The Internationalization of Privacy

How Europe is Driving the Global Privacy Agenda

Prepared for Canadian Bar Association
Annual Meeting, Winnipeg, August 16, 2004

Simon Chester, KNOW*law* Group,
McMillan Binch, Toronto

TABLE OF CONTENTS

Introduction

The privacy agenda around the world is being driven by Europe. All countries in the European Union have legislated privacy protections. And European models for privacy protection are being exported around the world. Indeed Canada's own privacy laws can be seen as being clearly shaped by European developments[1].

Yet, those European models have come under criticism as being too bureaucratic, as following pre-Internet paradigms of jurisdiction and territoriality and in elevating one moral interest above competing claims. From the perspective of the United States, with its preferences for market solutions and light-handed regulation, the European law on data protection is seen as academic, impractical and ultimately disruptive of consumer interests. Canada, as usual, can see both sides of the argument. Yet this issue is far from theoretical.

These new laws reflect the rapid growth of technology and electronic commerce in Canada and throughout the world. They also mirror similar legislation introduced in other countries. In today's world, global capital markets and the Internet combine to remind policy-makers and legislators that they cannot look to purely domestic models and that effective action requires regulatory co-ordination. To make the most of the new economy, governments are working together, to find ways of bolstering the use of new technologically-enhanced, communication systems while also assuring consumers that their privacy is protected.

Internationally, Canada is often seen as occupying a policy middle ground between Europe and the United States. Canadian attitudes and government responses to the privacy issue are generally not exceptional. In this case, however, it is Europe that has taken the initiative that we have followed while the U.S. still lags behind. Thus, to understand both Canada's new *Personal Information Protection and Electronic Documents Act*,[2] and secondly how multinational businesses should respond, one must look first to international and particularly, European initiatives, and then to America's contrasting actions.

The Tale of Three European Women

To illustrate how privacy is treated differently in Europe, one need look no further than three recent high level court decisions. They each involve the court considering the dimensions of privacy rights, and the extent to which those rights can be compromised or abridged. Each in its way presents an alternative vision of privacy to North American lawyers accustomed to according priority to freedom of speech, and to the application of a light regulatory hand.

---

[1] Portions of this paper were published earlier in Simon Chester and Barbara McIsaac, *The New Global Privacy Landscape*, Toronto 2000

[2] S.C. 2000, c. 5.

The Case of the Swedish Parishioners

On November 2,003, the European Court of Justice handed down its first case interpreting the substantive reach of the European Data Privacy Directive[3]. It did so in a case whose facts are as sympathetic as the action of the regulators is surprising.

Bodil Lindqvist was a volunteer in a Swedish church. To prepare parishioners for a first communion, she set up a web page with information about herself and eighteen other volunteers in the parish. She included their first names and sometimes their full names, going on to describe the work each did in mildly humorous terms. In some cases, she provided telephone numbers and contact information. She also mentioned that one of her team members had injured her foot and was working part-time on medical grounds. Lindqvist had not asked her colleagues for permission nor had she notified the Swedish Data Protection Authority that she was intending to put up the website. One of her colleagues asked her to remove the web site, and she took it off the server. However, the Swedish Data Protection Authorities commenced criminal proceedings against her, resulting in a fine of approximately Can.$600 (Swedish Krona 4000), for processing personal data without notifying the Authority in writing, for transferring data outside Sweden without authorization and for processing sensitive personal information (the line about the foot and the part-time work). Lindqvist appealed to the Gota Court of Appeal. She argued that:

- hosting information on an internet website does not amount to processing personal data;
- hosting information on a website does not amount to transferring data outside her home country to a third country;
- the Data Protection Director was not intended to apply to non-profit activities;
- the sanctions she was facing for violating the data protection law violated her freedom of expression;
- the sanctions were disproportionate to the harm done.

The Gota Court of Appeal referred several questions to the European Court asking it to clarify the correct interpretation of the Data Protection Director.

When the Court handed down its decision late last year, it gave an interpretation to the Director that surprised even privacy advocates. It rejected all but one of Lindqvist's arguments. Posting individuals' names and phone numbers did indeed constitute

---

[3] See http://curia.eu.int/jurisp/cgi-bin/form.pl?lang=en&Submit=Submit&docrequire=alldocs&numaff=&datefs=&datefe=&nomusuel=&domaine=&mots=Bodil+Lindqvist&resmax=100 also found at http://www.cr-international.com/docs/2003_ecj_bodil_lindqvist_6_11_2003.pdf. Bodil Lindqvist's home website is http://biphome.spray.se/mors/

the processing of personal data. The directive did apply to Lindqvist's hostings even though she was engaged in non-profit activities. Once personal data is posted on the internet, it is available to an infinite number of people, and accordingly there can be no resort to an exception for personal or household activities. Lindqvist did however win on the jurisdictional point. There was no evidence that anyone outside of Sweden had accessed the information on the website. Merely posting personal data on the internet does not subject persons to the legal regime governing the trans-border transfer of personal data unless they actually send the personal information to internet users who did not intentionally seek access to the web pages, or used a web server located outside Europe.

Ms. Lindqvist may be an unlikely figure to have established such ground-setting jurisprudence, but her case has quickly led to other activities by privacy regulators, building upon the Court's interpretation. In Norway, privacy authorities recently announced that they would pursue website operators displaying photographs of individuals taken without their prior consent. For a business audience, it may also be relevant that General Motors had to spend 6 months before it could post contact information for its staff on the GM intranet, satisfying privacy regulator's objections.[4]

The Case of the Cocaine-Addicted Supermodel

On May 6, the House of Lords[5], by a 3-2 majority decided in favour of Super-Model Naomi Campbell, in her action against the Daily Mirror.[6] Super-Model Naomi Campbell had a cocaine problem. She was getting treated at Narcotics Anonymous in King's Road in Chelsea. As she left the Narcotics Anonymous meeting one night, clad in a singularly unfashionable woolly hat she was surprised by a Daily Mirror photographer who took a series of pictures. Shortly afterwards, the Daily Mirror ran an expose, talking about her battle against drug addiction. The story was not unsympathetic, but did show the photographs. Naomi Campbell sued the Daily Mirror for breach of confidence. At trial, Morland J awarded her £3,500, despite the fact that he found that she lied to the media about her addiction. The paper appealed successfully to the Court of Appeal, which held that the paper was entitled to expose the model's lie that she did not take drugs, and that disclosing that she was attending narcotics anonymous did not constitute a breach of confidence.

The model then appealed to the House of Lords, which split. The Court had earlier decided against finding a free standing tort of privacy, but it nevertheless held that the Human Rights Act did provide her with a remedy. Under Article 8 of the European Convention on Human Rights, Campbell had a right to respect for her private life. The question was whether the information about her attending narcotics anonymous would be

---

[4] See David Scheer, Europe's New High-Tech Role: Playing Privacy Cop to the World, October 10, 2003, Wall Street Journal.

[5] *Campbell v. MGN Limited*, House Of Lords, Session 2003-04, [2004] UKHL 22, on appeal from: [2002] EWCA Civ 1373 at http://www.publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm

[6] See generally Simon Chester, Zapping the Paparazzi; is the Tort of Privacy Alive and Well? (2003) 27 Advocates' Quarterly 357.

regarded as private, rather than public. The test was whether disclosure of the information would give substantial offence to a reasonable person of ordinary sensibility placed in a similar position. Once the information is found to be private, the Court has to consider the balance between Article 8 Privacy Considerations and Article 10 Freedom of Expression Considerations. Two of the judges felt that the Mirror's freedom of speech should trump. The majority was however troubled by the fact that the information was medical information, whose disclosure had the potential to cause harm, and also that the photograph had been published. The mere facts of the story were true – what gave offence was the photograph. The Lords held that the fact that someone could be seen by anybody on a public street does not mean that pictures can be taken of them and circulated without consideration for the private life of the subject.

Campbell's case cost £1 million, an extraordinary amount for a photograph that was essentially accurate. The Daily Mirror described the Court's decision as "a very good day lying drug-abusing prima donnas who want to have their cake with the media, and the right to then shamelessly guzzle it with their Cristal champagne".

The paper was considering an appeal, when the third of the trilogy of cases was released, this time involving a minor European Royal.

The Case of Princess Caroline

Princess Caroline of Monaco is the daughter of Prince Rainier III and Grace Kelly. For the last ten years, she has been engaged in litigation against German tabloid publications, which published celebrity pictures. Indeed, her husband, Prince Ernst August von Hannover was once convicted of attacking a photographer. Princess Caroline sued to persuade Germany's Federal Constitutional Court to stop the pictures appearing in three magazines Bunte, Neue Post and Freizeit Revue. The Constitutional Court on December 15, 1999 upheld an injunction prohibiting the publication of photographs of Princess Caroline with her children on the grounds that children had a greater right to expect privacy. But they held that Princess Caroline was undeniably a figure of contemporary society and thus of general interest, and thus had to expect publication of photographs taken in a public place even if they showed her in scenes from her daily life (shopping, skiing or on a beach) rather than engaged in official duties.

Appealing that decision to the European Court of Human Rights[7], Princess Caroline won a significant victory: "the Court considers that the public does not have a legitimate interest in knowing where [Princess Caroline] is and how she behaves generally in her private life – even if she appears in places that cannot always be described as secluded and despite the fact that she is well known to the public".

The fundamental principle upon which future European privacy litigation would turn is "the fundamental importance of protecting private life from the point of view

[7] von Hannover v. Germany can be found at http://www.liberty-human-rights.org.uk/privacy/media-caroline-judgment.PDF

of the development of every human being's personality. That protection…extends beyond the private family circle and also includes a social dimension. The Court considers that anyone, even if they are known to the general public, must be able to enjoy "legitimate expectation "of protection of and respect for their private life.

These three decisions contrast markedly with precedents in North America. They reveal that Europeans attach a much higher priority to individual privacy. While the Court in both the Princess Caroline and Naomi Campbell cases notes the need to respect freedom of the press, in practice, the media can take scant comfort from these cases. Indeed, to an external observer it looks as if Europe's privacy laws really have teeth.

European And International Initiatives

The OECD Guidelines

The Organization for Economic Co-operation and Development ("OECD") was the first international organization to make an attempt at the harmonization of initiatives relative to the protection of personal information. In the early years of privacy protection, in a less technologically advanced time, the OECD drove the pace of the policy agenda. In 1980, the Member States of the OECD issued its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[8], known as the OECD Guidelines. These Guidelines are voluntary and do not carry the force of law. Consequently, they have been applied differently by different Member States. Still, they have provided the basis for most privacy protection schemes, adopted either legislatively or voluntarily, by Member States as well as those adopted by other states.

The OECD Guidelines enunciate the rights and obligations of individuals with respect to the processing of personal information and the rights and obligations of organizations that engage in the processing of personal information. These principles are applicable to both the public and private sectors, and to both the domestic use of personal information and the use of such information at the international level in transactions which span traditional state borders.

The OECD Guidelines comprise a number of principles intended to provide the basis for the adoption by member countries of specific legislation for the protection of personal information at both the national and international levels. The basic principles of national application are:

Collection Limitation Principle

> There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

---

[8] Online: <http://www.oecd.org/dsti/sti/it/secur/index.htm>.

Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle except: (a) with the consent of the data subject; or (b) by the authority of law.

Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

An Individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

Accountability Principle

> A data controller should be accountable for complying with measures which give effect to the principles stated above.

How These Principles Apply Outside Europe

The basic principles of international application are:

- Member countries should take into consideration the implications for other Member countries of domestic processing and re-exporting of personal data.

- Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

- A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

- Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

These principles are to be implemented by Member countries through the establishment of legal, administrative or other procedures or institutions for the protection of privacy and personal data. Implementation may be through the adoption of appropriate domestic legislation; encouraging and supporting self-regulation such as codes of conduct; providing reasonable means for individuals to exercise their rights in respect of personal information; providing for adequate sanctions and remedies for breaches of the means used to implement the principles; and ensuring that there is no unfair discrimination against individuals about whom personal information is held.

Member countries are also requested by the OECD Guidelines to make known to other countries, on request, the details of the measures they have implemented to observe the principles of the Guidelines. In addition, Member countries are directed to ensure that procedures for the transborder flow of personal information and for the protection of privacy are simple and compatible with those of other Member countries. The OECD Guidelines encourage the free transborder flow of personal information subject to legitimate restrictions for categories of data considered to be "sensitive" and for which the other county or countries do not provide equivalent protection.

The OECD has continued to play a role in the development of international privacy policies. In 1985, the governments of the OECD Member countries adopted a declaration stressing their intention to seek transparency in the regulation of, and in policies affecting, the transborder flow of personal information, and to co-operate in the development of common approaches and harmonized solutions for dealing with issues relating to the international exchange of personal information.[9] In 1997, the Information, Computer and Communications Policy Division ("ICCP") submitted a document to the OECD Group of Experts on Information Security and Privacy. That document was subsequently issued in 1998 as a paper entitled, *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet*.[10] The report looked at concerns relating to privacy and the burgeoning development of the Internet and the special challenges to the protection of privacy posed by the electronic age and e-commerce in particular. It reaffirmed that the OECD Guidelines were generic guidelines for the protection of privacy and the handling of personal data and suggested the following actions:

- to reaffirm that the Privacy Guidelines are applicable with regard to any technology used for collecting and processing data;

- for those businesses who choose to expand their activities to information and communication networks, to encourage them to adopt policies and technical solutions which will guarantee the protection of the privacy of individuals on these networks, and particularly on the Internet;

- to foster public education on issues related to protection of privacy and the use of technology.[11]

The report suggested that the OECD would be a good place to undertake the necessary study of these issues in light of its history in developing the Privacy Guidelines and its established competence in dealing with issues relating to the development of the global information society.[12] In keeping with this mandate, the OECD recently released a privacy statement generator on the development and posting of privacy statements on web sites.

---

[9] *Implementing the OECD* "Privacy Guidelines" *in the Electronic Environment: Focus on the Internet Copyright OECD*, 1998, Head of Publications Services, OECD, 2 rue André-Pascal, 75775 Paris, Cedex 16, FRANCE, online: <http://www.oecd.org/dsti/sti/it/secur/prod/reg97-6e.htm>at p. 9.

[10] Copyright OECD, 1998, Head of Publications Service, OECD, 2 rue André-Pascal, 75775 Paris, Cedex 16, FRANCE, online: <http://www.oecd.org/dsti/sti/it/secur/prod/reg97-63.htm>.

[11] *Ibid*. at 4

[12] The reader may be interested in consulting the 1992 OECD Guidelines for the Security of Information Systems, online: <http://www.oecd.org/dsti/sti/it/secur/index.htm>, and a Review of the Guidelines published in 1998 which is available from the Head of Publication Services, OECD, 2 rue Andre-Pascal, 75775 Paris Cedex 16, FRANCE.

United Nations Initiatives

The General Assembly of the United Nations adopted guidelines dealing with computerized files containing personal information in 1990.[13] These guidelines set out ten principles that nations should adhere to when drafting legislation to deal with issues relating to the collection, use and computerized storage of personal information. The ten principles are:

- collection and processing must be lawful and fair and personal information must not be used for purposes contrary to the purposes and principles of the Charter of the United Nations;
- those responsible for the collection and storage of personal information are also responsible for ensuring its accuracy;
- personal information should only be collected for specific and legitimate purposes and only used for the purposes for which it was collected;
- the individual to whom the personal information relates should have access to it;
- personal information which could give rise to unlawful or arbitrary discrimination should not be collected except in limited and restricted circumstances;
- departures from the first four principles should only be made if they are necessary to protect national security, public order, public health or morality;
- personal information must be securely stored;
- an authority should be designated to provide legal supervision of a nation's personal information handling practices and sanctions should be provided for violations of the protections guaranteed by the law;
- transborder flows of personal information should be restricted unless the other country has reciprocal safeguards;
- these principles are to apply initially to all public and private computerized files and should ideally be extended to manual files.

[13] United Nations General Assembly, *Guidelines Concerning Computerized Personal Data Files*, December 14, 1990, online: <http://www.unhchr.ch/html/menu3/b/71.htm>.

The Council of Europe's Convention 108

In 1980, the Council of Europe adopted the *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*[14] ("Convention 108"). The Council of Europe Convention 108 is legally binding on member states and requires them to enact personal information protection legislation that will cover the use of such information both by the public sector and the private sector.

Convention 108 is based on three main parts: 1) substantive law provisions in the form of basic principles; 2) special rules on transborder data flows; and 3) mechanisms for mutual assistance and consultation between parties to the Convention. The provisions of Convention 108 apply to every individual regardless of nationality or residence. The general principle is that clauses restricting data protection rights to a State's own nationals or legal residents would be incompatible with the Convention. Each party to the convention is to take the necessary steps to give effect to a common core of principles for the protection of personal information by enacting appropriate domestic legislation.[15] The core principles guarantee minimum protection with regard to automatic data processing. At the same time, countries enacting legislation to apply these principles also renounce restrictions on the transborder flow of data and agree to harmonize laws. Chapter III concerns this transborder flow of data and aims at the reconciliation of the competing requirements of free flow of personal information and data protection. Chapters IV and V provide the contracting states with mechanisms for co-operation.

The basic principles of data protection enunciated in the Convention 108 are:

- Quality of Data: Personal data undergoing automatic processing shall be: a) obtained and processed fairly and lawfully; b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; c) adequate, relevant and not excessive in relation to the purposes for which they are stored; d) accurate and, where necessary, kept up to date; e) preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which those data are stored.

- Special Categories of Data: Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

---

[14] Council of Europe Convention No. 108 of 18 September, 1980, Strasbourg, online: <http://conventions.coe.int/treaty/EN/cadreprincipal.htm>; see also Council of Europe, Explanatory Report on the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 1981.

[15] *Ibid.*, Chapter II, Article 4.

- Data Security: Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

- Additional Safeguards: Any person shall be enabled: a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 (Quality of data and Special categories of data); d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c is not complied with.[16]

While there are provisions for exceptions and restrictions to these principles, they are narrowly defined and, must be provided for by the law of a party. There must also be necessary measures in a democratic society in the interests of protecting State security, public safety, the monetary interests of the State, the suppression of criminal offences, for protecting the data subject or the rights and freedoms of others.

Although a number of the members of the Council of Europe have still not ratified the Convention, the Parliamentary Assembly voiced its unanimous support for the Committee of Ministers' adoption of the draft Protocol to the Convention No, 108 on strengthening personal data protection in April of this year. In doing so, the Assembly noted the importance of fundamental data protection safeguards in the age of information exchange and for the development of electronic commerce. The Council of Europe's Committee of Ministers also adopted guidelines setting out principles of fair privacy practices for users and Internet Service Providers (ISPs) last year.

The European Union and the Data Protection Directive

The European models for privacy legislation contain four distinct elements[17]:

- legislated norms controlling the collection and processing of personal information

- mandatory rights for citizens to access and review data about themselves and to review and challenge government and corporate information practices.

---

[16] *Ibid.*, Chapter II, Articles 5-8.

[17] See *Schwartz and Reidenberg, Data Privacy Law Charlottesville*: Michie, 1996, as quoted in Walczuch and Steeghs, Implications of the new EU Directive on Data Protection on Multinational Corporations, (2001) 14(2) Information Technology and People.

- special protection for sensitive data on ethnic origins, religious or political affiliations
- dedicated regulatory machinery to enforce and oversee privacy compliance.

In 1990, the European Union drafted its Proposal for a Council Directive Concerning the Protection of Individuals in Relation to the Processing of Personal Data. On October 24, 1995, the European Union adopted a Directive on the Protection of Personal Data With Regard to the Processing of Personal Data and the Free Movement of Such Data ("Data Protection Directive").[18] Member states were required to give effect to the Data Protection Directive by October 24, 1998.

This proposal and initiative was, at least in part, a response to the perception that there were inadequacies with the OECD Guidelines, which are not binding, and Convention 108, which had not received ratification by all European nations which are members of the Council of Europe.[19] The provisions of the EC Directive are directed toward two essential principles – the fundamental right to privacy and the establishment and functioning of an effective internal market within the Union for goods and services. These two principles are expressed in the recitals *inter alia* as:

> (2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;
>
> (3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded.

While the OECD Guidelines and Convention 108 provided important conceptual underpinnings for current privacy policy initiatives world-wide, it is the EU's Data Protection Directive that has really spurred the development of national laws in Europe as well as legislation outside of Europe. It did this not through conventional extraterritorial application, but through restrictions on data exports.

---

[18] *Directive 95/46/EC,* online at the Union's web site: <http://europa.eu.int>.

[19] Information and Privacy Commissioner for Ontario, *Privacy Protection Models for the Private Sector*, Tom Wright, Commissioner, December, 1996, online: <http://www.ipc.on.ca/scripts/index_.asp?action=31&N_ID=1&P_ID=11419&U_ID=0>.

Principles Relating to Data Quality

The EC Directive sets out the following principles that apply to the legislation that Member States must adopt for the protection of personal information:

- personal data must be processed fairly and lawfully;
- personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;
- personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- personal data must be accurate and, where necessary, kept up to date;
- every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed;
- Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.[20]

Criteria for Making Data Processing Legitimate

The processing of personal data must meet one of the following criteria before it is legitimate:

- there must be unambiguous consent;
- the processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps requested by the data subject prior to entering into a contract;
- the processing is necessary to comply with a legal obligation;
- the processing is necessary to protect vital interests of the data subject;

[20] *Supra* note 11, Article 6.

- the processing is necessary in the public interest or in the exercise of an official authority vested in the data controller or to a third party to whom the data are disclosed;

- the processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, but only if such interests are not overridden by the data subject's fundamental rights and freedoms, particularly the right to privacy with respect to the processing of personal data.[21]

Processing of Special Categories of Data

The processing of personal data which would reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life has particular restrictions which apply. Such processing is to be prohibited unless the specific and detailed criteria set out in Article 8 are met.[22]

Processing of Personal Data and Freedom of Expression

There are also special provisions in Article 9 to allow for the provisions of exemptions from the restrictions on data processing for processing carried out solely for journalistic purposes or for the purposes of artistic or literary expression. Member States need to draft laws that reconcile the right to privacy with the rules governing freedom of expression.[23]

Information to be Given to the Data Subject

Data subjects from whom personal data is being collected must be provided with: the identify of the controller of the data and the identity of his representative, if any; the purposes of the processing for which the data are intended; any further information such as the recipients or categories of recipients of the data and whether replies to the questions being asked of the data subject are obligatory or voluntary, as well as the possible consequences of failure to reply; and the existence of the right of access to and rights to rectify the data concerning him.[24]

When the personal data has not been obtained from the data subject, there is still an obligation to provide the data subject with at least the identity of the controller; the

---

[21] *Ibid*., Article 7.

[22] *Ibid*, Article 8.

[23] *Ibid*, Article 9.

[24] *Ibid*, Article 10.

purposes of the processing; and further information such as the categories of data concerned, the recipients or categories of recipients, and the existence of the right of access to and rights to rectify the data concerning him.[25]

The Data Subject's Right of Access to Data

The laws of Members States must provide rights of access to personal data held by a controller which must be without constraint, available at reasonable intervals and without excessive delay or expense. The right of access includes reasonable procedures for the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, and a method of notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking.[26]

Exemptions and Restrictions

Certain limited exemptions from the data processing requirements outlined above are permitted if the Member State requires such restrictions as a necessary measure to safeguard national security, defence, public security, criminal investigations or prosecutions, or the economic or financial interests of the Member State or of the European Union.[27] Anonymized data may also be used for the purposes of scientific research, and identifiable data may be used for scientific research as long as there are adequate legal safeguards to ensure that the data are not used for taking measures or decisions regarding any particular individual.[28]

Judicial Remedies, Liability and Sanctions

Articles 22 through 24 and Article 28 provide that the laws of Member States must provide for a public authority which will be responsible for monitoring the application of the provisions adopted by the Member State pursuant to the Directive.[29] There must be a right of every person to a judicial remedy for any breach of the rights guaranteed him under the laws of the Member State.[30] Any person who has suffered damage as a result of an unlawful processing of personal data or of any act incompatible with the law of the Member State is entitled to receive compensation for the damage suffered from the offending

---

[25] *Ibid*, Article 11.

[26] *Ibid*, Article 12.

[27] *Ibid*, Article 13.1.

[28] *Ibid*, Article 13.2.

[29] *Ibid*, Article 28.

[30] *Ibid*, Article 22.

controller.[31] Member States are to adopt suitable measures to ensure the full implementation of the provisions of the Directive and lay down the sanctions to be imposed in case of infringement of the measures taken to implement those provisions.[32]

Restrictions on the Transfer of Personal Data to Third Countries

Chapter IV[33] (Articles 25 and 26) provides that the laws of Member States must provide that the transfer of personal data to a third country for processing may take place only if the third country in question ensures an adequate level of protection for the personal data. There is a framework of criteria for assessing the adequacy of the data protection laws of the third country and Member States are to inform each other of cases where they consider that a third country does not ensure an adequate level of protection to personal data. Article 31 provides for a committee to be composed of representatives of the Member States which can rule on whether a third country has adopted adequate measures. If it finds that a third country does not ensure an adequate level of protection, Member States must take the measures necessary to prevent any transfer of personal data to the third country.[34] Article 26 sets out a number of exceptions to allow transfers of personal data in certain circumstances to third countries even if the personal data protection measures in that country are deemed to not be adequate.

Ongoing Working Party

Article 29 provides for the establishment of a Working Party to examine questions covering the application of the national measures adopted under the Directive in order to contribute to the uniform application of such measures. The Working Party may also give the Commission an opinion of the level of protection in the Community and in third countries and advise the Commission on any proposed amendment of the Directive or, on any additional or specific measures to safeguard the rights and freedoms of natural persons with regard to the processing of personal data. The Working Party has issued a number of Working Documents, Recommendations and Opinions. Many of these are available through the Commission's Web Site.[35]

Measures to be Adopted by the European Parliament and Council

At the time of the adoption of the Directive, the Commission declared it would also observe the principles contained within the Directive. The Commission and the

---

[31] *Ibid*, Article 23.

[32] *Ibid*, Article 24.

[33] *Ibid*, Articles 25 & 26.

[34] *Ibid*, Article 25.4.

[35] Online: <http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm>.

Council undertook to develop measures to implement the Directive in respect of Community institutions and bodies. On July 14, 1999 the Commission published a *Proposal for a Regulation of the European Parliament and of the Council*.[36] This Proposal represents a model code for the implementation of the principles and provisions of the Directive at the Community level.

The European Directive states in the Eighth Principle that "personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection. The process that countries go through to meet that test is multi-stage.

- a proposal from the EU Commission (this will be the final outcome of protracted negotiations between the EU and the national authorities of the state in question),
- an opinion from the Article 29 Working Party,
- an opinion of the Article 31 Management Committee delivered by a qualified majority of Member States,
- a 30-day right of scrutiny for the European Parliament to ensure that the Commission has acted properly,
- formal adoption of the decision by the EU Commission

This happened for Canada in Decision No. 2002/2/EC, O.J. L2/13 (2001) dated December 20, 2001.

The Cross-Cultural Dimension of Privacy

A paper like this is too short to explore fully the cross-cultural differences in privacy[37]. Although all commentators point to the seminal article by Brandeis and Samuel Warren, The Right to Privacy[38] as first articulating a conceptual base for the concept of privacy, America has followed a different policy track from the rest of the world. This may be because of First Amendment priority being attached to free speech concerns, because of a preference for market solutions and consumer choice over dirigiste regulation, or because of different history. When the Gestapo used French census rolls to identify French Jews for deportation, they showed in the most chilling fashion. The consequences of using personal information for purposes other than those for which it was collected. That historical memory still lingers, and has shaped European attitudes.

---

[36] Ibid.

[37] For a prolegomenon to such an analysis, see Walczuch, Singh and Palmer, An Analysis of the cultural motivations for transborder data flow legislation (1995), 8(2) Information Technology and People 37-57.

[38] *The Right to Privacy* (1890) L. Harv. L.R. 193.

The Contrast in Privacy Policy

EUROPE	*UNITED STATES*
More trust in government	More trust in private sector/market solutions
Government will root out and control abuse	Mass media will expose/shame abuse
Comprehensive laws preferable	Sector – specific laws where necessary
Self regulation is equivalent to no regulation	Regulation must pass cost benefit test
Broad rules with narrow exemptions	Technology can solve problems caused by technology
Overprotect consumers rather than under-protect	Empower consumers with information – let them choose

In May 2004, Ontario's Information and Privacy Commissioner and Arizona's Pouemon Institute released a Cross-National Study of Canadian and U.S. Corporate Privacy Practices. It dramatically showed how businesses on both sides of the border saw privacy. By significant margins, Canadian businesses saw privacy protection in terms of consumer relationships – building customer trust and brand loyalty; whereas for American businesses, privacy was simply another compliance and risk management issue.

The Report found:

(a) Canadian companies are more likely to have a dedicated privacy officer or leader responsible for privacy issues than comparable U.S. companies. In addition, privacy programs in Canadian firms tend to have a clearly articulated strategy, mission and charter. Canadian privacy leaders are more likely to have high level reporting authority and access to significant resources within their organization.

(b) Canadian companies are more likely to have a formal redress process for customers and other stakeholders to respond to queries and concerns about how personal information is used, shared and retained. Similarly, Canadian companies are more open to providing customers with access rights to see and correct personal information collected about them and their families.

(c) While Canadian and U.S. privacy policies have similar language and nearly identical levels of complexity, Canadian policies appear to offer more choice to customers and consumers in terms of opting out (or opting in) to secondary uses and sharing. In addition, while data sharing with third parties is a common practice in both Canada and the U.S., none of the Canadian companies actually permitted the sale of customer data.

(d) Canadian companies are more likely to offer privacy training or awareness programs for employees and contractors who handle sensitive personal information than comparable U.S. companies.

(e) Corporate marketers in Canadian companies appear to be more involved in their company's privacy initiatives than comparable U.S. companies.

(f) Canadian companies appear to hold their vendors and other third parties to higher standards or due diligence requirements. This is especially the case for companies that acquire sensitive personal data for legitimate business purposes. There is no clear evidence, however, that Canadian companies are more aggressive at monitoring or enforcing these standards than comparable U.S. companies.

(g) Canadian companies appear to have a more aggressive data control orientation when collecting and retaining sensitive personal information. Canadian companies are more concerned about insider misuse than external penetration.

(h) Canadian companies appear to require more rigorous data quality controls and monitoring requirements for transacting and moving of personal information about employees and customers, especially when the application involves transborder movement.

(i) U.S. companies use more rigorous data security mechanisms and controls to prevent potential hackers from penetrating the company's IT core and data warehouses.

(j) U.S. companies are less likely to have strict policies that protect the privacy of employees' personal data and records. In Canadian companies there are few policies governing the monitoring and surveillance of employee computer usage in the workplace.

(k) Both Canadian and U.S. companies have a difficult time measuring the effectiveness of specific controls intended to reduce privacy risks.

(l) Both Canadian and U.S. companies have an equally difficult time proving the economic value of privacy and data protection on corporate profitability (ROI).

The IPC/Powemon Study has no longitudinal dimension, but I suspect that since September 11, 2001, the priority given to privacy has shifted.

- Security, external threats and a war mentality loom larger than protecting individual privacy rights.

- The growth of electronic commerce no longer seems as linked to overcoming consumer fears about privacy threats – the technology of secure shopping is more advanced and accepted.

- In terms of corporate priorities, the Sarbanes – Oxley legislation commands much more attention in the boardroom – in part because the personal consequences for both management and directors are more severe and immediate.

Canada is markedly different, and in this respect more European in the way it approaches privacy in both regulatory and business terms.

Europe and the US

Article 25 of the EU Directive establishes the principle that transfers of personal data to third countries should only take place where the third country in question ensures an adequate level of protection. However, the United States has been reluctant to adopt a comprehensive legislative scheme for the protection of personal information. Accordingly the European Commission and the United States Government, through the Department of Commerce, entered into extensive discussions in order to develop mechanisms whereby personal data could be transferred across the Atlantic and the requirements of the Directive could be met. These discussions focussed on the establishment in the US of an agreed "benchmark" standard of protection or a set of "safe harbor" principles that would be enforced by the Federal Trade Commission and other U.S. public bodies (depending on the sector concerned). They involved consultation with industry and the general public.

The negotiations were conducted at senior levels. Ira Magaziner, fresh (though doubtless bruised) from being the architect of Hilary Rodham Clinton's health care reforms, led the effort from the White House. The Clinton Administration was the first US administration to have to confront the Internet, as a global force of economic and cultural transformation. It formally expressed a strong preference for regulatory abnegation.

Safe Harbor Compromise

On July 27, 2000, a "safe harbor" arrangement with the U.S. was finally, formally approved by the European Commission.[39] The principles adopted in this arrangement were deemed to provide "adequate privacy protection" in the context of Article 25 of the Data Protection Directive. If U.S. organizations choose to comply with these principles, they may continue to receive personal data from Europe that they require in the course of business operations.

The decision of an organization to enter the Safe Harbor is entirely voluntary. Once an organization decides to participate, however, it must comply with all of the requirements in the Safe Harbor framework and it must publicly declare that it is doing so. Organizations must self-certify annually and the US Department of Commerce will maintain a list of all those that have done so. The Safe Harbor is expected to become operational in

[39] Online: <http://www.ita.doc.gov/td/ecom/menu.html>

early November of this year. A list of Safe Harbor organizations should be posted on the Department of Commerce website around the same time.

Safe Harbor Principles

The seven Safe Harbor principles require the following:

- **Notice**: Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.

- **Choice**: Organizations must give individuals the opportunity to choose (opt out) whether their personal information is to be disclosed to a third party or to be used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorised by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorised subsequently by the individual.

- **Onward Transfer** (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

- **Access**: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

- **Security**: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorised access, disclosure, alteration and destruction.

- **Data integrity**: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

- **Enforcement**: In order to ensure compliance with the Safe Harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and

damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the Safe Harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants and Safe Harbor benefits will no longer be assured.

Enforcement of Safe Harbor Commitments

In general, enforcement of the Safe Harbor will take place in the United States in accordance with U.S. law and will be carried out primarily by the private sector. Private sector self-regulation and enforcement will be backed up as needed by government enforcement of the federal and state unfair and deceptive statutes. The effect of these statutes is to give an organization's Safe Harbor commitments the force of law *vis-a-vis* that organization.

If an organization persistently fails to comply with the Safe Harbor requirements, it is no longer entitled to benefit from the Safe Harbor. Persistent failure to comply arises where an organization refuses to comply with a final determination by any self regulatory or government body or where such a body determines that an organization frequently fails to comply with the requirements to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce of such facts. The Department of Commerce will indicate on the public list it maintains of organizations self certifying adherence to the Safe Harbor requirements any notification it receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of Safe Harbor benefits.

Frequently Asked Questions

To provide further guidance, the Department of Commerce has also provided a set of frequently asked questions and their answers, which clarify and supplement the principles.

Sensitive Data Exceptions

Organizations do not need to provide an explicit opt-in choice with respect to sensitive data if the use of the data is: a) in the vital interests of the data subject or another person; b) necessary for the establishment of legal claims or defences; c) required to provide medical care or diagnosis; d) carried out in the course of legitimate activities by a foundation, association or any other non profit seeking body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members of the body or to the persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; e) necessary to carry out the organization's obligations in the field of employment law; or f) related to data that are manifestly made public by the individual.

Journalistic Exceptions

Where the rights of a free press embodied in the First Amendment of the United States Constitution intersect with privacy protection interests, the First Amendment must govern the balancing of these interests with regard to the activities of U.S. persons or organizations. Personal information that is gathered for publication, broadcast, or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives, is not subject to the requirements of the Safe Harbor privacy principles.

Secondary Liability

The Safe Harbor privacy principles do not create secondary liability. Therefore ISPs, telecommunications carriers, or other organizations are not liable under the Safe Harbor privacy principles when on behalf of another organization they merely transmit, route, switch or cache information that may violate the principles. To the extent that an organization is acting as a mere conduit for data transmitted by third parties and does not determine the purposes and means of processing those personal data, it would not be liable.

Investment banking, audits and head-hunters

Investment bankers and auditors may process information relating to an individual without that individual's knowledge only to the extent and for the period necessary to meet statutory or public interest requirements, and in other circumstances in which the application of these principles would prejudice the legitimate interests of the organization. These legitimate interests include the monitoring of companies' compliance with their legal obligations and legitimate accounting activities, and the need for confidentiality connected with possible acquisitions, mergers, joint ventures or other similar transactions carried out by investment bankers or auditors.

Role of Data Protection Authorities (DPA)

Under the Safe Harbor arrangement, U.S. organizations receiving personal data from the EU must commit to employ effective mechanisms for assuring compliance with the Safe Harbor privacy principles. An organization may commit to co-operate with the DPA by declaring in a Safe Harbor notification to the Department of Commerce (see Self-Certification below) that the organization: a) elects to satisfy the requirement in points (a) and (c) of the Safe Harbor enforcement principle (7 above) by committing to co-operate with the DPA; b) will co-operate with the DPA in the investigation and resolution of complaints brought under the Safe Harbor approach; and c) will comply with any advice given by the DPA where the DPA take the view that the organization needs to take specific action to comply with the Safe Harbor privacy principles (including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the principles) and will provide the DPA with written confirmation that such action has been taken. The co-operation of the DPA will be provided in the form of information and advice in the following way.

The advice of the DPA will be delivered through an informal panel of DPA established at the European level, which will among other things help ensure a harmonized and coherent approach. The DPA panel will provide advice to the electing U.S. organizations on unresolved complaints from individuals about the handling of personal information that has been transferred from the EU under the Safe Harbor arrangements. This advice will be designed to ensure that the Safe Harbor privacy principles are being correctly applied and will include any remedies for the individual(s) concerned that the DPA consider appropriate. The panel will provide such advice in response to referrals from the electing organizations and/or to complaints received directly from individuals against the electing organizations, while encouraging and if necessary helping such individuals in the first instance to use the in-house complaint handling arrangements that the organization may offer. Advice will be issued only after both sides in a dispute have had a reasonable opportunity to comment and provide any evidence they wish to. The panel will seek to deliver advice as quickly as this requirement for due process allows. As a general rule, the panel will aim to provide advice within 60 days after receiving a complaint or referral and more quickly where possible. The panel will make public the results of its consideration of complaints submitted to it, if it sees fit. The delivery of advice through the panel will not give rise to any liability for the panel or for individual members of the DPA.

Self-Certification

Safe Harbor benefits are assured from the date on which an organization self-certifies to the Department of Commerce (or its designee) its adherence to the principles as set out below. To self-certify for the Safe Harbor, organizations can provide to the Department of Commerce (or its designee) a letter, signed by a corporate officer on behalf of the organization that is joining the Safe Harbor, that contains at least the following information: a) name of organization, mailing address, email address, telephone and fax numbers; b) description of the activities of the organization with respect to personal information received from the EU; c) description of the organization's privacy policy for such personal information, including: i) where the policy is available for viewing by the public; ii) the effective date of implementation of the policy; iii) a contact person for the handling of complaints, access requests, and any other issues arising under the Safe Harbor arrangements; iv) the specific statutory body that has jurisdiction to hear any claims against the organization regarding possible unfair or deceptive practices and violations of laws or regulations governing privacy; v) name of any privacy programs in which the organization is a member; vi) method of verification (e.g., in-house, third party); and vii) the independent recourse mechanism that is available to investigate unresolved complaints. The Department of Commerce (or its designee) will maintain a list of all organizations that file such letters, thereby assuring the availability of Safe Harbor benefits. Such self-certification letters should be provided not less than annually. Both the list and the self-certification letters submitted by the organizations will be made publicly available.

Verification

To meet the verification requirements, an organization may verify that the attestations and assertions they make about their Safe Harbor privacy practices are true, and that those privacy practices have been implemented as represented and in accordance with

the Safe Harbor privacy principles, either through self-assessment or outside compliance reviews. Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible and conforms to the Safe Harbor privacy principles, and that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints. It must also indicate that it has in place procedures for training employees in its implementation, and disciplining them for failure to follow its policy, and that it has in place internal procedures for periodically conducting objective reviews of compliance with the policy. Where the organization has chosen outside compliance review, such a review needs to demonstrate that its privacy policy regarding personal information received from the EU conforms to the Safe Harbor privacy principles, that it is being complied with and that individuals are informed of the mechanisms through which they may pursue complaints. The methods of review may include without limitation auditing, random reviews, use of "decoys" or use of technology tools as appropriate.

Access

Individuals must have access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the legitimate rights of persons other than the individual would be violated.

Human Resources Data

Where a company in the EU transfers personal information about its employees (past or present) collected in the context of the employment relationship, to a parent, affiliate, or unaffiliated service provider in the United States that has chosen to participate in the Safe Harbor, the transfer enjoys the benefits of the Safe Harbor arrangements. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected and any conditions for or restrictions on its transfer according to those laws will have to be respected. A U.S. organization that has received employee information from the EU under the Safe Harbor arrangement may disclose it to third parties and/or use it for different purposes only in accordance with the first Safe Harbor privacy principles regarding notice and choice.

Article 17 *Contracts*

Data controllers in Europe are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU. The purpose of the contract is to protect the interests of the data controller, i.e. the person or body that determines the purposes and means of processing and that retains full responsibility for the data with respect to the individual(s) concerned. The contract thus specifies the processing to be carried out and any measures necessary to ensure that the data

is kept secure. A U.S. organization participating in the Safe Harbor arrangement, and receiving personal information from the EU merely for processing, does not have to apply the principles to this information, because the controller in the EU remains responsible for it vis-à-vis the individual in accordance with the relevant EU provisions.

Dispute *Resolution* and Enforcement

Organizations may satisfy the enforcement requirements through the following: a) compliance with private sector developed privacy programs that incorporate the Safe Harbor privacy principles into their rules and that include effective enforcement mechanisms of the type described in the enforcement principle; b) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or c) commitment to co-operate with DPAs located in the European Community or their authorized representatives, provided those DPAs agree. This list is intended to be illustrative and not limiting.

Choice - *Timing* of Opt-Out

Generally, the purpose of the choice principle is to ensure that personal information is used and disclosed in ways that are consistent with the individual's expectations and choices. Accordingly, an individual should be able to "opt out" of having personal information used for direct marketing at any time, subject to reasonable limits established by the organization such as giving the organization time to make the opt-out effective. When it is impracticable for an organization to provide the individual with an opportunity to opt out before using the information, the organization may use the information for certain direct marketing purposes if the organization promptly gives the individual such opportunity at the same time to decline to receive any further direct marketing communications and the organization complies with the individual's wishes.

Airline *Passenger* Reservations

Airline passenger reservation and other travel information, such as frequent flyer or hotel reservation information and special handling needs, such as physical assistance or preparing meals to meet religious requirements, can be transferred to organizations located outside the EU in a number of situations. Under Article 26 of the Data Protection Directive, personal data may be transferred "to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2)" on the condition that it: a) is necessary to provide the services requested by the consumer or to fulfil the terms of an agreement, such as a "frequent flyer" agreement; or b) has been unambiguously consented to by the consumer. U.S. organizations subscribing to the Safe Harbor arrangement provide adequate protection for personal data and may therefore receive data transfers from the EU without meeting those conditions or other conditions set out in Article 26 of the Data Protection Directive.

Pharmaceuticals

If personal data is collected in the EU and transferred to the United States for pharmaceutical research and/or other purposes, the Safe Harbor privacy principles apply to

the data once they have been transferred to the United States. Data used for pharmaceutical research and other purposes should be made anonymous as appropriate.

Public *Record* and Publicly Available Information

It is not necessary to apply the Safe Harbor notice, choice or onward transfer principles to public record information, as long as it is not combined with non-public record information and as long as any conditions for consultation established by the relevant jurisdiction are respected. Also, it is generally not necessary to apply the Safe Harbor notice, choice or onward transfer principles to publicly available information unless the European transferor indicates that such information is subject to restrictions that require application of those principles by the organization for the uses it intends. Organizations will not have liability for how such information is used by those obtaining such information from published materials.

One of the key unresolved issues between Washington and Privacy is whether the current compromise Safe Harbor regime offers a sufficient guarantee for European data exports or whether Brussels will return to try to renegotiate more comprehensive and mandatory protections. After a slow take-up there are now 335 companies on the Safe Harbor list. While some of the names are impressive Fortune 500 household names (Procter and Gamble, Microsoft, IBM, Intel and Weyerhauser) they constitute a tiny fraction of US European trade participants.

Larger politics affects privacy. The Bush Administration's foreign policy has returned to historic isolationism in the light of terrorist threats and the Afghan and Iraqi wars. It has not been receptive to European policy priorities and it is difficult to imagine the administration yielding to what it would see as a business-hostile initiative with no domestic political benefits.

The evolution of privacy protection in Canada

Attitudes towards privacy in Canada fall, as they do in so many other respects, somewhere between the European and U.S. positions. Privacy policy had been an issue in Canada for some time before the introduction of the EU Data Protection Directive. However, the Directive had a definite influence on the development of privacy legislation in Canada.

The federal government had already passed the *Privacy Act*[40] in 1982 "to extend the present laws of Canada that protect the privacy of individuals and that provide individuals with a right of access to personal information about themselves".[41] The private sector does not fall within the scope of the Act. However, the Act did establish the office of Privacy Commissioner, with responsibilities similar to those of the European data protection authorities.

---

[40] R.S.C. 1985, c.P-21.

[41] *Ibid.,* see the preamble.

In 1990, the Canadian Standards Association brought together a number of groups to discuss the desirability and feasibility of a model privacy code that could serve as a standard for firms. Consensus was reached in September 1995 and the code was adopted as a national standard in March 1996. The code was closely modelled on the OECD Guidelines.

In the meantime, Quebec adopted the *Act Respecting the Protection of Personal Information in the Private Sector*[42] in 1993. This Act has a provision that could potentially stop data flows into other jurisdictions.[43] The existence of this law accelerated calls for harmonization and helped to make the legislative approach more acceptable among Canadian policy-makers.[44]

In 1995, the Information Highway Advisory Council, a group of industry representatives, recommended the adoption of federal legislation to protect personal information. Around the same time, Industry Canada was being warned about the possible effects of the new European Data Protection Directive.[45] The development of legislation for the protection of personal data in the private sector was labelled a "Key Priority" in Industry Canada's 1996-1997 Annual Report.[46]

Like the U.S., Canada has benefited enormously from the growth of electronic commerce. Estimated at about $45 billion in 1998, global electronic commerce revenue is expected to approach $2 trillion in 2004.[47] This growth should be encouraged as much as possible, but doing so requires clever balancing between individual privacy concerns and the high premium that the modern knowledge-based economy places on the sale and exchange of consumer information. Some may say, as many do in the United States, that the best way to do this is through self-regulation.

At the same time, Canada has felt pressure to respond to Article 25 of the Date Protection Directive. Again, from a non-European perspective, this provision in the Directive prohibits member countries from transferring personal information to non-member countries whose laws or other security measures do not ensure a comparable level of

---

[42] R.S.Q. c. P-39.1.

[43] *Ibid.,* see s.17.

[44] Sebastiaan Princen, "International Trade and Domestic Regulation: The Case of Data Protection Policies" (NKWP Politicologenetmaal, Veldhoven, 14-15 June 2001) [unpublished], online: <http://www.usg.uu.nl/organisatie/medewerkers/s.princen/Princen%20Veldhoven%20paper.pdf>.

[45] Industry Canada, *Privacy and the Information Highway* by Ian Lawson (Ottawa: Canadian Cataloguing in Publication Data, 1995), online: *strategis.ic.gc.ca* <http://strategis.ic.gc.ca/epic/internet/inoca-bc.nsf/vwapj/Priv_e.pdf/$FILE/Priv_e.pdf>.

[46] online: *Industry Canada* <http://www.ic.gc.ca/cmb/welcomeic.nsf/532340a8523f33718525649d006b119d/eba3880ce823fa03852569f30078bfd0!OpenDocument>.

[47] A. Diana, "Search Engines Critical to E-Business Success" *E-Commerce Times* (16 April 2004), online: <http://www.ecommercetimes.com/story/33441.html>.

protection. In practice, the provision could prevent, for instance, a European branch office from transferring customer information to its home office in North America. While Ottawa was able to fend off European pressures for a decade by arguing that private sector privacy codes (culminating in the work of the Canadian Standards Association) provided effective protection, ultimately only legislation could satisfy the concerns of the EU.

Personal Information Protection and Electronic Documents Act

The *Personal Information Protection and Electronic Documents Act*[48] was passed in April of 2000. Part I of the Act mandates how businesses may use, collect and disclose identifiable information about individuals. Under the Act's definition, personal information includes such data as race, ethnic origin, age, financial history and personal opinions, but does not cover the name, title, business address or telephone number of an organization's employees. Because the definition's original limitation to "information recorded in any form" was deleted from the final version of the Act, the law will likely protect such personal information as blood type and DNA. The law applies to any organization that collects, uses or discloses personal information in the course of commercial activity. Commercial activity is defined broadly, to include a range of activities such as sales, purchases, barters, exchanges and leases of individual personal information, fundraising or membership lists. Expressly excluded are hospitals, health clinics, physicians, and information used exclusively for journalistic, artistic or literary purposes. The Act applies to all federally regulated industries and all organizations that trade in personal information in more than one province; it is also supposed to apply to all private sector companies collecting, using or disclosing personal information within any one province, unless that province has passed its own, parallel legislation.

The *Personal Information Protection and Electronic Documents Act*[49] ("*Personal Information Protection and Electronic Documents Act*") was passed in 2000. *Personal Information Protection and Electronic Documents Act*'s scope is limited to the private sector. In the "Background" to Bill C-6 (that introduced *Personal Information Protection and Electronic Documents Act* to Parliament), *Personal Information Protection and Electronic Documents Act* is described as a response to the European Directive on Data Protection. The concern was that the Directive could "have a negative impact on Canadian businesses engaged in commerce with companies in European Union countries, unless adequate privacy legislation is introduced in Canada".[50] *Personal Information Protection and Electronic Documents Act* was Canada's response to that concern.

---

[48] For information on this Act and on what it means for businesses, see "Privacy Law's Bite May be Worse than its Bark", McMillan Binch Corporate Bulletin (May, 2000)

[49] S.C. 2000, c.5.

[50] "Bill C-6: Personal Information Protection and Electronic Documents Act", online: *Library of Parliament* <http://www.parl.gc.ca/common/Bills_ls.asp?Parl=36&Ses=2&ls=C6>.

The EU has approved the *Personal Information Protection and Electronic Documents Act* as providing an adequate level of protection for personal data that is transferred to recipients who are subject to it. It was noted in the Commission Decision that the Act does not apply to the public sector.[51] Unlike the American "Safe Harbor" agreement, the Act is direct legislation, in accordance with the EU Directive and akin to the sort that has been passed in most EU countries.

Other Initiatives

Canada and the EU are also synchronizing their e-commerce strategies to create a consistent international framework for e-commerce development. The Joint Statement on Electronic Commerce[52], proposed July 17, 2000, focuses on the areas of privacy, consumer protection and security. Action steps include the development of compatible standards in the protection of personal data; the development of consumer trustmarks and alternative dispute mechanisms; and the development of cross-border recognition of electronic signatures.

Current Controversial Issues

Conflict of laws

By preventing data transfers to third countries that do not adequately protect personal data, the Data Protection Directive closes a loophole available to companies that wished to avoid compliance with the European Union's strict standards. Whatever the motives of the EU in adopting this aspect of the Directive, it has had an extraterritorial effect. Other countries must comply with EU standards by implementing adequate protection for personal data, or face the prospect of a stoppage in the flow of that data. The economic consequences of a blockage in the cross-border transfer of personal data would be significant.

We may think of threats to stop data export as more theoretical than real yet European privacy regulators have not hesitated to act, if they see violations.

- In 1989 before Italy passed its data protection law, French regulators stopped Fiat's French subsidiary from transferring personnel records back to head office in Turin

- In 1995, American Airlines was blocked from transferring personal data on Swedish passengers back to the United States over the Sabre travel information network. The Swedish Data Protection Board held that there were simply inadequate privacy protections in place. The Board was particularly concerned that reporting on passengers preferences for Kosher or halal meals would signal religious information

---

[51] Commission Decision 2002/2/EC of 20 December 2001, online: <http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=en&numdoc=32002D0002&model=guichett>.

[52] Online: <http://europa.eu.int/comm/external_relations/canada/summit_12_99/e_commerce.htm>.

and that noting that a passenger would need a wheelchair on arrival disclosed disability

- Deutsche Bahn, the German National Railway was delayed in setting up a private label credit card with Citibank until transborder data safeguards had been negotiated.

Canada and the U.S. have reacted in different ways to the Directive. Canada quickly adopted the *Personal Information Protection and Electronic Documents Act*, which passed the adequacy determination of the European Commission. The U.S. has resisted this response from the beginning. The U.S. has always taken a self-regulatory approach to privacy. Americans do not believe that legislation is necessarily the most effective means to protect privacy.[53] Individuals value their personal data to different degrees. For example, some people will gladly give out personal information in exchange for free access to an online magazine, where others will not. As such, personal information may be well suited to regulation by market forces. Further, privacy legislation may encroach on the right to free speech.[54] Americans do not necessarily accept that privacy is a fundamental, freestanding right.[55] They are more inclined to see privacy as one concern that must be balanced against others.

This difference in approaches is an example of the difficulty with the harmonization of privacy standards. Many countries are in the process of developing their own policies on personal data protection. However, the EU Directive is influencing the development of those policies. The debate around the Safe Harbor agreement is the result of policy differences between the U.S. and EU. The U.S. does not want their privacy policy dictated to them by the EU.

This, in turn, creates a problem for businesses. Companies are faced with the difficulty of complying with each country's requirements. Businesses must be concerned about facing liability in other jurisdictions even if they are complying with the requirements of their home jurisdiction. Companies may have to implement multiple standards, or adopt the most costly measures wholesale in order to comply with the strictest jurisdiction in which they do business. It is this effect that Americans refer to when they label the EU Directive as extraterritorial.

Aircraft Passenger Data Sharing

In Summer 2003, following protracted negotiations, the European Commission reached a draft agreement with U.S. Securities Authorities on the sharing of air

---

[53] Aaron Lukas, "Safe Harbor or Stormy Waters? Living with the EU Data Protection Directive" *Center for Trade Policy Studies* (30 October 2001), online: CATO Trade Policy Analyses <http://www.freetrade.org/pubs/pas/tpa-016es.html>.

[54] See Eugene Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking about You" (2000) 52 Stanford L. Rev. 1049.

[55] *Supra* note 35.

passenger data. During March and April 2004, this draft agreement had a rough ride in the European Parliament. On March 31st, 2004, by a vote of 209 to 202, the European Parliament voted to reject the measure. A number of countries, including Sweden and France, rejected the idea that European passenger data would be stored by American authorities for up to 3½ years and shared with other government agencies. In negotiations between Brussels and Washington, American demands for significant quantities of passenger data were scaled back. The European Parliament Civil Rights Committee noted that "in the U.S.A., the protection of privacy is not regarded as a fundamental right" explaining why it had opposed the draft agreement.[56]

Three weeks later, on April 21st, 2004 the European Parliament voted by 276 to 260 in favour of referring the draft agreement on passenger data to the European Court of Justice in Luxembourg to assess whether the agreement would contravene EU law.

Airline companies were caught in the middle, between compliance (which would place them in breach of EU data protection laws) and refusing to comply with U.S. requests for the information (which could expose them to fines and the loss of airport landing slots in the U.S.).

By moving it to the European Court of Justice, this politically sensitive issue has effectively been sidelined during a U.S. election year.

Compliance and Enforcement

Actual compliance with privacy protection requirements has not been uniform. Some companies might be taking the chance that these requirements will not be enforced. In a 2001 survey of European data regulatory authorities, the Cato Institute (American policy analysts) concluded that the EU has not taken local enforcement of the Directive very seriously. Of the 16 European privacy offices surveyed, only 4 reported any enforcement actions related to illegal data transfers.[57]

It is not clear whether EU websites are better protected than those in the U.S. Three years after the Directive was adopted, Consumers International called for better enforcement in the EU after a study showed that American websites were doing a better job of protecting consumer privacy.[58] American authorities are unlikely to want to force companies to comply with strict legislation if a self-regulatory approach is more effective. And yet, in order to ensure global compliance, there must be co-operation among regulators as to enforcement.

---

[56] "Commission's passenger data policy attacked again" o*ut-law.com – legal news and business guides* (19 March 2004), online: out-law.com < http://www.out-law.com/php/page.php?page_id=commissionspasseng1079703509&area=news> (last modified: 19 March 2004).

[57] *Supra* note 36 at 23.

[58] Joris Evers, "U.S. beats Europe in online privacy protection", *Consumers International*, online: <http://www.consumersinternational.org/search/newssearch.asp?newsID=408&regionid=135&langid=1>.

Applying legislated requirements against small websites based in foreign countries will be very difficult. And yet, it would be unfair to enforce these policies only against large foreign-based business enterprises. To do so would call into question the consistency with which the Directive is applied and make strict privacy requirements look like a protectionist, non-tariff barrier to trade.[59]

It is possible that without the clear threat of enforcement, there will be no compliance with legislative requirements. If the EU is not serious about applying sanctions, the Directive may eventually be ignored. If that is the case, then the U.S. will have won the policy standoff and privacy will be governed by the American self-regulatory regime.

Cookies

A recent European Union initiative respecting Internet cookies calls into question the commitment of EU Member States to privacy legislation.

In June 2002 the EU passed a directive on data protection, which had to be incorporated into national law by legislation.[60] What the European Union was attempting to do in this as in other areas was to develop a multi-national approach to cookie abuse. Yet, by the deadline for implementation, only four countries (Austria, Sweden, Denmark and Italy) had implemented the requirements on cookie protection.[61] The directive required members of the European Union to enact legislation providing for complaints to a national authority if websites failed to alert Internet users concerning cookies that were automatically downloaded to their computers. Websites were required to display prominently on a popup window or elsewhere immediately visible on a homepage, details about the cookies and their functionality. While it did not forbid websites from initially setting the cookies onto user's computers, they did have to provide easy instructions to help them remove the cookies and to refuse any future cookies. In theory, the national legislation would also permit legal action to be taken against spammers (although given the extent to which spam is exported from the United States, merely national protections may be insufficient).

Trade

The EU Data Protection Directive may yet constitute a trade irritant between the U.S. and the EU. If an amicable arrangement about Safe Harbor cannot be reached, the U.S. may challenge the EU Directive at the WTO. The trade aspects of data protection have been addressed in the General Agreement on Trade in Services (GATS). The GATS seeks to

---

[59] Matthew Broersma, "Data protection laws still face uphill battle" (19 May 2003), online: ZDNet UK News <http://news.zdnet.co.uk/hardware/emergingtech/0,39020357,2134904,00.htm>.

[60] *Directive 2002/58/EC Directive on Privacy and Electronic Communications*, online: <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf>.

[61] Paul Meller, "Only four EU countries enacted cookie directive" IDG News Service, online: ComputerWeekly.com <http://www.computerweekly.com/Article126168.htm>.

reduce barriers on information flows. However, the focus of the U.S.-EU dispute will rest on the General Exceptions to the GATS requirements that are set out in Article XIV.

Article XIV makes specific allowance for "measures … necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to … the protection of the privacy of individuals in relation to the processing and dissemination of personal data".[62] The EU would argue that the Data Protection Directive falls under this exception. However, reliance on Article XIV is "subject to the requirement that such measures are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail". The Americans would claim that these conditions apply and the EU cannot rely on the exception.

The American argument would be that the self-regulatory approach to the protection of privacy is as effective as the EU legislative approach. Thus, "like conditions prevail" in the two jurisdictions, and the prevention of data flows due to the manner in which that protection is achieved amounts to "unjustifiable discrimination between countries". The outcome of such arguments before the WTO is by no means certain.

To date, no challenge has been brought. The U.S. did not want to make this into a trade dispute, and chose to engage in talks that led to the Safe Harbor agreement instead.[63]

Outsourcing

Outsourcing of the processing of personal data has become a major trade issue. For a clear example of how domestic privacy requirements shape actions abroad, consider how India's outsourcing sector has responded to fears that the success of the sector would be hurt unless privacy was fully guaranteed.[64] To satisfy its American clients, Indian businesses have installed advanced technological and physical security, and invited international accounting firms to audit the adequacy of privacy practices. To assuage Brussels, New Delhi is drafting a law, explicitly responding to the European Directive. Market and technological responses contrast with legislation as the primary instrument of policy response.

Yet Capital One, a U.S. credit card company, recently pulled their outsourcing activities out of India after discovering that staff at its call centre were offering U.S. customers unauthorised credit levels and free gifts. The Evening Standard, a London

---

[62] Article XIV(c)(ii)

[63] Sebastiaan Princen, "International Trade and Domestic Regulation: The Case of Data Protection Policies" (NKWP Politicologenetmaal, Veldhoven, 14-15 June 2001) [unpublished], online: <http://www.usg.uu.nl/organisatie/medewerkers/s.princen/Princen%20Veldhoven%20paper.pdf>.

[64] See Simon Chester, Will Privacy Kill Outsourcing, National Post. August 16, 2004, and Simon Chester, Do Privacy Risks Doom Outsourcing? Counsel to Counsel, September 2004.

newspaper, reported that criminal gangs are bribing Indian staff with a year's wage to steal credit data from UK and U.S. customers (though this is so far unsubstantiated). A campaign has been launched by Amicus, a financial service sector union, to prevent such offshore outsourcing.[65]

Amicus cites a recent report by Ernst & Young predicting that "given the volume of offshoring that is going on and the risks attached, there will be a major regulatory failing within five years." David Fleming, the Amicus National Secretary for Finance, has said: "Offshoring is an accident waiting to happen. It is only a matter of time before a serious crime is committed which ruins the reputation of the British financial services industry."[66]

Though this issue is largely framed in terms of privacy concerns, other factors may also be in play. At present, India has no data protection regulations, and companies rely on individual contracts negotiated with Indian outsourcing contractors to address data protection issues.[67] However, this type of arrangement is specifically allowed under the EU Data Protection Directive. According to the Information Commission in the UK, no rules have been broken by any companies with call centres in India.[68]

The real motivation for Amicus may not be concern over actual data protection shortcomings in India, but rather the loss of UK jobs. However, perhaps due to mounting pressure abroad, India is considering implementing data protection legislation of its own.[69] Thus, outsourcing is an example of the extraterritorial effects of the EU Directive and of how privacy concerns could arguably be leveraged for protectionist agendas in trade.

Sharing Data Down South: Interjurisdictional Issues With The United States

Unlike the European data protection directive[70] and the various European national statutes implementing that convention, Canada's privacy legislation does not specifically address trans-border data flow[71] nor have the findings of the Privacy

---

[65] Amicus, "Offshore Credit Card Fraud Causing Chaos in India" (25 March 2004), online: na europe <http://www.naeurope.co.uk/en/print.htx?nr=300002225>.

[66] BBC News, "Fear over India call centre fraud", (5 April 2004) online: BBC News - Business <http://news.bbc.co.uk/1/hi/business/3593885.stm>.

[67] "MEPs protest offshoring of data", o*ut-law.com – legal news and business guides* (5 April 2004), online: out-law.com <http://www.out-law.com/php/page.php?page_id=mepsprotestoffshor1081155146&area=news>.

[68] Andy McCue, "Offshore data security fears dismissed by UK" (6 April 2004), online: silicon.com <http://www.silicon.com/management/government/0,39024677,39119817,00.htm>.

[69] "India to upgrade data protection this year" o*ut-law.com – legal news and business guides* (23 April 2004), online: out-law.com <http://www.out-law.com/php/page.php?page_id=indiatoupgradedat1082713196&area=news>.

[70] Found at http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf

[71] For an earlier study on this matter see *Laperrière, René Crossing the borders of privacy : transborder flows of personal data from Canada, Université du Québec à Montréal. Groupe de recherche en informatique et droit*

Commissioner shed any great light on the rights and obligations of Canadians with respect to personal information which is transferred outside Canada.

Given the increasing integration of North American retail markets, it is conceivable that a new American entrant into a retail sector might seek to purchase customer lists from an existing Canadian retailer. Alternatively, the American parent of a Canadian retailer may seek access to the Canadian subsidiary's customer lists for the purpose of conducting an integrated North American marketing campaign. Can this be done without breaching Personal Information Protection and Electronic Documents Act? The answer will turn on the disclosure that has been made to each customer, and the extent of consent which has been granted. If the form of consent expressly states that information may be transferred to a third party or shared with a parent or affiliate, then both retailers can argue that their transaction concerning the personal information of customers has been contemplated when consumer consent has been given to the collection, storage and disclosure of personal information. However, more frequently, the consent will be narrower, ambiguous or missing. Under such circumstances, Personal Information Protection and Electronic Documents Act would prohibit the transfer of data to the American party, unless the Canadian retailer contacts Canadian consumers informing them of the proposed transaction and seeking their consent.

In addition, the Canadian retailer must ensure in its transaction documents (or intra-company transfer protocols) that the receiving party agrees to provide comparable protection to the personal information, comparable to that given it by the Canadian retailer. If this were not the case, then the receiving American party would, presumably, be free to exploit the information without limit or restriction.

Of course, the jurisdiction of the Canadian Privacy Commissioner would not extend to sanctioning directly the receiving American party for any such breach. Instead, the original Canadian retailer would find itself exposed to sanctions for failing to take adequate care in the disclosure of personal information, specifically by failing to require "comparable protection". Finally, if any of the personal information was itself receiving internationally, from a country in the European Union, then to transfer it to a third jurisdiction which did not have legislation which met the requirements of the European data protection directive, would be prohibited under that directive. While the United States has a framework Safe Harbor Agreement with the European Union, it applies only to specific businesses which have agreed to conducted themselves in accordance with stated principles. Generally, transfers of European – sourced personal information to most businesses in the United States would breach the requirements of the directive[72].

---

[72] For general discussions of the impact of Personal Information Protection and Electronic Documents Act on American businesses, see Charnetski, William, Graeme Coffin, Steven Schoenfeld. Canada's privacy law is now in effect: while impact on U.S.-based e-commerce not entirely clear, ignoring it is not wise. New York Law Journal April 30, 2001 v225 i82 s0 pS-5. Klosek, Jacqueline, Walter Krzastek. The impact of Canadian privacy legislation on U.S. organizations. The Computer & Internet Lawyer June 2001 v18 i6. Plotkin, Bruce L. Canada's new privacy statute touches U.S. companies. Colorado Lawyer March 2001 v30 p87. Spaeth, Juliana M., Mark J. Plotkin, Sandra

Outsourcing Of Personal Information Handling

Given the shifting of information, telecommunication, data transfer, and comparative labour costs, there has been a growing trend in recent years to contract to outsource the handling of consumer transactions, including the handling and processing of personal information, to contracting parties outside the jurisdiction. Within North America, the more common flow is for American processes to outsource to Canadian provinces like Ontario, New Brunswick and Alberta. However, in some sectors (particularly, some financial services and medical insurance information handling) the data flow may be from Canada to the United States. The analysis on page 35 would apply to the processing of Canadian personal information in the United States, if it was collected by a Canadian entity. That is, the Canadian entity should ensure, by contractual or other means, that the receiving American entity understands its obligations to protect the confidentiality of personal information.

For American personal information, being handled in Canada, the answer is partly clear. However, the definition provisions in Personal Information Protection and Electronic Documents Act speak generally about the protection of an individual's personal information, and do not limit its safeguards in protecting Canadian citizens or permanent residents. Thus, the more prudent course would be for any Canadian organization handling American personal information to effect privacy rights and to apply the same safeguards that it would for Canadian personal information. In practice, it would be extremely difficult to do anything else.

Of course, it is even less likely that a U.S. party may seek to exercise access and correction right under Personal Information Protection and Electronic Documents Act than Canadians would. Finally, the border provides no immunity for those who would breach consumer protection laws, as a Calgary company recently found out. The company had aggressively marketed business directory listing services to U.S. residents. They charged consumers and businesses up to $399 for unauthorized listings and for business directories. While they guaranteed a full refund for unsatisfied purchasers, they frequently failed to honour their commitments. The company's collections department harassed non-payment consumers. The Federal Trade Commissioner responding to consumer complaints took on the case and obtained an ex parte temporary restraining order from U.S. District Court of Washington State, Western District. The FTC permanently barred the defendants and the employees from engaging or participating in the advertising, promoting of telemarketing business directories to U.S. residents. The final judgment also barred the Calgary defendants from selling their customer lists and imposed the judgment of close to $2.4 million, if the defendants were found to have misrepresented their financial conditions to the FTC. The judgment was entered into the U.S. District Court for the Western District of Washington on May 11th, 2004. The lesson of the case is that consumer regulators will not hesitate to pursue fraudulent conduct across the border. In this case, they worked closely with the

---

C. Sheets. Privacy, eh! The impact of Canada's Personal Information Protection and Electronic Documents Act on transnational business. Vanderbilt Journal of Entertainment Law and Practice Winter 2002 v4 p28-46.

Federal Competition Bureau, the Alberta Government, the Calgary Police, the RCMP and the Better Business Bureau of Southern Alberta.

Conclusion

The American approach to the Internet and the new digital economy has been to try to encourage the market through a lack of direct control. However, it may be argued -- as the Europeans have argued -- that the new global market is made less, not more efficient by the "patchwork" approach to regulation that has resulted in the U.S. and world-wide. Europe insisted that it was not mandating its standards extraterritorially in the restrictions on data exports in the Data Protection Directive but rather ensuring that massive loopholes in privacy protection were not created by the mere fact of the global interconnectivity of information. Domestic laws or policies, whether direct legislation or self-regulatory alone cannot provide the consumer confidence necessary to encourage real growth of e-commerce and to maximize new global markets. The simple truth is that regulating a global market requires global co-operation.

In passing the *Personal Information Protection and Electronic Documents Act*, Canada acknowledged this reality. The FTC's grudging admission that direct legislation may indeed be the only way to effectively address the issue of privacy in today's online, electronic world portends the possibility of a more complete change in American policy as well. A country once committed to the idea of self-regulation in online and electronic industry may eventually have to succumb to public and international pressures to pass comprehensive privacy legislation.

At the same time, advocates of self-regulation continue to maintain that legislation is not an effective way of protecting privacy in cyberspace. The pace of evolution in information technology is just too quick for the slow, limited response of national and international law. While the European Data Protection Directive, the Canadian *Personal Information Protection and Electronic Documents Act* and the U.S. "Safe Harbor" agreement may fulfil the purposes for which they were designed (particularly, the transfer of personal information in a commercial context) they do not protect consumers against all invasions of privacy that are currently and potentially possible in a "cyber" world. Self-regulation advocates maintain that only consumer self-protection can provide that level of security.

Cynical observers have noted that in practice, European privacy appears to be no better protected than American. Building a regulatory and compliance bureaucracy may not change actual behaviour that much. At this point, the only thing that is certain is that these laws are not the final word on privacy protection.

At this stage in the evolution of global privacy law it is too soon to say how far multinational business will be changed or constrained by privacy legislation. In the short-run, the dialectic will continue as business and their advertisers explore the technology of marketing. What may appear to us as intrusive exploitation of personal information may someday seem simply the acceptable (though inevitable) consequence of the intelligent deployment of technology to ensure that messages are neither unsolicited, irrelevant nor unwelcome, but instead are attractive, targeted and with personalized incentives or pricing.

Whether in Europe, as in Canada, this evolution will continue, will depend as much on public attitudes and acceptance, as it will on the pronouncements of under-resourced privacy watchdogs. It will also turn on scandals and mistakes, since policy in this area is largely driven by such media events.[73] In this area, observers need not follow the law reports to see how the law and practice is evolving. For good or ill, concerns about privacy will be an inescapable part of being human in the Twenty-First Century.

[73] See the Equifax-Lotus Marketplace affair and the Double-click controversy: see generally, Cate, Fred H. Privacy in the Information Age, (Brookings Press, 1997, found online at http://brookings.nap.edu/cgi-bin/chaphits.cgi?term=&isbn=0815713169. For Double-click see Kotzker, Jason A. The great cookie caper: internet privacy and target marketing at home and abroad St. Thomas Law Review Spring 2003 v15 i3 p727-756; Burger, Michael, Internet privacy chronicles: DoubleClick's cookie monster. Corporate Counsel May 2000 v7 i5 p15 (2); Culberg, Katya, Bill Reilly. DoubleClick settles; implements greater transparency procedures in data collection, agrees to pay settlement of $450,000. Journal of Internet Law Sept 2002 v6 i3 p25 (2); Major online advertiser agrees to privacy standards for online tracking. The Computer & Internet Lawyer Nov 2002 v19 i11 p32 (2); Riccardi, Michael A. DoubleClick wins dismissal of suit alleging 'cookies' harmed Web users. New York Law Journal March 30, 2001 v225 i61 p1; Roth, Mark S. Beware of cookies; do marketers that track a user's online activities threaten privacy? The National Law Journal August 20, 2001 v23 i52 pC1; Shepherd, Ritchenya A. Tackling the Web's privacy problems. The National Law Journal April 24, 2000 v22 i35 pB1