PROTECTING TRANSBORDER DATA FLOWS: A PRIVACY MODEL FOR THE 21ST CENTURY*

*Piero Iannuzzi***

I.0 INTRODUCTION

> That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.[1]

With the advent of new information technologies, it has never been more important to "define anew" the meaning of the right to privacy. A century ago, the two Harvard scholars who are quoted above were preoccupied with the transgressions of privacy with regard to the unauthorized publication in newspapers of a person's likeness and the common law remedy available to the victim of the unlawful reproduction.[2] The dissemination of such materials pales in comparison to the capacity that modern society has to disseminate information. Given this fact, to what extent does the above definition suit the privacy needs of the 21st century? Does the "right to be let alone"[3] provide adequate privacy protection in the information age or do we need a new privacy model for the 21st century?

In addition, and more importantly for the purposes of this article, flows of information in modern society occur instantaneously and cross the borders of many states and jurisdictions. The "global village" in which we live has forced us to deal with the problem of transborder data flows (TBDFs) by providing privacy protection to digital information. Computers have caused Warren and Brandeis's prediction that "what is whispered in the closet shall be proclaimed from the house-tops"[4] to ring true.

This article studies how privacy can be protected in multiple jurisdictions given the international nature of modern governments, organizations, and businesses and their capacity to exchange information through computer technology and the Internet. More specifically, it looks at the protection of personal information as it is transacted in the private sector from one country to another thus creating TBDFs.

In order to do this we must examine information privacy in the Internet age and modern legislative and regulatory schemes designed to protect it, particularly in the context of TBDFs. Individual states have enacted statutes that protect, at varying levels, the information privacy of their nationals. These disparate levels of protection

* Submission to the Editor, May 3, 2001.

 The author has chosen to retain the original language of many quotations used in the article. Readers needing assistance with these quotations may contact the author at iannuzzi@canada.com.

have meant, however, that TBDFs have compromised certain national privacy principles. To eliminate these differences, national statutes must be harmonized so that personal information will be equally protected in all countries where such harmonization has occurred. Where such harmonization is not possible, the law must be flexible enough to allow alternative arrangements that protect privacy, including individual contracts and sectoral "privacy codes" or "codes of conduct."

We will examine these two alternative or supplemental methods of protecting information privacy in the context of TBDFs and explain how certain industries and commercial associations customize them to suit their particular needs. We will posit that the whole of these measures, legislative and non-legislative, constitutes a "privacy model for the 21st century," designed to regulate TBDFs and protect personal information privacy.

In shaping our privacy model, we will divide this article into five parts. First, we will propose a modern definition of privacy that highlights individual control of personal information. Second, we will describe the Organisation for Economic Co-operation and Development (OECD) guidelines and European instruments that provided an early framework for TBDF privacy protection. Third, we will examine methods employed by various national statutes to protect data both within their borders and TBDFs. The discrepancies present from one legislative scheme to another will be illustrated using the examples of the European Union, the United States, Canada, and Quebec. Fourth, we will discuss the above-mentioned non-legislative methods, including the extent to which they can provide adequate privacy protection. Finally, we will put forward our privacy model for the 21st century designed to promote data protection and free-flowing exchanges of information, thus striking a balance between the rights of the individual to protect personal information and the commercial and organizational needs of businesses and organizations to exchange information.

2.0 DEFINITION AND SCOPE OF PRIVACY

The notion of the "right to be let alone" posited by Warren and Brandeis is a definition of privacy that is clearly insufficient in the computer age. Indeed, the advent of e-mail, the World Wide Web, and the Internet only compound the need for the protection of data. More specifically, computer technology in the 21st century allows for the dissemination of information in an unprecedented manner. Privacy issues and privacy protection have gone far beyond the original more limited concept of the "right to be let alone" aimed at protecting personal property. Computer data must be conceptualized as information and, therefore, a modern interpretation of the "right to be let alone" would clearly "[be] protective of more than one's right to peaceful enjoyment of one's property."[5]

As a result, we must widen the definition and scope of privacy to incorporate concepts of control over one's personal information. The definition proposed by Alan Westin, a leading privacy scholar, puts the information and control elements at its core: "Privacy is the claim of individuals, groups, or institutions to determine for

themselves when, how, and to what extent information about them is communicated to others."[6]

Westin's definition is flexible enough to be adapted to the multitude of situations present in the computer age yet maintains the normative elements of individual control of information necessary for its effective application. This fluidity is particularly well suited for the information age since "la vie privée gagne à être fluide en ce que cela permet d'y incorporer des situations nouvelles que ne saurait envisagé la 'meilleure' des définitions."[7] Hence, Westin offers a good working definition that can be used to circumscribe data protection legislation. Let us now examine how TBDFs are protected.

3.0 HARMONIZATION: A FRAMEWORK FOR TBDF PROTECTION

3.1 The "Basic Rules" of Data Protection

> As transborder flows of data (including personal data) contribute to economic and social development, international moves towards harmonization have focused on the removal of unintended or unexpected impediments arising from differing regulatory machinery.[8] The adoption at an international level of agreed principles might help to promote harmonization or standardization of laws.[9]

Justice Kirby's words underline the fact that the harmonization of national laws can promote economic and social development and cooperation. It is no coincidence that the OECD was, from the outset, a key player in the harmonization debate given the keen interest it had in the elaboration and promotion of a standard privacy policy. The question of how to harmonize the privacy laws of very disparate countries, however, remained whole. The need to identify common ground on privacy issues would be the first step in influencing the development of national data protection legislation. After much thought and debate within the OECD[10] and the Council of Europe,[11] a general consensus was established that finally led to the elaboration of a "golden rule" and the setting down of "basic principles" on this issue.

The "golden rule" is simply the idea that, in order for there to be adequate protection of privacy, the individual would have the right to access and control personal data.[12] From this principle derive the complementary "basic rules" of data privacy protection. We will briefly identify and explain the 10 rules around which all effective modern privacy legislation is constructed. These rules constitute a framework for data protection and are the following:

1. *The Social Justification Principle*; elaborated to ensure that the collection of data occurs for purposes and uses which are socially acceptable.

2. *The Collection Limitation Principle*; needed to circumscribe the amount of data collected.

3. *The Information Quality Principle*; guarantees that data is accurate, complete and up to date.

4. *The Purpose Specification Principle*; limits the use of data to the specific purpose for which the data subject consented.

5. *The Disclosure Limitation Principle*; consent remains the cornerstone of any disclosure of personal information, subject to specific legislative derogations or to the fact that the method of disclosure is a publicly known practice.

6. *The Security Safeguard Principle*; reasonable security measures should be employed by the data controller to protect data.

7. *The Openness Principle*; a means of identifying the data controller must be available and the controller must reveal the purpose for which he is using the data.

8. *The Time Limitation Principle*; once the data has been used for a specific purpose, it must be destroyed.

9. *The Accountability Principle*; the data controller must be identified or identifiable and legally accountable, making legal recourse possible.

10. *The Individual Participation Principle*; known as the "golden rule" (discussed above) whereby the data subject participates in controlling the personal information being used by others.[13]

3.2 First Generation Legislation

The above principles formed the basis of the OECD Privacy Guidelines of 1980[14] and of the European Convention of 1981.[15] The two regulatory instruments constitute the first generation of multijurisdictional legislation dealing with data protection and offered a framework for harmonization of national laws. With regard to TBDFs, these instruments introduced the notion of "equivalent protection."

In art. 17 of the OECD Privacy Guidelines and in art. 12 of the European Convention of 1981, the expression is used to signify that "un pays ne s'opposera pas à la transmission de données à caractère personnel vers un pays tiers pour autant que ce dernier assure une protection aux données personnelles qui équivaut en substance à celle existant dans le pays exportateur."[16] The challenge in elaborating balanced data protection laws lies essentially in reconciling "concepts of privacy with the free flow of data."[17]

There exist two fundamental differences between the two above-mentioned instruments. The most important one is that the European Convention is binding on its members, whereas the OECD Privacy Guidelines are not.[18] The second is a corollary to the first. The OECD Privacy Guidelines permit each member state to choose the method of implementation, be it by statute or through self-regulation. The use of the word "should"[19] proves that legislation need not be implemented to conform to the Guidelines and thus a member state may simply urge industry to adopt voluntary codes of conduct.

The opposite is true of the European Convention. While not altogether prohibiting self-regulation, it does not advocate this method of implementation to be "le véhicule

exclusif de régulation interne du droit de la protection des données personnelles. L'autoréglementation apparaît alors comme un mode de régulation complémentaire à une action étatique."[20] As such, the preferred method of privacy protection is through legislation with self-regulation as a complementary instrument.

However, irrespective of the method of implementation of the privacy policy, failure to harmonize data protection laws would create imbalances within states, as different levels of protection would be present within the European Community. In fact, the European Commission harboured fears that trade between its member states would suffer if equivalent protection laws were not passed. Given that certain states had failed to pass legislation in the late 1980s, the "Commission of the European Community, concerned that data commissioners might block data transfers between countries and thus hinder the development of a single European common market, decided to act."[21]

3.3 Second Generation Legislation

This action that the European Commission took came in the form of second generation legislation, known as the European Union Data Protection Directive.[22] Chapters IV and V of the EU Directive deal with TBDFs, including harmonization principles, cases where derogations are admissible, and codes of conduct. This second generation of legislation differs from the first in the following ways.

First, art. 25(1) of the EU Directive stipulates that TBDFs can occur only if the recipient country ensures an "adequate level of protection." It is not clear whether this expression has the same meaning and scope as "equivalent protection" found in the first-generation legislation.[23] Professor Blume attempts to define the expression by postulating, "in practice this means that third countries must have data protection legislation that covers both the public and the private sector—a condition that many countries fail to fulfill."[24]

As a consequence, the EU would follow a procedure whereby it will compile a list of countries that meet the "adequate protection" standard. For countries that do not meet the required protection levels, there will be the possibility to derogate from the principle found in art. 25. These derogations found in art. 26 deal primarily with "singular data exports" and encompass cases where the individual concerned has consented or when his best interest or the public interest justifies it.[25]

The possibility of using contracts to ensure that personal data transferred from one country to another receive "adequate protection" under the EU Directive is explicitly recognized by art. 26(2). These contractual agreements can palliate data protection deficiencies in national legislation and conform to the "adequate protection" requirement.[26]

The legislative scheme dealing with TBDFs is completed by art. 27, which stipulates that the EC Commission "encourages" businesses operating in the member states to draw up their own privacy codes of conduct. The objective is to establish rules that best suit specific sectors and to "generate a mutual understanding which

can sustain a tendency towards a broader international regulation."[27] Article 28 establishes a supervising authority that has wide powers designed to effectively implement the EU Directive. In short, "l'Europe est à l'heure des codes de conduite sectoriels nationaux et internationaux et de la réglementation obligatoire."[28]

Through this Directive, the EU has decided to apply further pressure on both EU and non-EU states to conform to its data protection standards. As a result, both professors Benyekhlef and Blume believe that the EU Directive has put pressure on the Canadian and American governments to adopt comprehensive federal data protection legislation in the private sector.[29] We will now examine the legislative schemes of both these countries and others and examine the effects of not having uniform legislation.

4.0 DEFINING EQUIVALENCY: THE PROBLEM OF UNIFORMITY

4.1 The European Approach

The lack of "equivalency" provisions in national data protection laws regulating TBDFs can have adverse effects on multinationals who wish to obtain personal information from one of their branches. One such example occurred in a 1989 case[30] between France, who had legislation pertaining to TBDFs,[31] and Italy who did not. The supervising authority in France, the Commission nationale de l'informatique et des libertés (CNIL), took this fact into account in rendering its decision.

The case involved the Fiat motor company and its desire to set up a computer system designed to transmit personal information across French borders. The CNIL concluded that it would not allow Fiat-France to transfer personal information about French managers through the computer system to Fiat headquarters in Turin, unless the head office "s'engage par voie contractuelle à respecter les principes fondamentaux en matière de gestion de l'information personnelle consacrés par la Loi française et la Convention européenne."[32] This obviously imposed an administrative and operational burden on the corporation since Fiat had to contractually conform to certain external principles in order to obtain information concerning its own French subsidiary!

The equivalency provision was the major driving force in ensuring that each member of the Council of Europe adopted legislation that is compatible with the standards and objectives laid out in the European Convention.[33] Hence, the European approach to equivalent data protection has been one of adopting national omnibus legislation that adheres both to the OECD Privacy Guidelines and the Council of Europe Convention.[34] Most national laws forbid data transfers to countries that do not have equivalent protection. As a consequence, European states incorporate this principle in their laws since it is a "precondition to the free flow of information."[35]

We can generally conclude that national data protection laws in Europe have a common foundation.[36] Professor Hondius summarizes the precepts of the laws in this manner:

> National data protection regimes, though differing from one country to another, share certain principle features. They apply to the storage, processing and dissemination (input, throughput, output) of information relating to identifiable persons. Their aim is to ensure that information is correct, kept up to date, relevant to the purpose, and used for legitimate ends. They impose duties and obligations on the data users and confer rights and remedies on the data subjects.[37]

4.2 The Approach of the United States

4.2.1 The Sectoral Approach

In the United States, electronic privacy in the private sector is protected by a federal law, the *Electronic Communications Privacy Act*.[38] The statute prohibits all persons and businesses from accessing data stored in a computer or from intercepting messages in transmission. In fact, s. 2511 states that "any person" who intercepts or attempts to intercept an electronic communication can have criminal or civil sanctions imposed on them. Nonetheless, in order to reconcile the privacy rights of the users on the online system with the rights of the system operator "the user agreement should specifically set the privacy agreed to by operator and user in light of the *Electronic Communications Privacy Act* (ECPA)."[39]

The ECPA has extended data protection in the private sector to all forms of digital communications and to the transmission and storage of messages on a computer system. One must, however, question the effectiveness of the ECPA since a contract may "grant users more expansive privacy rights than they are given by state or federal law, or it may cut back in those rights or *deny privacy altogether*."[40]

This means that the ECPA does not provide for a minimal level of protection, having great consequences on personal privacy. For example, although stored non-voice messages are protected under the Act, system operators may review them, provided that they do not disclose the information. As a result, messages left in someone's e-mail box or on bulletin boards would not be protected because they can be considered "stored" data.[41]

The U.S. model applies two different types of legislative schemes to protect privacy.[42] In the public sector, it has adopted omnibus-style legislation that strikes a balance between access to information[43] and the protection of privacy.[44] In the private sector, the sectoral approach prevails and specific legislation has been enacted for certain key sectors, such as credit reporting.[45]

Another example of legislation applicable to particular sectors is the *Children's Online Privacy Protection Act*[46] also known as COPPA. The Federal Trade Commission has now implemented COPPA, which was signed into law in 1998 and came into force on April 21, 2000. One significant change brought about by COPPA is that it applies to commercial Web sites and online services directed to, or that knowingly collect information from, children under the age of 13. As a result, the Web sites in question must obtain "verifiable parental consent"[47] under s. 9 of COPPA before they may collect and use private data on children.

We can extrapolate from this model that, when transborder transfers of personal information occur, the data subject and data user must be aware that the "general approach [of the U.S.] grants the individuals specific rights that are connected to more general rights to privacy, including common law, statutory law, and constitutional rights, and that [they] extend to both the public sector and the private sector."[48] However, only the foreign data subjects can invoke the statutory right with certainty since the constitutional right is not extended to foreigners.[49] In this respect we have illustrated why general legislation in the field of electronic communications[50] is largely ineffective given the possibility to deny privacy altogether through contracts.[51] It is also unclear whether a breach of information privacy is considered a common law tort.[52]

4.2.2 Safe Harbor Privacy Principles and Self-Regulation

In order to comply with the "adequacy standard" required by the EU, the United States has adopted a self-regulatory model based largely on a Department of Commerce "Frequently Asked Questions on Self-Certification" document of July 21, 2000 that establishes "principles."[53] These "principles" are designed to provide a safe harbour for American companies when dealing with the EU. According to the Department of Commerce, the safe harbor privacy principles "are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of 'adequacy' it creates."[54]

It is important to point out that adherence to the safe harbor privacy principles is voluntary and that there are many ways to qualify for safe harbor. This self-regulatory scheme provides a minimum of personal data protection and failure to comply is actionable only if the act is "unfair or deceptive." In sum, the safe harbor privacy principles may be used only for the limited purpose of complying with the EU Directive on TBDFs and therefore "cannot be used as a substitute for national provisions implementing the Directive that apply to the processing of personal data in Member states."[55]

4.3 The Canadian Approach

4.3.1 The Canadian Standards Association and Self-Regulation

In the early 1990s, the Canadian government adhered to the OECD Privacy Guidelines by establishing similar guidelines set out in the Canadian Standards Association (CSA) Model Code for the Protection of Personal Information[56] under the auspices of the CSA. The CSA Model Code not only sets standards for the way organizations collect, use, disclose, and protect personal information but it also sets forth the right of individuals to have access to personal information about themselves and, if necessary, to have the information corrected. Organizations may use the CSA Model Code as a basis for developing sector-specific codes. In fact, the CSA Model Code was approved and published by the Standards Council of Canada as a National Standard in 1996.

The policy decision of the Canadian government at the time, however, was not to adopt omnibus-style legislation aimed at conforming to the OECD Privacy Guidelines. In the private sector, the Canadian approach was instead to encourage enterprises to adopt privacy codes based on the CSA Model Code and the OECD Privacy Guidelines. This sectoral approach is, moreover, confirmed by the presence of legislation in certain key sectors aimed at regulating the storage of data.[57]

The obligations in the *Bank Act*, for example, extend only to the conservation of a register. This does not prevent banks from prohibiting TBDFs on the basis that the information privacy of Canadians would be threatened abroad. Therefore, the *lacunae* in the legislative scheme is that s. 157 "se limite à exiger le maintien continue au Canada des livres et registres visés, mais n'empêche nullement l'exportation pour fins de traitement ou le stockage à l'étranger d'une copie de ceux-ci."[58]

The example of the *Bank Act* is typical of the shortcomings of Canadian data protection legislation in the private sector. It certainly does not meet the requirements of the European legislation because, as we have seen above, there is no authority granted to prevent TBDFs from occurring if privacy is not protected.[59] To compound the problem, although codes of conduct, which respect the OECD Privacy Guidelines, have been elaborated,[60] the nature of these private codes is that they are declarations of principle and are not enforceable.[61]

The *Privacy Act*[62] and the *Access to Information Act*[63] are omnibus statutes, but apply only to government activity. The major problem with Canadian legislation before the enactment of the *Personal Information Protection and Electronic Documents Act*[64] in the year 2000 was that it applied only to the public sector—that is, an invasion of privacy occurs only as a result of the government's[65] obtaining information without an individual's consent and thus illegally.

This phenomenon coupled with the fact that, except for Quebec,[66] all other provincial governments who have enacted privacy-related legislation have also applied it solely to the public sector leaves certain companies in a legislative vacuum. In other words, companies who were incorporated in provinces other than Quebec and companies that fell under federal jurisdiction, whether or not based in Quebec, were not subject to omnibus data protection laws. This prompted the Privacy Commissioner in 1994 to call for an end to "piecemeal legislation" and to recommend a "national privacy legislation to establish [data protection] principles and [a privacy] framework for both businesses and government."[67]

The same report does point to potential constitutional problems linked to the separation of powers that may impede any attempt to harmonize legislation.[68] However, any neglect to provide equivalent privacy protection mechanisms within the Canadian federation would lead to the quixotic situation wherein personal information privacy in Quebec would be better protected if a company transacted with the EU than with its neighbouring provinces!

In addition, information from companies that do not fall within the jurisdiction of the Quebec law could be prevented from entering the EU because it does not meet the

equivalency requirement. Hence, there was a pressing need for either further federal sectoral legislation that conforms to the equivalency principle or an extension of the *Privacy Act* to the private sectors of federal jurisdiction. The failure to do so would have had adverse economic effects on trade between Canada and the EU.

An illustration of how hindering information flow could obstruct trade was brought to the forefront by Canada's former privacy commissioner, Bruce Phillips, when he warned that "[w]ithout comparable data protection laws in Canada's private sector, European countries may no longer allow companies to transfer their citizen's information to Canada. In effect, European data protection laws could become a non-tariff barrier, seriously hampering Canadian firms in their dealings with what promises to be one of the strongest trading blocs in the world."[69]

Notwithstanding this apparent necessity for comprehensive legislation, companies and associations were opposed to the Quebec law. They contended that they were already over-regulated.[70] Further regulation, they argued, would have a negative impact on their businesses.[71] Moreover, the non-interventionist approach they espoused would in no way affect individual privacy because, through self-regulation, adequate protection already existed.[72] However, the government of Quebec, which adopted omnibus-style legislation in 1993, did not adopt this position.

The federal government also agreed to intervene and decided to bring forth omnibus-style privacy legislation applicable to the private sector as part of "Canada's overall strategy on electronic commerce" according to Industry Minister John Manley.[73] This led Parliament to enact the *Personal Information Protection and Electronic Documents Act*.[74]

4.3.2 Omnibus Private Sector Legislation

The *Personal Information Protection and Electronic Documents Act* came into force on January 1, 2001. The Act marks a watershed in Canadian privacy law legislation because it is the first piece of federal omnibus-style legislation that applies to the private sector and to personal information. The legislative scheme adopted palliates three *lacunae* found in the sectoral and self-regulatory models. First, the Act has a broad application and regulates many sectors and industries that were previously only subordinated to their own voluntary privacy codes. Second, it entrenches the principles set out in the CSA Model Code and the OECD Privacy Guidelines in legislation—as such, the failure to comply with these principles is now enforceable. Third, it grants the privacy commissioner the powers and duties to investigate, apply, and enforce the law.

In terms of the scope and application of the Act to personal information, part I of the Act "will initially apply to organizations in the federally regulated private sector, including telecommunications, broadcasting, banking, and interprovincial transportation."[75]

The application of the Act will have its full effect three years after its coming into force. On January 1, 2004, s. 4 stipulates that the Act "will apply more broadly

to all personal information collected, used, or disclosed in the course of commercial activities, as well as to inter-provincial and international flows of personal information in the course of commercial activities generally."[76] Some authors perceive this delay in its full application to most Canadian businesses as a weakness because the Act "will not have widespread impact on Canadian Internet use until at least 2004."[77]

Second, schedule I of the Act enumerates and gives legal effect to the "basic principles" found in the OECD Privacy Guidelines and later adopted by the CSA Model Code. In fact, in the words of Professor Michael Geist:

> The heart of the legislation is the Canadian Standards Association Model Code for the Protection of Personal Information. The subject of intense negotiation between consumer groups, and government in the early and mid-1990s, the Code represents a compromise between the need to protect individual privacy and the desire of organizations to collect personal data for marketing and other commercial purposes. This compromise remains intact in the new legislation, and is reflected in its purpose clause, which explicitly refers to the balance between the competing interests of individuals and business.[78]

The "Purpose" clause found in s. 3 recognizes the need, in an era in which technology increasingly facilitates the dissemination of information, for "rules to govern the collection, use and disclosure of personal information." This policy statement coupled with the legal effect given to the principles of the CSA Model Code found in schedule I of the Act grant wider powers to individuals to protect their personal information, and more particularly, ensure enforceability of the rules and principles governing the Act.

Finally, division 2 of the Act outlines the remedies available under part I and establishes the privacy commissioner as the watchdog for the Act. According to s. 11 of the Act, an individual "may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or for not following a recommendation set out in Schedule I." In addition, ss. 12 and 13 grant the privacy commissioner powers and duties to investigate complaints. The complainant may apply to the Federal Court for a remedy if the commissioner's report establishes violations of specific provisions of the Act.[79]

The enactment of the *Personal Information Protection and Electronic Documents Act* was long overdue and yet its full application as discussed will lag behind Internet growth. Notwithstanding this fact, the Act is necessary in the Internet era given the *lacunae* found in the self-regulatory model, notably the enforceability of the principles. In his conclusion to a paper presented to Industry Canada on privacy and personal information, Rick Shields emphasized the need for legislation protecting personal information in the digital age:

> [T]his paper has only served to fortify our belief that technological advances have fundamentally altered the parameters of "private" life; both government and business now possess the means to compile and analyze vast amounts of data derived from our individual public interactions. Left unregulated, this ever developing technological proficiency could run roughshod over our conventional concepts of privacy.[80]

He concludes by illustrating the need to strike a balance in this delicate public policy debate:

> The challenge, therefore, will be to develop reasonable rules to frame the private sector's dealings with third party personal information. In doing so, federal authorities will need to avoid unduly impeding both the public's ability to oversee government operations and the business sector's ability to carry on business in an efficient manner. If they can master this delicate balancing act, the result should benefit all Canadians.[81]

We can conclude that the *Personal Information Protection and Electronic Documents Act* does strike a balance between the varying competing interests who fashioned the original CSA Model Code. Of course, the Act does have certain *lacunae*, notably with regard to its application period and with the exceptions to the CSA Model Code. However, the enforceability of the principles found in the CSA Model Code and the powers and duties conferred on the privacy commissioner represent important steps forward in protecting personal privacy and in establishing recourses to ensure that the principles found in the Act are adhered to.

Finally, the Act does not apply to Quebec given that omnibus private sector legislation similar to the *Personal Information Protection and Electronic Documents Act* already exists in that jurisdiction. Let us now turn to the case of Quebec and examine the legislative scheme adopted by the Quebec government.

4.4 The Case of Quebec: Adopting Comprehensive Private Sector Legislation

In 1993, the province of Quebec was the first jurisdiction in North America to enact a statute specifically intended to protect data in the private sector.[82] The *Personal Information Act* complements the rights conferred by arts. 35 to 40 of the *Civil Code of Quebec*[83] and the privacy protection provided for in arts. 4 and 5 of the *Charte des droits et libertés du Québec*.[84]

A study by the Groupe de recherche en informatique et droit (GRID) shows that over 80 percent of TBDFs in the private sector in Quebec occur within multinational corporations.[85] Furthermore, the seminal study on the subject recommended to the Quebec government to conform to the OECD Privacy Guidelines.[86] Given the growing importance of TBDFs in the information age, the *Personal Information Act* provides a legal framework for their protection in the form of omnibus legislation.[87] As such, it governs the relationship with regard to data transfers between Quebec and foreign businesses relative to TBDFs. It had as a particular goal to conform to the EU Directive that could have excluded Quebec from doing business with Europe. This is confirmed by Kyer and Shea when they affirm that "[t]he *Personal Information Act* was clearly drafted with the view to providing 'adequate' protection as the term was used in the EC Directive and thereby facilitate the transfer of data from EC Member States to Quebec."[88]

In attempting to conform with the EU Directive, art. 17 of the *Personal Information Act* stipulates that any person "carrying on an enterprise in Quebec"[89] and who

communicates personal information about a Quebec resident to someone outside the province must take "all reasonable steps to ensure" that first, the consent of the individual has been obtained, subject to the exceptions granted for in arts. 18 and 23 and, second, the individual is made aware that he or she can refuse that any information be communicated to a third party and that he or she be given the option to remove his or her name from the nominative list.[90]

The legislative scheme recognizes principles of consent and control over personal information that are central to the protection of personal information privacy. These are the precise goals of the original international instruments that regulated TBDFs and thus "the law in Quebec, as it presently stands, guarantees, it would appear, that companies located in Quebec which wish to obtain information from EC Member States will encounter few problems."[91]

The Act, however, was not shielded from all criticism. It has been said that art. 17 fell short of granting Quebeckers the data protection offered by the EU Directive. In fact, the article does not prohibit the exportation of data to jurisdictions that do not offer "adequate protection" or the importation of data that does not meet the standards of the *Personal Information Act*.[92] Therefore, the protection offered by the Act is limited to the territory of Quebec. Only data imported into Quebec would be protected to the extent provided for in the statute.[93]

With regard to information that is being exported, the protection provided by art. 17 would need to be supplemented by non-legislative means. Professor Benyekhlef contends that the obligation to take "reasonable steps to ensure" could be met by the signing of a contract. The interpretation of the intent of the statute necessarily leads to the conclusion that these alternative methods would not only be admissible, but also encouraged in order for the law to be respected. It would nonetheless be difficult to control the actions of the data-importing business given the limited scope of the legislation.[94]

We agree that the *Personal Information Act* could have regulated TBDFs from Quebec to other jurisdictions more carefully. It seems that the primary concern was to comply with the European standards in order not to hinder trade. The net effect is that the *Personal Information Act* in matters of TBDFs protects foreign data coming into Quebec, but fails to guarantee the same protection for Quebec data travelling to other countries. We can conclude that the protection of personal information for Quebeckers is not absolute. However, the legislative scheme is set up in a manner that protects Quebec companies since if "l'entreprise québécoise a déployé tous les *moyens raisonnables*, notamment par la conclusion d'un contrat, on voit difficilement en quoi elle pourrait être tenue responsable d'un manquement de son cocontractant."[95]

In this section we have examined countries and jurisdictions whose legal systems derive both from the common law and the civil law traditions. We can generally conclude that the legislative scheme adopted by a particular jurisdiction directly depends on its legal regime. For example, Europe has opted for comprehensive regulation and strong institutional implementation of data protection, while

the United States and many Pacific Rim countries insist on free flow and adopt a sectoral approach with loose implementation.[96] This explains why Quebec, a civil law jurisdiction in North America, was the first jurisdiction to adopt European-style comprehensive data protection legislation in the private sector in 1993. Canadian legislation followed suit in 2000.

If true harmonization at an international level is to take place, these two legal traditions must be reconciled. It is likely that commercial considerations and the need for the free flow of information will eventually lead to a compromise position. Beyond these incentives, the incongruous legislative schemes employed by the American and European continents "reveal profound philosophical and political differences, reflected in legal cultures, about the fundamental values behind privacy and the role of the state in balancing individual freedoms with social control."[97] Meanwhile we must reconcile these values by finding alternative methods aimed at maintaining trade between important economic trading blocs.

5.0 NON-LEGISLATIVE OR "ALTERNATIVE" METHODS

5.1 Contractual Solutions to the Problem of Uniformity

In examining the role contracts play in protecting personal information, we must determine the extent to which they can provide "adequate protection." Hence, we are primarily concerned with legal situations wherein an enterprise domiciled in a jurisdiction that does not have "adequate" data protection legislation transacts with an enterprise that has ratified and respected the precepts of the EU Directive. If the enterprise receiving the information does not have "adequate protection," it has the possibility to resolve the conflict by signing a contract that has the effect of protecting the data in the transaction.[98]

The legal foundation of this option lies in art. 26(2) of the EU Directive, which permits the use of contracts as an alternative to legislation in the event that there is "sufficient proof that an adequate level of protection will be provided" to the singular data export. The supervising authority of the exporting jurisdiction would approve the contractual relationship therefore ensuring its effective application.[99]

The OECD, through its Committee for Information, Computer and Communications Policy has laid down the following principles aimed at providing a framework for privacy protection in transborder data flow contracts:

> A number of fundamental requirements for privacy contractual solutions, as well as additional relevant factors such as constraints or ancillary requirements and other privacy protection mechanisms, are considered important in promoting privacy compliance. Among these requirements are the substantive rules—the minimum level threshold being the Principles in the OECD Privacy Guidelines—which set out the parties' privacy obligations; a workable complaints and investigations process, and the provision of appropriate dispute resolution mechanisms. The substantive rules proposed in the report are intended to serve as a common reference for the discussion of

> and conditions for what is currently in use or under development, the experience to date, and possible further work in respect of contractual approaches.[100]

The parties to the TBDF contract need to ensure that there are substantive data protection rules that apply to the data transfer. These rules could be a reiteration of the principles of the OECD Privacy Guidelines or drawn from some other instrument that sets out equivalent principles. Contractual privacy solutions can achieve an appropriate level of privacy protection, such as that articulated within the OECD Privacy Guidelines. This objective is qualified by the balancing exercise inherent in the preamble or introductory statement in the OECD Privacy Guidelines that recognizes

> that although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;
>
> that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;
>
> that transborder flows of personal data contribute to economic and social development;
>
> that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows.[101]

The use of contracts is particularly suitable to govern TBDFs that occur between EU and non-EU countries. In the United States, for example, the approach is the so-called safe harbour contract, which complies with the EU Directive and protects TBDFs between the United States and the EU, but differs sharply from the harmonized legislative scheme used in EU member states. As a consequence, Professor Blume sees contracts as a short-term solution to these types of problems; he affirms "before an international regulation is fully developed contracts will sometimes be the only method to make singular data export possible."[102]

The contractual solution proposed can therefore aid trade between countries by proposing an alternative method of protecting personal information. If effective equivalency cannot be achieved through legislative means due to diverging legal traditions, the notion of "functional equivalency" may provide an attractive alternative. Functional equivalency can be achieved through the use of contracts or choice of law approaches that may be incorporated in contracts.[103]

This approach is justifiable and viable because it recognizes that data protection laws seek the respect of the finality of the law. Hence, notwithstanding the differences in methods used, the finality of the national laws is respected. We can therefore envision a system wherein "a state requires an equivalent level of protection abroad, but leaves open the means of ensuring that protection, be it by the law of the importing state, by contract, or by other means."[104]

The advantage of employing contracts is that they are effective legal remedies to the non-compliance of protection standards. The objective of the contract is to ensure a means of data protection that conforms to the exporter's law. The content

of the contract will therefore either include the data protection standards and procedures of the exporter's law or incorporate the law by annexing it to the contract or by referring to it.[105] As a result, the "equivalency" requisite of the exporter's law will be met and the enforceability of the contract will be ensured, providing recourses in damages, if any.

In the case that a contract does not refer to certain industry norms, the courts could nonetheless take them into account to aid them in interpreting a contract. To be more precise, the will of the parties in the contract could be interpreted in conformity with voluntary codes of conduct given that the industries designed them and the individuals implicitly accepted them when they signed the contract. These norms would be considered usage within the industry and could be enforceable.

In fact, the judicial interpretation of the effects of contracts between parties can elevate "les usages au rang de règle de droit, leur conférant ainsi certains attributs de règle de droit."[106] In Quebec, for example, the section in the Civil Code on the binding force and content of contracts includes art. 1434, which has this effect.[107] This principle of interpretation is also recognized in common law.[108]

Although the contract option seems palatable, several legal and jurisdictional problems remain. In order for a contract in international private law to be effective, it must contain a choice of law provision. The choice of law approach suffers from a few weaknesses linked to the lack of uniformity in national legislation coupled with the inherent mobility of computer data and thus TBDF. In addition, choice of law clauses can be used to circumvent a restrictive regulatory scheme by simply choosing the jurisdiction of the party with the least restrictive regulations. The countries with less stringent privacy rules are sometimes referred to as "data havens."

For instance, information may be generated in Italy, processed in France, and stored in the United States. Which country's law would apply in this situation? This example illustrates that the major problem with the choice of law approach is that "national laws may have different compliance requirements before any transmission of digitised personal data can take place."[109]

Another difficulty associated with this approach is linked to jurisdiction. A tribunal in one country may interpret the choice of law clause differently from a tribunal in another country. In fact, the international private law rules will differ depending on the jurisdiction chosen to interpret the clause.[110] Lack of clear rules can, therefore, lead to situations where a court will rule that it does not have jurisdiction to make a decision according to its international private law.[111]

Contractual solutions provide flexibility and are therefore an essential element of the "functional equivalency" we are attempting to implement. In addition, the jurisdictional problems we have imagined are not new to international private law. The need for uniformity remains our main concern and this can be achieved by drawing up a "model contract" based on the principles of the EU Directive[112] with the addition of the preamble from the OECD Privacy Guidelines. Ultimately, TBDFs will benefit from a "functional equivalency" approach that would satisfy the "adequate protection" requirement of the EU Directive.

5.2 Internal Voluntary "Codes of Conduct"

> Les deux caractéristiques qui nous semblent indispensables à la réussite de cette construction juridique d'auto-réglementation, c'est la participation des personnes et des entreprises interessées ("auto") et la force obligatoire des règles convenues et approuvées ("réglementation").[113]

This quote demonstrates the dual nature of the self-regulatory process. The first aspect (self) is the participation necessary by businesses in order to develop sector-specific codes that respond to the particular needs of a given industry. The second (regulatory) is the obligatory nature of the codes necessary to provide legal recourse to those whose privacy rights have been violated. In order to examine the effectiveness of voluntary codes of conduct in the private sector let us use as an example the Canadian Direct Marketing Association (CDMA) Guidelines:

1. Privacy considerations must be recognized specifically in the provision, use and regulation of the information system;
2. The network must be governed by a fair information code established in law;
3. Individuals should be able to control their own information, including what details are transmitted over the network. …
5. Service providers should not disclose information without the individuals' explicit consent and should explain their data collection practices to individuals;
6. Information about individual transactions must also be governed by the [information] code; that is the pattern of the transactions, not just the data in each individual transaction; …
8. There should be no charge to protect your privacy.
9. There should be an independent oversight body to monitor the system.[114]

These guidelines were designed to conform to the OECD Privacy Guidelines. For example, in recommendations (3) and (5) we recognize the notions of control and consent, respectively. These concepts are compatible with the "basic rules" we outlined above. However, they remain voluntary and are not enforceable. Therefore, the OECD Privacy Guidelines' ninth principle, accountability, is absent from the non-legislative scheme.

For the effective implementation of these information codes to become a reality, they must be "established in law" as recommendation (2) suggests. This could be accomplished by either annexing these codes to a statute or publishing them in the official gazette of the relevant jurisdiction thereby making them public and giving them the force of law. This method would hold the industries in question accountable for breaching their own codes and thus ensure effective application of the codes through legal recourse; "il s'agit d'obliger les entreprises, regroupées en secteur ou individuellement, à adopter un code de conduite qui, après approbation par la Commission, aurait force de loi."[115]

Let us examine an alternative. Is it feasible to achieve accountability through voluntary codes? In the case of contracts, as we have seen, the interpretation of usage can constitute an effective means of enforcing the contract. Can the elaboration of voluntary codes, therefore, constitute usage and thus be enforceable? In determining whether usage exists, a court may attribute to voluntary codes "un certain rôle comme révélateurs des usages généralement suivis."[116]

However, voluntary codes must be differentiated from usage. A voluntary norm must be notorious in order for it to be qualified as a usage. In addition, while a norm states a principle, a usage is formed by a series of repeated actions and commercial behaviour over time. Notwithstanding this distinction, the continued respect of self-imposed norms or commercial behaviour with regard to TBDFs will most likely elevate them to the level of a usage. Within this context, the legal effect of the continued use of voluntary norms may thus grant them a degree of enforceability. Although we advocate direct enforceability through legislative texts, it remains true "[q]ue les normes d'autoréglementation aient ou non été intégrés dans les textes législatifs ou contractuels, les tribunaux gardent la possibilité d'y référer lorsqu'ils ont à juger les comportements ou à interpréter les textes législatifs ou contractuels."[117] As such, the voluntary norms are considered an interpretative tool by judges.

There are different views on the effectiveness of voluntary codes. However, Professor Blume argues that the "data users" already have strong incentives to voluntarily comply with the rules of data protection. He contends that the incentives are tied into the image of the company, both internally with its employees and externally with its clients. Therefore, a legislative scheme, which recognizes that the control of personal data should rest with the data user, would best reflect the "reality" that privacy would nevertheless be protected according to the specific needs of each industry. For these reasons, Professor Blume concludes that self-regulation should be the "basic foundation of data protection."[118]

In contrast to this position, in an article where he comments on each section of the *Personal Information Act*,[119] René Laperrière argues that the business community has no incentives to go beyond what the law dictates. The statute grants a minimal level of protection, but the code of conduct is not enforceable, rendering its content legally meaningless. Therefore, in elaborating a code of conduct, there is no reason for a business to go beyond the stating of general, but ineffective principles. Professor Laperrière recommends that a commission should oversee these codes in order to add a "public" element to the process. Otherwise, self-regulation would be "laissé à l'initiative privée sans encadrement public."[120] He is, therefore, more critical of privacy codes than Professor Blume, especially when the codes are not enforceable.

Professor Benyekhlef concurs with the assessment that "privacy codes" do not offer adequate protection and that legislation regulating private sector activity must therefore prevail. He posits: "[i]l nous semble clair, à la lumière des législations européennes existantes, de la Convention européenne et des travaux de la Commission, qu'il ne saurait être question de laisser le secteur privé complètement libre de ses actions en matière informationnelle. Une forme quelconque de régulation semble s'imposer."[121]

5.3 A Privacy Model for the 21st Century: Principles and Foundations

The globalization of data transfers and the impact that the Internet has had on data transfers and personal information privacy was summarized by the OECD's Committee for Information, Computer and Communications Policy: Working Party on Information Security and Privacy in the following manner:

> The advent of the global economy, and the increasing sophistication of information and telecommunications technologies, are resulting in the globalisation of international data transfers. International information systems are the basic infrastructure of a multinational company's operations in trading goods and services. More and more companies are moving data between countries. Organisations who have control over the collection and processing of personal data, have the means to reuse and transfer those data on an unprecedented scale. This can be high volume TBDF, such as in the form of databases, or multiple one-off collections from activities such as Web browsing on the Internet.[122]

This comment from the OECD underscores our basic premise that the Internet age has caused privacy protection legislation to evolve. In fact, modern privacy legislation in many jurisdictions has been passed to deal specifically with the flow of data and the increased capacity that modern society has to disseminate information. These factors are crucial in determining the scope and objectives of data protection policies and privacy legislation.

In addition, the political positioning and lobbying discussed above in the case of Canada before the enactment of Canadian omnibus legislation forces us to revert to this basic question: what is the appropriate balance between the social benefits of data protection and the commercial imperatives of freely using advanced technologies? The answer to this question will provide the foundation to our privacy model.

It is clear that the right to privacy is not absolute. In fact, when doing business with a credit card company, most people are aware that data on their transactional patterns are kept and may be used for other commercial purposes. However, they choose to continue doing business with a particular firm because the benefits of using the credit card outweigh the costs to their personal privacy.[123] This situation can be transposed in the international setting where the lack of harmonization could lead to impediments with international commercial transactions for consumers.

Therefore, in order to strike an appropriate balance between competing needs, we revert to the notion of "reasonable expectation of privacy."[124] This expression provides us with the framework necessary to define data protection rights. In fact, this notion already pervades most privacy legislation because the control over one's personal information is not absolute.

For example, although the *Personal Information Act* in Quebec is recognized as offering comprehensive privacy protection, it nonetheless allows for derogations. Articles 18 and 23 govern circumstances under which, respectively, no consent from the data subject is necessary in order to communicate information about him

or her to a third person and under which a nominative list may be used for commercial or philanthropic ends.[125] Similarly, the principles enunciated in art. 25 of the EU Directive are also subject to derogations found in art. 26.

6.0 CONCLUSION

Our primary concern in giving a more modern definition to "privacy" was to include the protection of information privacy. It is well established that the information that flows from computers is protected as information privacy. The protection of information privacy entails individual control over information about oneself and, therefore, consents to the use of the information. The basic principles that flow from these notions are internationally recognized and constituted the foundation of first-generation legislation within the OECD and the EC.

However, the intent of the OECD Privacy Guidelines and the European Convention were short-circuited by some states that did not implement national data protection laws conforming to the principle of "equivalent protection." The ineffectiveness of these international instruments arising from imbalances in national laws coupled with the trade problems they caused led to second-generation legislation.

The EU Directive recognized that a more flexible approach to TBDF protection was necessary to liberalize trade within the community and to achieve a single European market. Notwithstanding the preoccupation with trade, the protection of personal data was not forsaken. However, the right to privacy is not absolute and certain compromises were made as the equivalency provision was watered down.

It was acknowledged that the concept of "equivalent protection" was surpassed by the concept of "adequate protection" present in second-generation legislation. The latter expression has more flexible language and is therefore more conducive to private arrangements—for example, contracts or sectoral arrangements such as privacy "codes of conduct." First-generation legislation failed to recognize the importance of these complementary methods and should have encouraged the implementation of the international instruments through non-legislative means.

The survey of the legislative schemes of common law and civil law jurisdictions was indispensable to our study because it provided us with a comparative perspective of data protection legislation. Moreover, the nature of TBDFs dictates the study of multiple jurisdictions thereby giving us an overview of the various methods used to protect data. The analysis permits us to draw from different models the necessary tools to formulate our privacy model.

We can now elaborate our privacy model for the 21st century based on the need to reconcile the right to information privacy and the free flow of information. We justify this approach by pointing out that the OECD Privacy Guidelines had as an objective "de concilier ces deux principes antagonistes que sont le droit à la vie privée et la libre circulation des biens."[126] In the age of the globalization of trade and TBDFs, we must balance the commercial interests associated with obtaining information with the individual interests of protecting it.

The OECD Privacy Guidelines therefore represent a consensus on fundamental requirements and objectives for privacy protection and an appropriate balance between effective privacy protection and the free flow of information. However, the appropriate level of privacy protection can also be drawn from other national law or self-regulatory frameworks, based on the OECD Privacy Guidelines.

In order to reconcile the above principles our model is divided into two parts. The first part of the model recognizes the minimal level of protection that TBDFs and personal privacy require. The criteria ensuring this minimal protection will be consent and control over personal information. The second part provides tools, which allow the derogation from certain data protection rules in order to accommodate commercial needs, without compromising the minimal level of protection. Our challenge will be to guarantee that these tools—contracts and codes of conduct—respect the consent and control criteria.

Agreement on the general principles identified by Justice Kirby constitutes a *sine qua non* condition to the first part of our privacy model. Of course, we have seen that these are generally accepted. However, countries such as the United States did not extend the protection of these principles to the private sector through omnibus legislation, but enacted statutes that protected specific groups in a piecemeal manner. In this respect, an omnibus private sector law has the advantage of applying indistinctly to all sectors that deal with information technology. This approach was recently embraced by Canada with the passage of the *Personal Information Protection and Electronic Documents Act*. The "golden rule" that every individual must have access to and must control personal information is now generally accepted in the western world.

The second part of our model recognizes that international trade is based on the concept that all companies that transact with each other do so on a "level playing field." Similarly, data protection laws must apply equally to all businesses irrespective of the country or jurisdiction they operate in. In this manner, there will be no commercial disadvantage to obeying data protection laws. Hence, it is imperative that "equivalency" be achieved.

That is why we favour a more flexible concept like "adequate protection," found in the recent EU Directive. We have already shown that privacy is not absolute and we must therefore allow for a data protection model that puts contracts and codes of conduct on the same level as legislation. This would allow for a "functional equivalency" that respects the finality of legislation while not regulating the means used to reach that finality.

We have also outlined certain problems inherent with international contracts and voluntary codes of conduct, including the possibility of choosing jurisdictions seen as "data havens" in contracts and the uncertain enforceability of voluntary codes. One possible solution to the jurisdictional problem would be to prohibit the use of choice of law clauses and force the parties to choose the law of the exporter's jurisdiction. This would at least eliminate the arbitrary nature of allowing parties to choose the jurisdiction with the least stringent data protection law. Finally, if we are

to ensure accountability, we recommend the use of contracts coupled with sector-specific "privacy codes" that have the force of law.

In our privacy model, the possibility to contract and to elaborate "privacy codes" is not an alternative to legislation, but is meant to complement it. This gives individuals as well as data controllers the option to tailor their privacy needs to their activity or industry.

In conclusion, a "functional equivalency" approach will not only increase international trade by decreasing barriers associated with TBDFs, but will also recognize and respect the different legal traditions and business practices of all countries. The combination of the respect of basic privacy principles with flexible ways to respect them will lead to a privacy model that encourages TBDFs and ensures "a reasonable expectation of privacy."

ENDNOTES

1 Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" (1890-91), vol. IV *Harvard Law Review* 193, at 193.

2 In violation of copyright laws.

3 Warren and Brandeis, *supra* note 1, at 193.

4 *Ibid.*, at 195.

5 H. Patrick Glenn, "The Right to Privacy in Quebec Law," in Dale Gibson, *Aspects of Privacy Law* (Toronto: Butterworths, 1980), at 50; Original French version: Glenn, "Le droit au respect de la vie privée" (1979), 39 *R. du B.* 879, at 888. Constitutionally, the criteria of "reasonable expectation of privacy" has been recognized both in Canada (*Hunter v. Southam, Inc.*, [1984] 2 S.C.R. 145 and *R. v. Dyment*, [1988] 2 S.C.R. 417) and in the United States (*Katz v. United States*, 389 U.S. 347 (1967)).

6 Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), at 7.

7 Karim Benyekhlef, *La protection de la vie privée dans les échanges internationaux d'informations* (Montreal: Les Éditions Themis, 1992), at 55.

8 See the Fiat example in section 4.0 of this article.

9 Hon. Justice Michael D. Kirby, "Transborder Data Flows and the 'Basic Rules' of Data Privacy" (1980), 16 *Stanford Journal of International Law* 27, at 28.

10 OECD Expert Group on Transborder Data Barriers and the Protection of Privacy.

11 Council of Europe, Committee of Experts on Data Protection, Draft Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (May 1979).

12 Kirby, *supra* note 9, at 29.

13 *Ibid.*, at 46-64.

[14] Organisation for Economic Co-operation and Development Guidelines on the protection of privacy and transborder flows of personal data—Paris; Organisation for Economic Co-operation and Development—Washington, D.C.; OECD Publications and Information Center, 1981. See also OECD, "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data," *Transnational Data Report*, vol. 4, no. 1, January 1981 (hereinafter "OECD Privacy Guidelines"). On line at http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

[15] European Convention, 1981. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (hereinafter "European Convention").

[16] Karim Benyekhlef, "Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commission des Communautés européennes," (1991-92), 2 *Media and Communications L.R.* 149, at 177.

[17] R.K.A. Becker, "Transborder Data Flows: Personal Data" (1981), 22 *Harvard International L.J.* 241.

[18] H. Patrick, "Privacy Restrictions on Transnational Data Flows: A Comparison of the Council of Europe Draft Convention and OECD Guidelines" (1980-81), 21 *Jurimetrics Journal* 405, at 419. See also Peter Blume, "An EEC Policy for Data Protection," (1992), vol. XI *Computer Law Journal* 399.

[19] Article 19, OECD Privacy Guidelines.

[20] Benyekhlef, *supra* note 16, at 185.

[21] Privacy and the Canadian Information Highway: Building Canada's Information and Communication Infrastructure (October 1994). Communications Development and Planning Branch, Spectrum, Information Technologies and Telecommunications Sector, Industry Canada, section 4, "How have other countries protected privacy?" http://debra.dgbt.doc.ca/isc/isc.html.

[22] 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 the free movement of such data, *Official Journal of the European Communities*, no. L. 281 (November 23, 1995), at 31 (hereinafter EU Directive).

[23] Benyekhlef, *supra* note 16, at 194-95.

[24] Blume, *supra* note 18, at 418.

[25] Article 26, EU Directive.

[26] For further discussion see section 5.0 of this article.

[27] Blume, *supra* note 18, at 419-20.

[28] René Laperrière, "La protection des renseignements personnels dans le secteur privé et la loi québécoise de 1993," in René Côté and René Laperrière, eds. *La vie privée sous surveillance-la protection des renseignements personnels en droit québécois et comparé* (Cowansville: Les Éditions Yvon Blais, 1994), at 78.

[29] See Benyekhlef, *supra* note 16, at 206, and Blume, *supra* note 18, at 418-20.

[30] Fiat case (1989).

[31] Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[32] Benyekhlef, *supra* note 7, at 247.

[33] For an overview of Italian law, see Pietro Tamburrini, "Italy: Bill on Protection of Private Data" (October 1994), 2(10) *The International Computer Lawyer* 31. For Spain see Enrique Batalia, "New Personal Data Protection Law Proposed in Spain" (November 1991), 6(2) *International Computer Law Adviser* 17. The Japanese have also realized that it would be costly to be left out of the EU commercial loop. See Prof. Dr. Tsuyoshi Hiramatsu, "Japan Adopts Privacy Protection Act" (May 1989), 3(8) *International Computer Law Adviser* 17.

[34] René Laperrière, René Côté, and Georges Lebel, "The Transborder Data Flow of Personal Data from Canada: International and Comparative Law Issues" (1992), 32 *Jurimetrics Journal* 547, at 557. For a list of European countries that have implemented national legislation in conformity with EU Directive 95/45/EC, visit the Web site of the European Commission at http://europa.eu.int/comm/internalmarket/en/dataprot/law/impl.htm.

[35] *Ibid.*, at 558.

[36] For an overview of the German Act see K. Bohloff and A. Baumans, "Harmonising German Data Protection and the Council of Europe Convention" (1984), 12 *International Business Lawyer* 175. In the United Kingdom, see E.J. Howe, "Data Protection in the United Kingdom" (July–August 1987), 3(6) *Computer Law and Practice* 204.

[37] F.W. Hondius, "A Decade of International Data Protection" (1983), 30 *Netherlands International Law Review* 103, at 109-10, cited in Benyekhlef, *supra* note 16, at 173.

[38] 18 U.S.C.S. 2510 (1988); its predecessor was originally enacted to respond to the "wiretapping" activity surrounding the Watergate scandal.

[39] Lance Rose, *NETLAW-Your Rights in the Online World* (Berkeley, CA: Osborne McGraw Hill, 1995), at 185. For privacy legislation governing the telecommunications sector in Europe, see Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector at http://europa.eu.int.eur/ex/en/lif/dat/1997/en397L0066.html.

[40] *Ibid.*, at 177 (emphasis added).

[41] *Ibid.*, at 168.

[42] GRID, *L'identité piratée* (Montreal: SOQUIJ, 1986), at 122, tableau 13.

[43] *Freedom of Information Act*, 5 U.S.C. 552.

[44] *Privacy Act of 1974*, 5 U.S.C. 552a.

[45] *Fair Credit Reporting Act of 1970*, 15 U.S.C. 1681-81t.

[46] *Children's Online Privacy Protection Act*, 15 U.S.C. 6501. For more information go to http://www.ftc.opa/1999/9910/childfinal.htm.

[47] "Section 9 Verifiable Parental Consent.—The term "verifiable parental consent" means any reasonable effort (taking into consideration available technology), including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that a parent of a child receives notice of the operator's personal information collection, use, and disclosure practices, and authorizes the collection, use, and disclosure, as applicable, of personal information and the subsequent use of that information before that information is collected from the child."

[48] Laperrière, Côté, and Lebel, *supra* note 34, at 556.

[49] In *United States v. Verdugo-Urdiquez*, 110 S. Ct. 1056 (1990), the Supreme Court refused to extend the protection of the search and seizure (Fourth Amendment) to aliens.

[50] *Electronic Communications Privacy Act*, 18 U.S.C.S. 2510 (1988).

[51] According to BNA's Internet Law News (ILN)—12/6/00: Congress may pass Netlaw privacy legislation in its next session. Newsbytes reports that Congress will likely pass a Net privacy law. Privacy is a general public concern and both political parties would be inclined to assist in developing and implementing Internet privacy laws. http://www.newsbytes.com/news/00/159002.html.

[52] For a discussion of how the common law right to privacy first identified by Warren and Brandeis can now be extended to include informational privacy, see J. Graham, "Privacy, Computers, and Commercial Dissemination of Personal Information" (1987), *Texas L.R.* 1395.

[53] U.S. Department of Commerce, July 2000, http://www.ita.doc.gov/td/ecom/SHPRINCIPLESFINAL.htm.

[54] *Ibid.*

[55] *Ibid.*

[56] Model Code for the Protection of Personal Information, CAN/CSA-Q830-95; online on CSA Web site: http://www.csa.ca/english/home/index.htm.

[57] *Bank Act*, R.S.C. 1985, c. B-1, ss. 157(4)-(9).

[58] Benyekhlef, *supra* note 7, at 260.

[59] *Ibid*. ("[L]a nature du dispositif sectoriel canadien est bien en deça des exigences européennes.")

[60] See C.D.M.A. guidelines, in section 5.2 of this article. In September 1990, the Canadian Banker's Association also adopted such a code.

[61] Benyekhlef, *supra* note 7, at 261.

[62] *Privacy Act*, R.S.C. 1985, c. P-21.

[63] *Access to Information Act*, R.S.C. 1985, c. A-1.

64 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

65 The problem is compounded when one takes into account that there is no constitutionally protected right to privacy in the private sphere. In fact, the *Canadian Charter of Rights and Freedoms* applies only to the government. See: *R.W.S.D.U. v. Dolphin Delivery, Ltd.*, [1986] 2 S.C.R. 573.

66 See section 4.3 of this article, *infra*.

67 Privacy and the Canadian Information Highway, *supra* note 21, section 5, "Possible Approaches for Canada, Legislation and Regulation." For a bibliography on the Information Highway Advisory Council reports on the Web, visit http://info.ic.gc.ca/info-highway/final.report/eng/app3.html.

68 *Ibid.*

69 1990-91 Annual Report of the Privacy Commissioner, cited in Ian C. Kyer and Patrick E. Shea, "Data Protection Laws Come to Quebec" (August 1994), 2(8) *The International Computer Lawyer* at 20.

70 Laperrière, *supra* note 28, at 67.

71 *Ibid.*, at 66-67, "[T]rois d'entre elles [the associations] ont même déclaré que la loi les forcerait à fermer leurs portes."

72 See GRID, *supra* note 42, at 94 and Kyer and Shea, *supra* note 69, at 22. The GRID, however, strongly believed that private sector legislation had to be enacted and appropriately made it its first recommendation. See GRID, *supra* note 42, recommendation 1.1, at 273.

73 Industry Canada, E-Commerce Task Force: Building Trust in the Digital Economy, *Privacy: The protection of personal information*, December 1, 1998, http://e-com.ic.gc.ca/english/privacy/632d28.html.

74 *Supra* note 64 (hereinafter "the Act").

75 Michael Power, "Bill C-6: Federal Legislation in the Age of the Internet" (1999), 26(2) *Man. L.J.* 235, at 238.

76 *Ibid.* See also Michael A. Geist, *Internet Law in Canada* (North York: Captus Press, 2000), at 265.

77 Geist, *supra* note 76, at 253.

78 *Ibid.*

79 Section 14.

80 Rick Shields, "Publicly Available Personal Information and Canada's Personal Information Protection and Electronic Documents Act," presented to Industry Canada by McCarthy Tétrault, Ottawa, October 12, 2000, at 57, http://www.mccarthy.ca/en/whatsnew/wn-ann20.htm.

81 *Ibid.*

[82] *An Act respecting the Protection of Personal Information in the Private Sector*, R.S.Q. c. P-39.1 (hereinafter the *Personal Information Act*).

[83] *Ibid.*, s. 1.

[84] *Charte des droits et libertés du Québec*, L.R.Q., c. C-12.

[85] René Laperrière, René Côté, G. Lebel, P. Roy, and K. Benyekhlef, *Vie privée sans frontières. Les flux transfrontalières de renseignements personnels en provenance du Canada* (Ottawa: Ministère de la Justice, 1991).

[86] GRID, *supra* note 42, recommendation 4.3.4, at 304.

[87] *Personal Information Act*, s. 17.

[88] Kyer and Shea, *supra* note 69, at 22. See also: Côté and Laperrière, *supra* note 28, at 174, where it is asserted that the principle of equivalency "est destiné à devenir la règle en matière d'échanges internationaux de données."

[89] This expression now appears in art. 1525, para. 3 of the new Civil Code of Quebec, S.Q. 1991, c. C-64 and will most likely follow the same interpretation.

[90] The full text of s. 17 reads as follows: "Every person carrying on an enterprise in Quebec who communicates, outside Quebec, information relating to persons residing in Quebec or entrusts a person outside Quebec with the task of holding, using or communicating such information on his behalf must take all reasonable steps to ensure: (1) that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned, except in cases similar to those described in sections 18 and 23; (2) in the case of nominative lists, that the persons concerned have a valid opportunity to refuse that personal information concerning them be used for purposes of commercial or philanthropic prospection and, if need be, to have such information deleted from the list."

[91] Kyer and Shea, *supra* note 69, at 22.

[92] Laperrière, *supra* note 28, at 69-71.

[93] Karim Benyekhlef, "Les transactions dématérialisées sur les voies électroniques: Panorama des questions juridiques," in Danel Poulin, Pierre Trudel, and Ejan Mackay (dir.), *Les autoroutes électroniques—Usages, droit et promesses* (Cowansville: Les Éditions Yvon Blais, 1995), at 141.

[94] *Ibid.*

[95] *Ibid.*, at 142.

[96] Laperrière, Côté, and Lebel, *supra* note 35, at 567.

[97] *Ibid.*, at 566.

[98] These conflicts often occur when there is a transfer of information from EU to non-EU states. As we have seen in section 4.0 of this article, this is primarily due to differing legal traditions. The Fiat example, however, demonstrates that these problems can also occur within the EU.

99 See art. 28 of the EU Directive granting member states the power to establish such a public body.

100 OECD, Committee for Information, Computer and Communications Policy: Working Party on Information Security and Privacy: Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection on Global Networks, http://www.oecd.org/dsti/sti/it/secur/index.htm.

101 OECD Privacy Guidelines, *supra* note 14.

102 Blume, *supra* note 18, at 418.

103 Michael G. Epperson, "Contracts for Transnational Information Services: Securing Equivalency of Data Protection" (1981), 22 *Harvard International L.J.* 157.

104 *Ibid.*, at 164.

105 *Ibid.*, at 171.

106 Pierre Trudel, "Les effets juridiques de l'autoréglementation" (1988), 19 *R.D.U.S.* 247, at 274.

107 Section 1434 C.C.Q stipulates: "A contract validly formed binds the parties who have entered into it not only as to what they have expressed in it but also as to what is incidental to it according to its nature and in conformity with *usage*, equity or law."

108 Trudel, *supra* note 106, at 275.

109 Chris Hoyle, "Trans-border Data Flows: Many Barriers Stand in the Way for Users" (November-December 1992), 1(1) *The International Computer Lawyer* 14, at 19.

110 *Ibid.*, at 15.

111 In Quebec law, for example, the notion of "*forum non conveniens*" has been codified in s. 3135 of the Civil Code of Quebec. For further discussion of this doctrine, see: Ethel Groffier, *Précis de droit international privé québécois*, 4e éd. (Cowansville: Les Éditions Yvon Blais, 1990).

112 B.W. Napier, "Contractual Solutions to the Problem of Equivalent Data Protection in Transborder Data Flow" (September 1990), 4(12) *International Computer Law* Advisor, at 18.

113 Laperrière, *supra* note 28, at 78.

114 Enumerated and discussed at Web site: Brian Foran, Special Advisor to the Privacy Commissioner, "Privacy on the Information Highway: Myth or Reality?" Address to the Records Management Institute Annual General Meeting, Ottawa, June 21, 1995, http://info.ic.gc.ca/opengov/opc/pubs/950621bf.txt. In Canada, to visit the Voluntary Codes Research Forum Web site, go to http://strategis.ic.gc.ca/SSG/ca00973e.html. To subscribe to the online Voluntary Codes Research Forum, contact Kernaghan Webb, at webb.kernaghan@ic.gc.ca. For a hard copy of "Voluntary Codes: A Guide to Their Development and Use," contact Kernaghan Webb. For an online version, go to http://www.strategis.ic.gc.ca/SSG/ca00962e.html. For an online version of the Evaluative

Framework for Voluntary Codes, a summary of a symposium on Voluntary Codes, and executive summaries of research on voluntary codes, go to http://strategis.ic.gc.ca/SSG/ca00880e.html. In the United States, visit http://www.privacyalliance.org/.

115 Pauline Roy, "*La Loi sur la protection des renseignements personnels dans le secteur privé*, un acte de foi dans les vertus de l'auto-réglementation," in Côté and Laperrière, eds., *supra* note 28, at 111.

116 Trudel, *supra* note 106, at 277.

117 *Ibid.*, at 276.

118 Peter Blume, "How to Control Data Protection Rules" (March 1992), 6(6) *International ComputerLaw Adviser* 17, at 20.

119 René Laperrière, "La loi sur la protection des renseignements dans le secteur privé—Commentaire et guide d'interprétation," in Côté and Laperrière, eds., *supra* note 28, at 141.

120 *Ibid.*, at 240.

121 Benyekhlef, *supra* note 16, at 206.

122 OECD, Committee for Information, Computer and Communications Policy, *supra* note 100.

123 Privacy and the Canadian Information Highway, *supra* note 21, section 2, "Privacy Issues for the Information Highway."

124 Phrase used by the Supreme Court of Canada to delimitate the right to privacy conferred by s. 8 of the Charter in *Hunter v. Southam Inc.*, *supra* note 5.

125 For a commentary on these articles see: Côté and Laperrière, eds., *supra* note 28, at 177-88 and 195.

126 Benyekhlef, *supra* note 7, at 406.