Other People's Standards: Privacy in International E-Commerce

By Paul Jones*

Introduction

The growth of e-commerce, both business-to-consumer and business-to-business, continued unabated long after the collapse of the internet bubble in March 2000. As it grows and matures, the policy differences between nations on the handling of personal information and protection to be afforded to the internet consumer have given rise to concerns about the foreign treatment of the personal information of consumers, and the terms under which business-to-consumer e-commerce is conducted.

On February 20, 2007 Jim Webb, a newly elected Democratic senator from Virginia, expressed those concerns from an American perspective when he said "When you start sending data to India and subcontracting it down to China, that's an issue. It's a liability issue for a lot of the companies and a security issue for the government." [1] He went on to say that "I'm not sure that you need legislation, but you'll definitely see oversight from me on the issues of security and privacy. Data transmission outside this country, into countries that don't have the same privacy standards that we do and security standards we do, I'm absolutely opposed to it."[2]

Which countries do not have the same privacy standards as the United States? Most of the developed countries in the world do not have the same privacy standards as does the United States, the same is true for most of the developing countries. Most of these countries have better and stricter standards than does the U.S., and they share Senator Webb's concerns about the transfer of their citizens' personal information to countries that they perceive to have less stringent privacy laws, such as the United States. And their concerns are exacerbated by reports

that even minimal American standards on security are not being adhered to, such as the failure of the FBI to properly monitor its use of "National Security Letters."[3]

Europe has been a leader in developing privacy laws. The first law regulating the collection and use of personal information in computer files was adopted by the German state of Hesse (the area around Frankfurt-am-Main) in 1970[4], and the first national law was adopted by Sweden in 1973.[5] A model data protection law, known as the "European Data Directive,"[6] was developed by the European Union to harmonize the privacy laws of member states. Europe in turn has influenced the development of privacy laws in Canada,[7] Argentina,[8] Australia, [9] New Zealand[10] and Hong Kong SAR.[11]

Even one of the targets of Senator Webb's concerns, the People's Republic of China, began drafting a comprehensive private sector privacy law based on the European model, in 2002.[12] It has held consultations on a draft to which it invited representatives from Hunton & Williams, a law firm based in Senator Webb's home state of Virginia. Progress on the draft has been slow while the new Property Law was being debated.[13] The drafting is now expected to accelerate.

Taiwan has had a data protection law for computer processed information[14] since 1995, and Japan enacted legislation[15] that came into effect April 1, 2005. But in the Congress, attempts to pass a comprehensive private sector privacy law have not been successful. The United States is the only remaining developed country[16] in the world that relies on sector specific privacy laws for the protection of the personal information of its citizens.

Use of the internet has greatly expanded the markets available to entrepreneurs. A web site may attract visitors from all over the world. This inevitably has led to questions regarding the applicable law (or laws) implicated when an on-line transaction is made between persons

located in different countries. One of the first general rules to develop was that the simple passive availability of a web site did not attract the jurisdiction of foreign courts.[17] Currently, the consensus appears to be that a retailer must take active steps to target a particular jurisdiction in order for a court to find the retailer subject to the laws of the jurisdiction.[18]

But if the entrepreneur wishes to increase foreign sales, the logical next step is to modify the web site to be more attractive to foreign visitors. Modifications could include adding pages in other languages, posting prices and accepting payments in other currencies, adding store locators adapted to other countries and making other product or service specific adaptations. It also could include the addition of a privacy policy that complies with the privacy laws in the target country.

One American entrepreneur, Accusearch Inc. of Cheyenne, Wyoming, operates a web site known as "Abika.com" offering background checks, criminal record checks, and similar services. It has a privacy policy that selects laws of the State of Wyoming as the controlling law. But in early 2004 it agreed to provide a background check on a Canadian privacy activist, Philippa Lawson.[19] The report purported to provide a criminal record check for the Province of Ontario for Ms. Lawson. It should be noted that in Canada all criminal law is federal and national in nature, and that criminal records are not publicly available.

Ms. Lawson complained to Canada's Privacy Commissioner that such a report was a breach of Canada's privacy law, PIPEDA.[20] The Commissioner investigated and discovered that Accusearch also operated a Canadian web site "Abika.ca." But the Commissioner ultimately concluded in her decision that she lacked jurisdiction to deal with the actions of a United States party.[21] Ms. Lawson sought judicial review of the Privacy Commissioner's refusal to further investigate the matter. In a decision released on February 5, 2007[22] the Federal Court held that

the Privacy Commissioner did indeed have jurisdiction to investigate complaints against United States parties, and pointed out that:

> Private parties in a lawsuit in Canada cannot compel a foreigner to appear here to testify. Letters rogatory issued by a Canadian court to a foreign court requesting that a subpoena be issued in that jurisdiction requiring the witness to appear before a commissioner there are commonplace. By the same token, section 46 of the *Canada Evidence Act* contemplates that a foreign court or tribunal may likewise seek the aid of a Canadian court.[23]

In essence, the Canadian court held that Canada's Privacy Commissioner had jurisdiction over an American based e-commerce business that sold the personal information of a Canadian to a Canadian. That alone is not decisive in the grant of letters rogatory, but it does indicate to e-commerce businesses targeting Canada or doing business with Canadians that a failure to comply with Canada's privacy laws may have negative consequences.

In contrast to Senator Webb's concerns about transfers of American personal information to inappropriate countries, Canadian and European commentators and politicians are expressing concerns about the transfer of the personal information belonging to their citizens to the U.S. Their fears are compounded by the actions of the current U.S. Administration in the "war on terror."

A columnist for Canada's largest circulation daily newspaper recently wrote:

> What is Dalton McGuinty thinking of? The Ontario premier and his Liberal government now want to introduce a new, intrusive driver's licence chock full of personal information about the holder – and then hand all that data over to the U.S. government.
>
> This, incidentally, is the same U.S. government that recently passed a law to exclude foreigners it imprisons without charge outside America from enjoying the most basic of legal rights – that of challenging their detention before a judge.[24]

The Office of Canada's Privacy Commissioner has expressed similar concerns in somewhat less journalistic tones,[25] but it is the newspaper columnist that is more likely to have been read by a

potential Canadian e-commerce customer. In Europe similar concerns have been expressed most recently regarding the SWIFT case.[26]

E-Commerce business models that wish to expand their international markets will need to consider their compliance with foreign privacy laws or risk a mix of regulatory action, civil lawsuits and/or unfavorable publicity in such foreign jurisdictions, and possibly in the U.S.

Privacy Laws Around the World – General Principles

Privacy concerns found early expression in laws in Europe. By 1980 the concerns were general enough that the OECD issued its now famous Guidelines.[27] The Guidelines identified what it called the "Basic Principles of National Application." These 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.
>
> *Data Quality Principle.* Personal data maintained by the data custodian 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 fulfillment 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 Paragraph 9 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 unauthorized access, destruction, use, modification or disclosure of the 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 to: (a) obtain from a data controller confirmation of whether or not the data controller has data relating to him; (b) have his data communicated to him, relating to him within a reasonable time at a charge, if any, that is not excessive; a reasonable manner and in a form that is readily intelligible to him; (c) be given reasons if a request made is denied, and to be able to challenge such denial for the data, and (d) challenge the accuracy 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.

These principles find an American analog in the principles articulated by the Federal Trade Commission as "Notice, Choice, Access and Security."[28] In other words:

1. Individuals should be given notice of the proposed collection, including use and disclosure, of personal information and the specific purposes for such activity.
2. In order for the data to be collected, used or disclosed, appropriate consent should be obtained with respect to the specified purposes.
3. The data collected should be protected by appropriate security measures.
4. The individual must have access to the data collected, and to details of its use and disclosure.

Informational privacy legislation is based on what might be called a "contract" model. An offer is made to an individual to collect, use or disclose the individual's personal information for a specified purpose. The individual has the choice of agreeing or declining. In this way individuals have the option of defining privacy in their own way, to their own particular sensitivity.

Other jurisdictions differ from the United States in the balance that they strike between the strict enforcement of consumer contracts and the protection of consumers in their jurisdiction. Most notably courts in France have struck down standard form clauses used by American internet service providers.[29]

As with contracts, problems have developed with the nature of the consumer's understanding of the contract that is being proposed, the meaning of some of the terms, and the balancing of interests or fairness of the contract or consent. In traditional contract law these are often referred to as problems of "unconscionability" or "good faith." Thus significant variations are developing between jurisdictions with respect to the limitations or restrictions that they impose on privacy contracts.

For example, a number of European jurisdictions prescribe various types of personal information that must be considered sensitive, and they either require more explicit consent or prohibit collection of such personal information altogether. In Canada the federal privacy law requires that organizations collect, use and disclose personal information "…only for purposes that a reasonable person would consider appropriate in the circumstances."[30]

On the other hand, in the United States under the Gramm-Leach-Bliley Act regarding financial institutions, there is no such limitation and marketers are free to seek the consent of the individual for the collection of their personal information for any purpose. This has resulted in what some might see as abuses. One bank said that it would make two kinds of disclosures. The first was to "Financial Service Providers." The second was to "Non-financial Service Providers." Another had a list of categories of organizations with which it would share information. The final category was "Other." [31]

The balance between freedom to contract and consumer protection is a critical difference in the privacy laws and consumer policies between the United States and jurisdictions such as the European Union and Canada. This difference is becoming a source of significant liability for American e-commerce entrepreneurs wishing to expand their markets.

Several of the other principles identified could be explained as the state prescribing certain basic terms to the contract, such as an obligation to keep the personal information secure, to grant the individual access to her own file, to disseminate basic information about the relationship, in order to correct market failures in the negotiation of the contract.

Another common problem with consumer contracts is that they are seldom read, and even less often fully understood. So it is with privacy policies. The question then arises as to what may be inferred in such situations. Did the individual consent to the "contract" or not? For a marketer who sends out mass mailings of a flyer with a privacy notice on the back, the choice of presumptions is critical. If the individual is required to opt-in to further mailings, say by ticking a box and mailing back the notice failing which the individual's name and address must be deleted from the marketer's mail list, then the marketer will probably lose most of the names on the list. On the other hand, a presumption that failure to respond implies consent, or "opt-out," is open to considerable abuse in certain circumstances. Consider the example provided earlier from certain banks. Was that even a real choice?

In some jurisdictions the solution to this conundrum is to vary the nature of the permitted consent with the sensitivity of the information and its proposed use or disclosure in the context of the material facts of the transaction. This approach was discussed in the "Detailed Comments" to the OECD Guidelines,[32] but it is not an approach that is easily reduced to specific rules. While some jurisdictions have tried to define the concept of "sensitivity" with respect to personal information, others have left it to the courts to determine on the facts of each particular case.

Such vagueness may or may not be a bad thing, depending on your perspective. While businesses are concerned that some of their practices may fall into a grey area with respect to compliance, an individual is also less likely to commence a costly court action if the chances of

winning are less certain. While the consumer may complain, the most appropriate and cost-effective dispute resolution procedure for both parties in these circumstances is negotiation and mediation. And this is in fact what many privacy commissioners do.

Such a solution, however, does not produce a very bright-line test that gives the certainty so often desired by clients. But outside of the United States, that tends to be how privacy law is structured. The practice of privacy law may well require the development of the ability to judge what, for example is sensitive personal information without the aid of specific rules.

Specific Provisions in the European Market

General Provisions

As mentioned earlier , a very early law attempting to regulate the collection and use of personal information in computer files was adopted by the German state of Hesse (the area around Frankfurt-am-Main) in 1970,[33] and the first national law was adopted by Sweden in 1973.[34] France adopted a national law on data protection in 1978.[35] But other jurisdictions in Europe, despite their close relationship with these countries, and the use of a civil law model derived from the laws of either Germany or France, did not adopt privacy or data protection laws until relatively recently.

For example private sector data protection was introduced in Italy in 1996,[36] and then further developed in a comprehensive privacy code that came into force on January 1, 2004.[37] Spain adopted its law in 1999,[38] and Luxembourg was among the last to adopt a law in August 2002.[39]

The differing rules for the protection of personal information in the European Union interfered with the ability of retailers in particular to operate through the E.U., thus jeopardizing the establishment and functioning of the internal market that is one of the primary goals of the

E.U. Accordingly, the European Parliament and Council adopted what has since become known as the "European Data Directive"[40] to require the member states to harmonize their laws. It was the adoption of the European Data Directive that led to the adoption of data protection laws in Italy, Spain and Luxembourg.

The European Data Directive became the model for all data protection laws of its member states, although only the laws of the individual member states are actually effective and enforceable in a given jurisdiction. There are a number of features of the European model of data protection that distinguish it from other models to some degree, and should be noted in order to more easily review and understand the model.

As it arose specifically out of concerns about the use of computers to collect and store personal information on a scale not previously experienced, Article 3 of the Directive limits the scope of application of the Directive to "…the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system." Thus member states are not required to provide protection for personal information that is collected manually other than as part of a filing system.[41]

In much of privacy and data protection law, distinctions are made between the laws applicable to the public sector and those applying to the private sector. In Canada the privacy protection for personal information collected and used by the public sector is generally dealt with in 'Freedom of Information' legislation that is separate from private sector privacy legislation. In Australia the two are combined into one statute, but operate relatively independently. The European Data Directive applies to the processing of personal information in both the private and public sectors (except for criminal and security matters), and the provisions applicable to the two

sectors are fully integrated. Consequently, care must be taken when reviewing European laws to be sure that it is clear that the relevant provision applies to the private sector and not just to the public sector.

Otherwise, the European Data Directive requires that personal information be collected only for specified, explicit and legitimate purposes, that excessive data not be collected, that the data be accurate and where necessary kept up to date, and be kept for no longer than is necessary. Data may be processed only if the data subject has given unambiguous consent or where the processing fits within certain other exceptions set out in Article 7 of the Directive. Article 10 specifies the information that must be given to a data subject, such as identity of the data controller and the purposes for the processing, and Article 12 specifies the data subject's rights of access to data relating to him or her. The data subject also has certain rights to object to the data being processed. And, of course, the data must be kept confidential and secure.

Article 8 prohibits the processing of special categories of data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership and data concerning health or sex life unless the processing fits within certain specific exceptions, one of which is if the data subject has given explicit consent. These may be described as "sensitive areas" of personal information. In the opinion of some, the concept of "sensitive information" is key to the effective application of privacy principles to particular situations, and the use of appropriate forms of consent. However, the concept is not defined, for example, in Canadian privacy law.

With respect to the consent of the data subject to collection and processing of personal information, the Directive specifies that certain minimum information must be given to the data subject to ensure that consent is properly obtained.[42] But the provisions in national laws vary

significantly in this area. In the Netherlands and the United Kingdom the requirements are deliberately not specified and an obligation is placed on the data controller to disclose any further information that is necessary to make the giving of consent fair and informed.[43]

Generally, information that must be provided so includes the identity and address of the data controller and the identity of its or their representative, the purpose for the processing, the identity of the recipients or categories of recipients of the data, whether the provision of certain information is voluntary or required, the consequences of a failure to provide the information and the existence of a rights of access to and a utility to rectify the data. The development of a form of consent for use across Europe requires the review of each jurisdiction's requirements, and cannot be prepared based only on a review of the Directive.

Advance Notification to the Data Protection Authority

One of the most significant aspects of the European Data Directive is the requirement for notification to the data protection authority by a data controller before processing may commence, as set out in Article 18. The contents of the required notice are specified in Article 19. The purpose of such notification is to allow the data protection agency to assess the risk posed to the rights and freedoms of the data subjects by the proposed processing, and to post such information in a national register accessible to all. While this process is intended to be simple and easy to comply with, in practice notification can be more involved and is likely to be the part of the law with which a foreign retailer or e-commerce entrepreneur will have the most contact.

First, data processing is not supposed to start until notification is complete. Different data protection authorities have different positions on when this occurs. The United Kingdom Information Commissioner has taken the position that notification is complete when a completed

form has been filed and the fee (35 pounds) is paid, even though it may be some weeks before a receipt is issued. But the Netherlands College Bescherming Persongegevens has in the past taken the strong position that processing can not begin until the receipt has been received by the data controller, which in their jurisdiction may not occur for more than a month.

Data controllers are required to appoint a local representative and identify that person on the notification form. Many European data protection authorities have set up web sites where the forms can be downloaded or even completed and submitted online. To assist foreign data controllers with their notifications, a growing number of data protection authorities provide English language translations of their notification laws and the guidelines for notification. However, the actual notification forms always are in their national language, as must be any correspondence with the authority.

There also may be a question as to who a data controller is, and who therefore has to be included in the notification.[44] The Directive states that:

> "controller"shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data….[45]

The precise wording of the definitions varies in the member states' national laws. Some specifically include all data processors.[46] If an American franchisor wishes to operate an international promotional contest from its head office in the United States, using its local franchisees or distributors to do some of the processing in their home jurisdiction, it may be necessary to list both the franchisor and franchisees or distributors on the notification.

The penalties for failing adequately to notify are fairly significant and constitute a substantial incentive to fully comply with the notification requirements. Remedies and penalties are not dealt with in the Directive, but rather in the national laws. Generally, these laws impose

a fine for failure to notify or for supplying incomplete or inaccurate information, and make the failure an offense punishable by a fine or imprisonment where the failure is deliberate.[47]

Transfer of Personal Data outside of the European Union

Compliance with the Directive cannot be ensured if personal data can be freely transferred outside of the European Union. Such transfers are particularly easy with respect to information. For this reason the European Data Directive requires that the member states restrict such transfers only to third countries that ensure an adequate level of protection.[48]

There are provisions in the Directive for the assessment of third countries privacy laws, and the European Commission has investigated and issued decisions recognizing that Switzerland, Hungary, Canada, Argentina and companies certified under the United States Department of Commerce's Safe Harbor Privacy Principles as providing adequate protection.[49] These approvals often are qualified depending upon the scope of the privacy law. In the case of Canada the approval is limited to "recipients subject to the Personal Information Protection and Electronic Documents Act."[50] The decision provides for a review three years after its notification to the member states.

The Directive also provides for derogations from the requirement that the third country have an adequate level of privacy protection.[51] For a foreign franchisor the exceptions of primary relevance are where:

(a) the data subject has given his or her unambiguous consent;[52]

(b) the transfer is necessary for the conclusion or performance of a contract between the data subject and a controller; and

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of a data subject between a controller and third party.

There also is a derogation allowing a member state to authorize a transfer to a third country if the data controller has ensured an adequate level of privacy protection for the

individuals concerned by contractual means. However, the local data protection authority is required to inform the European Commission regarding each of these transfers, and the Commission reserves the right to object to the transfer. There are serious concerns that not all of these arrangements are being reported. [53]

The Commission, also has approved a set of standard contractual clauses for the transfer of data to processors in third countries.[54] These may be used independently or included as part of larger contract. They are an option to assist persons doing business in the European Union and are neither a requirement nor a minimum standard. The advantage is that member states are required to recognize the clauses as providing adequate protection. The clauses also contain a restriction regarding onward transfer to countries that do not have adequate protection.

Because the United States has taken a different approach to privacy protection, and as such would not be considered as a jurisdiction having adequate protection by the European Union, there was considerable concern that the European Data Directive would become a trade barrier for American companies wishing to do business in the European Union. The European Commission and the United States Department of Commerce held negotiations that resulted in the development of the Safe Harbor Principles and its system of self-certification.[55]

Organizations wishing to self-certify must be subject to the jurisdiction of either the Federal Trade Commission or the United States Department of Transportation.[56] They are required to develop a privacy policy that contains the Safe Harbor Principles and appoint a person to administer the policy. The Safe Harbor Privacy Principles consist of seven stated principles that generally parallel the Date Directive. The policy also must specifically state that the organization adheres to the Safe Harbor Principles, which then becomes an enforceable representation to the public, as the policy must be made publicly available. Under the

enforcement principle, the organization must establish an independent recourse mechanism to which individuals can turn for the investigation of unresolved complaints. While it was initially anticipated that most participants would choose organizations such as TRUSTe, BBBOnline, the American Arbitration Association or JAMS which have developed Safe Harbor compliance programs, a review of the list of participants suggests that a large number have chosen to co-operate directly with European data protection authorities.

Upon submission of the self-certification form to the Department of Commerce, the materials are reviewed for completeness before being posted on the Safe Harbor list. As of June 5, 2007 there were 1,189 companies listed as adhering to the Safe Harbor Principles, of which 959 were current.[57]

One of the reasons may be that some Europeans, including some representatives of data protection authorities, mistakenly view Safe Harbor adherence as a requirement for American companies, even if for example the data subject has unambiguously given his or her consent to the transfer of their personal information to the United States. In other words, instead of being a legal alternative, adherence to the Safe Harbor Principles appears to be becoming a marketing or public relations requirement for American companies wishing to transfer personal information to the United States. However, concerns have been expressed about whether all listed companies truly adhere to the Safe Harbor Principles, as one review indicated that less than half the privacy policies met the standards expressed in the Principles.[58]

Enforcement

Europe is often seen by some as the leader in data protection law. Certainly it had some of the earliest laws and, on paper at least, some of the strictest. But its enforcement and awareness of these laws was surprisingly weak. In 2003 there were cases in Sweden[59] and France[60] in which fines of about $500.00 US were imposed for failures to notify data protection authorities or obtain consent for the use of personal information. Generally it is felt that the national data protection agencies are not well funded and have therefore not been vigorous about enforcement.

More recently, however, the climate in Europe appears to have shifted towards more vigorous enforcement. The OECD recent report on the cross-border enforcement of privacy laws[61] described the volume and characteristics of cross-border data floes as evolving and leading to elevated privacy risks. Some privacy commissioners and data protection authorities have discussed instituting tougher enforcement, as did the Canadian Federal Court with respect to cross-border complaints as mentioned earlier in this article.[62] For example, the United Kingdom the Information Commissioner has called for a penalty of imprisonment for up to two years for those found guilty of knowingly or recklessly of obtaining or disclosing personal data from data controllers without their consent or for selling such data. The Commissioner said:

> I repeat my call for a two year jail term to deter those convicted of trading unlawfully in personal information and am very encouraged that the government has consulted publicly on this.[63]

On the same day the Information Commissioner announced that Liverpool City Council had been fined £300 for failing to act on an information request by an employee.

In addition, the new United Kingdom *Fraud Act 2006*[64] came into effect in January 2007. Some have suggested that people who gather personal data in the course of their business without issuing a valid data protection notice could be subject to fines and imprisonment under this law.[65]

In the SWIFT affair mentioned earlier, after the Belgian Data Privacy Commission,[66] the Swiss Federal Data Protection Commissioner[67] and the Unabhäniges Landzentrum für Datenschutz Schleswig-Holstein (the Data Protection Commission for the State of Schleswig-Holstein)[68] had decided that SWIFT had broken their respective Data Protection Laws by the undeclared transfers of personal information to the United States on November 23, 2006 the Article 29 Working Party of the European Union announced that, in its opinion, SWIFT and the respective European financial institutions had failed to comply with the provisions of the European Data Directive.[69]

The decision rests on the finding that SWIFT was not a mere "data processor" but rather a "data controller." These are key concepts in the European data protection laws that are not found in other countries, and are used in determining notification obligations. They are not easy concepts to use and to have subtle variations from country to country. The participating financial institutions were found to be "joint controllers." The opinion states that:

> the hidden, systematic, massive and long term transfer of personal data by SWIFT to the United States Department of the Treasury in a confidential, non-transparent and systematic manner for years without effective legal grounds and without the possibility of independent control by public data protection supervisory authorities constitutes a violation of the fundamental European principles as regards data protection and is not in accordance with Belgian and European law. The existing international framework is already available with regard to the fight against terrorism. The possibilities already offered should be exploited while ensuring the required level of fundamental rights.[70]

Put more succinctly, SWIFT did not comply with European notification requirements and thus avoided having to respond to queries from the European data commissioners as to whether the transfers were a proportionate response to the risk.

There is a deep underlying reason for this. As has been revealed in the negotiations between the European Union and the United Stateds over the Safe Harbor program and over airline passenger name records, the two jurisdictions have deeply rooted differences in their conceptualization of privacy. Europeans tend to see privacy as a fundamental right that cannot be traded away. In the U.S. privacy is seen more as a property right that is tradable. Andreas Busch of Oxford has written a very useful paper discussing these negotiations and the differences.[71] It is very difficult to reconcile these differences, and perhaps SWIFT did not wish to try.

Finally, the French data protection authority, Commission Nationale de l'Informatique et des Libertés (known as "CNIL"), imposed its first fine pursuant to the 2004 amendments to the French law against a bank, Crédit Lyonnais,[72] for errors in reporting the credit status of several individuals. On December 21, 2006 it was reported that a French court had ruled that music companies and other copyright holders cannot conduct unrestrained internet monitoring to find pirates.

In summary, slowly enforcement of data protection and privacy laws has increased in Europe, and American e-commerce merchants doing business in Europe without complying with the local privacy laws increasingly are at risk. The same may be said for Canada.

Practical Solutions

American e-commerce business or other merchants planning on expanding outside of the United States should include a review, and where appropriate, upgrade of their privacy compliance measures and their privacy policies in their expansion plans, as compliance with United States privacy standards is most likely not sufficient for compliance with the standards

and laws in the target countries. If they are targeting just one foreign country, this can be accomplished by retaining local counsel in that jurisdiction. But if they wish to develop sales in several foreign jurisdictions the development of a compliance program requires some familiarity with the privacy and data protection laws of multiple jurisdictions. A coordinated approach can result in significant savings in legal fees. It is possible to develop one privacy policy that will be effective and compliant in multiple jurisdictions.

The steps in an international compliance program are otherwise similar to good practice in the United States. A compliance officer should be appointed and this person should prepare a draft plan for compliance implementation. A privacy audit should be conducted to determine where the business model is not yet in compliance with international privacy standards.

The next step is the development of a list of approved purposes for the collection, use and disclosure of personal information. The identification of the purposes for such activities is a requirement of international privacy standards. Drafting such purposes neither too narrowly nor too broadly is one of arts of an attorney familiar with international requirements.

Once this has been accomplished new privacy policies, online statements, consent forms and other communications can be prepared. Serious consideration should be given to registering under the Department of Commerce's Safe Harbor Program.

Although it is definitely possible to transfer personal information from Europe to the U.S. without registering with this Program, the Safe Harbor Program has come to symbolize American compliance to many Europeans. This may make registration a business requirement rather than a legal requirement.

Finally, once compliance has been achieved, the investment should not be lost. Policies should be developed to ensure that evidence and documentation exists for (a) each individual's

consent, for each database and purpose; (b) all uses of, or disclosures from, each database are properly recorded and protected, and are in accordance with the purposes; (c) and reviews of the databases for accuracy in accordance with the sensitivity of the information.

Responsibility for compliance may be better separated from responsibility for collection, use and disclosure. Collection, use, and disclosure should not be able to proceed without authorization from the compliance officer.

Provisions should be made for the regular training of new staff, and for review and update of the policies and for internal or external compliance audits. The development and application of privacy laws in the relevant jurisdictions should be monitored, particularly as the business expands into new markets. And a response plan to use in the event of allegations of a data breach should be developed. This may be part of a general crisis response plan or unit.

These are the steps being undertaken by businesses in foreign jurisdictions to ensure compliance with their own privacy and data protection laws. American businesses wishing to expand foreign markets will have to consider undertaking the same privacy compliance procedures.

---

*Paul Jones is the principal of Jones & Co. in Toronto, Canada and is a member of the Executive Committee of the Privacy Section of the Ontario Bar Association.

[1] David McGee, "Senator Concerned About Customer Data Overseas" *E-Commerce Times,* February 21, 2007; *Bristol Herald Courier*, February 21, 2007.
[2] *Ibid.*
[3] U.S. D.O.J., Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (Washington, DC: Office of the Inspector General, March 2007).
[4] Now part of *Hessisches Datenschutzgesetz* (HDSG) in der Fassung vom 7 Januar 1999.

[5] *Datalagen*, SFS 1973:289
[6] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L281, 23/11/2003 p. 0031-0050.
[7] *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c.5 (known as "PIPEDA").
[8] *Ley 25.326 Proteccion de los Datos Personales,* adopted October 4, 2000.
[9] Private sector privacy protection is provided primarily by the federal *Privacy Act 1988,* Act No. 119 of 1988 as amended by the *Privacy Amendment (Private Sector) Act 2000*, which came into effect December 21, 2001.
[10] *Privacy Act,* 1993 No.28.
[11] *Personal Data (Privacy) Ordinance,* Chapter 486.
[12] Sue Anne Tay, "China weighs credit database options," *Asia Times Online,* March 16, 2006.
[13] The Property Rights Law (物权法 or Wuquan Fa) was adopted by the National People's Congress on March 16, 2007. China has now completed two of the major sections of a full civil code, as the Contract Law (合同法 or Hetong Fa) was adopted in 1999. The next major section that they may work on is the section on "Persons," which includes privacy rights.
[14] *Computer-Processed Personal Data Protection Law* (电脑处理个人资料保护法, or "Diannao Chuli Geren Ziliao Baohu Fa") Republic of China, 84th Year, Ordinance No. 5960, adopted August 11, 1995 to come into force May 1, 1996. There are currently proposals to expand it.
[15] *Personal Information Protection Law*, Law No. 57, passed May 23, 2003, fully in force April 1, 2005.
[16] With the possible exception of Singapore, which is now considering whether to introduce a general data protection law, according to Channel News Asia, May 21, 2006.
[17] *Zippo Manufacturing Co. v. Zippo Dot Com, Inc*., 952 F. Supp. 1119 (W.D. Pa. 1997).
[18] See for example**:** Michael Geist, Is There a There There: Towards Greater Certainty for Internet Jurisdiction, Uniform Law Conference of Canada and Industry Canada, (64 pp.) (2001), *KK Sony Computer Entertainment v. Pacific Game Technology (Holding) Limited*; [2006] England & Wales High Court (Patents Court) 2509 (18 October 2006) regarding jurisdiction for patent infringement for goods advertised on a Hong Kong website; *Fernand c. S.A. Normalu*, Cour d'appel de Paris. O5/05038, 26 avril 2006 regarding use of a trademark on a Lebanese site; and the series of decisions regarding Yahoo!, Inc. and La Ligue Contre le Racisme et l'antisemitisme, in the U.S. and France.
[19] Ms. Lawson is a lawyer and the executive director of the Canadian Internet Policy and Public Interest Clinic at the University of Ottawa's Faculty of Law.
[20] *Supra* note 7.
[21] Issued November 18, 2005 and available at: http://www.privcom.gc.ca/legislation/let/let_051118_e.asp .
[22] *Lawson v. Accusearch Inc.*, 2007 FC 125.
[23] *Ibid.,* paragraph 40.
[24] Thomas Walkom, "Too much licence for U.S.: Why would McGuinty want to hand over so much personal data after recent abuses?, *Toronto Star*, Page 1, February 23, 2007.
[25] Patricia Kosseim, General Counsel, Office of the Privacy Commissioner of Canada, "Protecting Personal Information in Canada and Abroad: [Address to] The Canadian Corporate Counsel Summit," March 6, 2006, Toronto, available at http://www.privcom.gc.ca/speech/2006/sp-d_060306_pk_e.asp ; Office of the Privacy Commissioner of Canada, "Fact Sheet: What Canadians Can Do to Protect Their Personal Information Transferred Across Borders" published online August 18, 2004, available at: http://www.privcom.gc.ca/fs-fi/02_05_d_23_e.asp .
[26] Society for Worldwide Interbank Financial Telecommunication. See the Press Release on the SWIFT Case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the of the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 23 November 2006, available at http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_23_11_06_en.pdf .
[27] "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Recommendation of the Council of the Organization of Economic Co-operation and Development adopted on September 23, 1980. Available on-line at *http://www.oecd.org/dsti/sti/it/seur/prod/PRIV-EN.HIM*.

[28] In a Canadian context the words would be "Purpose, Consent, Access and Safeguards." "Notice" and "Choice" are very similar to "Purpose" and "Consent", but they are not the same.
[29] See for example *L'Union Fédérale des Consommateurs Que Choisir(UFC) c. Société AOL Bertelsmann Online France,* No. R.G. 02/03156, Tribunal de Grande Instance de Nanterre, rendu le 2 juin 2004.

[30] Section 5(3) of Canada's PIPEDA, *supra* note 7.
[31] John Swartz, *Privacy Policy Notices Are Called Too Common and Too Confusing*, New York Times, May 7, 2001. It must be noted that on March 21, 2007 the FTC released a Notice of Proposed Rulemaking requesting comment on a model form for privacy notices under the Gramm-Leach-Bliley Act.
[32] See Paragraph 45.
[33] *Supra* note 4.
[34] *Supra* note 5.
[35] *Loi No. -78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*
[36] Law No. 675/1996. *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali* (Protection of individuals and other subjects with regard to the processing of personal data).
[37] *Codice in materia di protezione dei dati personali* (Personal Data Protection Code), Decreto legislative n. 196 del 30 giugno 2003 (Legislative Decree no. 196/2003).
[38] *Ley Orgánica 15/1999, de 13 diciembre, de Protección de Datos de Carácter Personal.*
[39] *Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.*
[40] *Supra* note 6.
[41] The concept of a "filing system" is defined in Article 2(c) of the Directive thus: " 'personal data filing system' (filing system) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographic basis." The concept was considered in the U.K. case *Michael John Durant v. Financial Services Authority* [2003] EWCA Civ.1746, Court of Appeal (Civil Division), December 8, 2003. The decision in this case has since caused the U.K. Information Commissioner and the Irish Data Protection Commissioner to issue guidances on what is "manual data" and what is a "relevant filing system." Some regard this decision and the guidances as restricting the application of the U.K. *Data Protection Act 1998* to apply only to computerized personal information which focused on a living individual in a biographically significant way. In May 2004 Mr. Durant filed papers with the European Commission in Brussels claiming that the U.K. Government had not implemented the European Data Directive properly and the European Commission has now asked the U.K. Government to justify its approach (see " UK's data Protection Act might not meet European Union standards" *OUTLAW.COM* , May 19, 2004 and " European Commission suggests UK's Data Protection Act is deficient" *OUTLAW.COM*, July 15, 2004).
[42] Articles 10 and 11.
[43] Section 2(3) of Part II of Schedule I to the Data Protection Act 1998 in the U.K.; Article 33 of the *Wet bescherming persoonsgegevens* in the Netherlands.
[44] This is a significant issue in the SWIFT case, *supra* note 24.
[45] Article 2(d).
[46] See for example Germany's *Bundesdatenschutzgesetz,* Section 4e(2); Luxembourg's *Loi du 2 août 2002*, Article 13(1)(a).
[47] See for example the Netherlands' *Wet bescherming personsgegevens*, Articles 27 and 28 in the first instance, and Article 75(2) where the failure is deliberate.
[48] Article 25.
[49] "Commission decisions on the adequacy of the protection of personal data in third countries", available at *http://europa.eu.int/comm/internal _market/privacy/adequacy_en.htm.*
[50] 2002/2/EC Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act (notified under document number C (2001) 4539), *Official Journal L* , 04/01/2002 p. 0013-0016.
[51] Article 26.
[52] As always the law of the jurisdiction should be consulted for the precise wording of the requirement. For example in the U.K.'s Data Protection Act 1998, the wording in Schedule 4 regarding the consent required does not use the word "unambiguous."
[53] The first Commission Report on the implementation of the European Data Directive issued May 15,2003 stated that "many unauthorized and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection" (at page 19). As evidence of this was the very limited number of notifications received pursuant to Art. 26(3) of the Directive. Accordingly on August 21, 2003 a notice was sent out reminding national data protection authorities of the reporting requirements.

[54] Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC. The "Standard Contractual Clauses (processors)" are attached to the decision as an annex. The are available at *http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm.*

[55] Information about the Safe Harbor is available online at: *http://www.export.gov/safeharbor/index.html*, including the list of corporations that have self-certified and advice on how to self-certify. The self-certification form may be completed online.

[56] For a broader discussion about privacy and the Safe Harbor program, see Charles B. Cannon, "What Franchisors Need to Know About Privacy Rights, a Safe Harbor, and Standard Contractual Clauses Before Exchanging Personal Information with Europeans", *Franchise Law Journal* 176 (Winter 2003).

[57] Organizations that have self-certified within the last twelve months will have the note "current" under the certification status column. Those organizations that have not certified or re-certified in the last year, or which have notified the Department they no longer adhere to the safe harbor framework, will be identified as "not current" in their self-certification. Organizations that are "not current" are not assured the benefits of the safe harbor.

[58] Rosemary Jay and Angus Hamilton, *Data Protection: Law and Practice – Second Edition*, 227 (London: Sweet & Maxwell, 2003), based on an interim working paper from the E.U. issued February 13, 2002.

[59] *Sweden v. Bodil Lindqvist*, Case C-101/01 (E.C.J. November 6, 2003). Ms. Lindqvist was a volunteer on a church committee. In furtherance of her volunteer work she set up a web site that the church recognized and used. To make her committee appear more approachable she gave personal details about some of the members, including that one had hurt her foot and was off work. When there were complaints she immediately removed the information. Nonetheless criminal proceedings were commenced and she was fined 4,000.00 Swedish Kroner.

[60] *Procureur general pour le Procureur de la République de Villefranche sur Saône c. Roger G.*, Septième Chambre de la Cour d'Appel de Lyon, E.R. 390/03, 25 février 2004. The defendant maintained a web site critical of the Church of Scientology. As part of his commentary he posted personal information about an individual. There was a complaint, and he was fined 450 Euros for failing to send a notification to the Commission Nationale de l'Informatique et Libertés, also known as the "CNIL", the French data protection authority.

[61] OECD, *Report on the Cross-Border Enforcement of Privacy Laws* (Paris: OECD, 2006) available on-line at http://www.oecd.org/dataoecd/17/43/37558845.pdf .

[62] *Supra* note 22.

[63] Information Commissioner's Office, Press Release: Information Commissioner exposes league table of media's trade in personal information, released December 14, 2006 and available at http://www.ico.gov.uk/upload/documents/pressreleases/2006/what_price_privacy_2.pdf .

[64] C. 35.

[65] OUT-LAW News, "Dishonest data protection notices could earn jail time," January 17, 2007.

[66] See http://www.privacycommission.be/communiqu%E9s.htm .

[67] See http://www.edoeb.admin.ch/aktuell/index.html?lang=en .

[68] See http://www.datenschutzzentrum.de/presse/20060825-swift.htm .

[69] See http://ec.europa/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_23_11_06_en.pdf .

[70] *Ibid,* at p. 3.

[71] Busch, "From Safe Harbour to the Rough Sea? Privacy Disputes across the Atlantic," 3(4) *SCRIPT-ed* 305, June 2006, available on-line at: http://www.law.ed.ac.uk/ahrc/script-ed/vol3-4/busch.asp .

[72] See http://www.cnil.fr/index.php?id=2104&news[uid]=381&cHash=20ea8ddf3c .