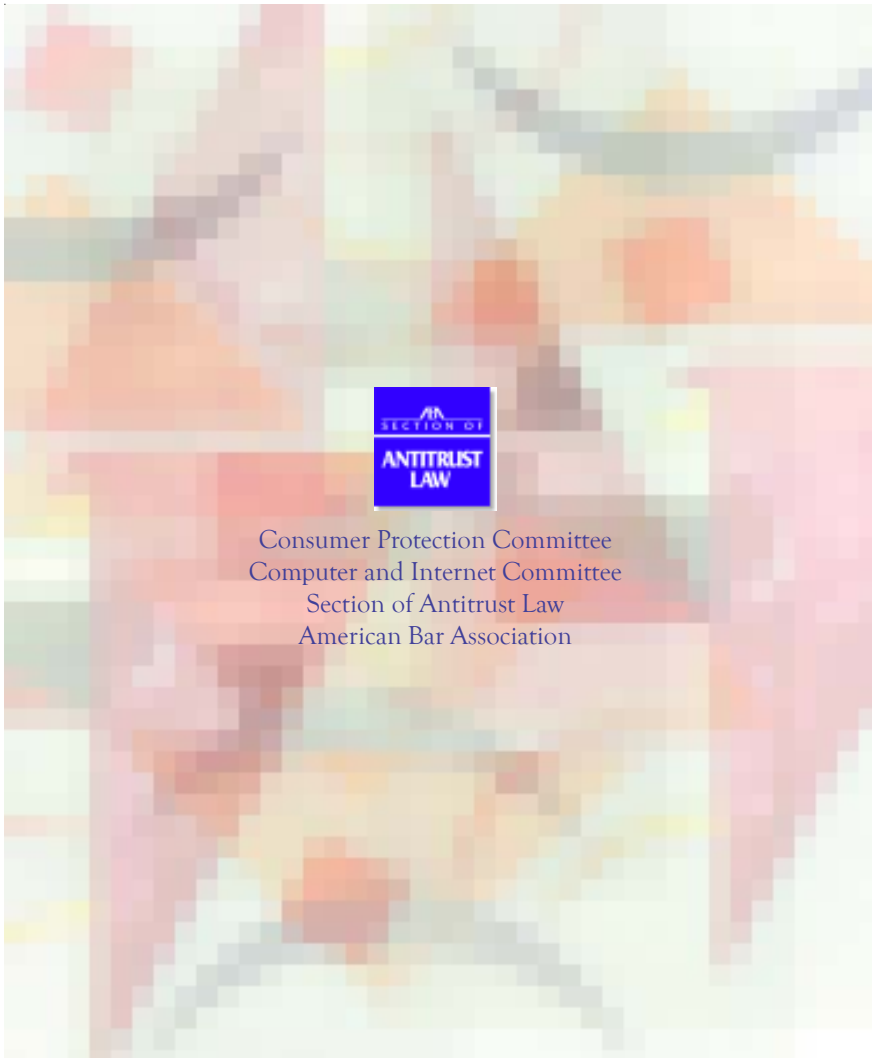
Leslie C. Overton
Co-Chair
Gray, Cary, Ware & Freidenrich LLP
Sacramento, CA
loverton@graycary.com

Mark C. Del Bianco
Vice-Chair
Skadden, Arps, Slate, Meagher & Flom LLP
Washington, DC
mdelbian@skadden.com

Patrick Kelleher
Vice-Chair
Gardner Carton & Douglas
Chicago, IL
pkelleher@gcd.com

Gail Levine
Vice-Chair
Federal Trade Commission
Washington, DC
glevine@ftc.gov

Paul Saint-Antoine
Vice-Chair
Drinker, Biddle & Reath LLP
Philadelphia, PA
paul.saint-antoine@dbr.com



Consumer Protection Committee
Computer and Internet Committee
Section of Antitrust Law
American Bar Association