Text and Context: Making Sense of Canada's New Personal Information Protection Legislation

*Teresa Scassa**

Les dispositions normatives concernant les renseignements personnels de la nouvelle Loi sur la protection des renseignements personnels et les documents électroniques *du Canada sont aussi générales qu'on pourrait s'y attendre, puisqu'elles sont issues d'un Code modèle volontaire et multisectoriel. Le caractère général qui fait le mérite d'un code modèle peut toutefois devenir un vice dans le contexte d'une loi impérative à force exécutoire. Cet article fait une analyse critique des dispositions de la loi ayant trait à la notion clé de consentement. L'auteure argumente qu'il sera particulièrement difficile pour les entreprises et les consommateurs, eu égard aux problèmes dans la loi, de déterminer quelle est la norme de protection exigée en la matière dans un bon nombre de cas. L'auteure examine ensuite divers « outils » qui pourraient s'avérer utiles pour déterminer les mesures requises dans diverses circonstances afin de se conformer à la loi. Celles-ci incluent le bureau du commissaire à la vie privée, la coutume, les autres textes législatifs, les codes sectoriels, les programmes de sceau de protection, le protocole P3P (plate-forme de préférences des données privées) et le générateur de déclarations de politique de protection de la vie privée.*

The normative provisions relating to privacy in Canada's new Personal Information Protection and Electronic Documents Act *are as general as one might expect, given their origin in a voluntary, multi-sectoral model Code. The generality which is the virtue of a model code, however, may well be a vice for mandatory and enforceable legislation. This paper provides a critique of the provisions of the legislation that deal with the key concept of consent. The author argues that the problems with the legislation will make it particularly difficult for businesses and consumers alike to determine what privacy protections are required across a range of different circumstances. The author then explores a variety of "tools" which may be of use in determining what measures are required in different circumstances in order to comply with the legislation. These include the office of the Privacy Commissioner, past practice, other legislation, sectoral codes, privacy seal programs, P3P and privacy statement generators.*

---

* Associate Professor, Dalhousie Law School. A version of this paper was presented at the Canadian Information Technology Law Association Conference in Halifax, October 20, 2000. I would like to thank John MacDonnell for his careful reading and comments on this manuscript.

TABLE OF CONTENTS

I. INTRODUCTION

The normative provisions of Part I of Canada's new *Personal Information Protection and Electronic Documents Act*[1] are as general as one might expect, given their origin in a voluntary, multi-sectoral model code. The generality that is the virtue of a model code, however, may well be a vice for mandatory and enforceable legislation. This paper considers the tools that may be useful in understanding and applying the normative provisions of the *Act* across a range of commercial contexts. In the forefront is the concern for a degree of certainty in law, both from the point of view of businesses which must implement the *Act*'s provisions regarding the collection, use and disclosure of personal information, and from the viewpoint of consumers who will seek to ensure that their rights to privacy are respected within the boundaries of the law.[2] While the discussion is not limited to e-business, online business is a particular focus of the paper.

In the first part of this paper, I will explain some of the ways in which *PIPA*'s generality may raise problems of interpretation. My particular focus is on the consent principle. The second part of the paper examines various tools available for understanding or elaborating upon the privacy norms. In particular, I consider the role of the Privacy Commissioner, past practice, other legislation, sectoral codes, seal programs and technological tools such as P3P and privacy statement generators.

II. THE *PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT*

The *Personal Information Protection and Electronic Documents Act* was enacted on April 13, 2000, following a push by the federal government to produce legislation that would facilitate electronic commerce by fostering consumer confidence in the protection of personal information.[3] The privacy provisions, awkwardly fused

---

[1] S.C. 2000, c. 5 [hereinafter the *Act,* the *Personal Information Protection* part of the *Act* will be referred to as *PIPA*].

[2] Both businesses and consumers face these interpretive questions with respect to *PIPA*. Businesses will need to either review existing policies for compliance with *PIPA*, or they will need to draft new privacy policies to meet the requirements of *PIPA*. Consumers are given a right of recourse under *PIPA* through the vehicle of complaints to the Privacy Commissioner (s. 11). Although the Commissioner may play a key role in interpreting the requirements of the legislation, consumers dissatisfied with the report of the Commissioner following a complaint have a further recourse to the Federal Court of Canada (s. 14). Note that in the first five years of Quebec's legislation, the Commission d'accèss à l'information received over two thousand inquiries, from which one thousand and fifty files were opened. Nine hundred went to the investigation stage: Quebec, Commission d'accès à l'information du Québec, *Avis de la Commission d'accès à l'information du Québec concernant le projet de loi C-54: loi sur la protection des renseignments personnels et les documents éléctroniques* (November 1998), online: Commission d'accès à l'information du Québec <http://www.cai.gouv.qc.ca/a981514.htm> (date accessed: 17 November 2000) [hereinafter *Avis de la Commission d'accès à l'information*]. There is no reason not to expect that *PIPA* will generate at least this much activity.

[3] Canada, Task Force on Electronic Commerce, *The Protection of Personal Information: Building Canada's Information Economy and Society* (Ottawa: Industry Canada, 1998), online: <http://e-com.ic.gc.ca/english/privacy/632d3.html> (last modified: 10 April 2000) [hereinafter *Protection of Personal Information*].

with legislation regarding electronic signatures,[4] were appended as a schedule to the *Act* which, in its provisions, offered some qualifications to the privacy principles, as well as enforcement and oversight mechanisms.

A. *The Application of the* Personal Information Protection and Electronic Documents Act

The sheer scope of the *Personal Information Protection and Electronic Documents Act* is relevant in exploring its normative generality. Part 1 of the *Act*, which deals with the protection of personal information, is meant to capture virtually all commercial activity in Canada.[5] On the date of coming into force of the *Act*,[6] *PIPA* will apply to the federally regulated private sector[7] and to provincially based organizations which disclose the information they collect outside the province for consideration.[8] Three years after the coming into force of the *Act*, *PIPA* will apply to the private sector more broadly, extending to every organization that "collects, uses or discloses" personal information in the course of commercial activity, regardless of whether that organization falls under federal or provincial jurisdiction.[9] This general application is subject to possible exceptions where individual provinces have enacted legislation that is considered to be equivalent.[10] Such legislation may be applicable to all commercial activity within the province, or only to particular sectors, leaving the federal legislation in place for the sectors not governed by provincial legislation.[11] Since the federal government has already indicated that Quebec's *An Act respecting the protection of personal information in the private sector* [12] is considered to be equivalent,[13] *PIPA* will

---

[4] Hence the long title. The fusing of these two pieces of legislation supports the view that *PIPA* was part of an overall plan to facilitate e-commerce, lending it an e-commerce rather than a personal privacy slant.

[5] *PIPA* only applies to organizations which collect, use or disclose personal information in the course of commercial activities, or to information that relates to employees of organizations who collect, use or disclose that information in connection with the operation of a federal work, undertaking or business: s. 4(1).

[6] Part 1 of the *Act* will come into force on January 1, 2001. Parts 2, 3 and 4 of the *Act* came into force on May 1, 2000.

[7] The *Privacy Act*, R.S.C. 1985, c. P-21, continues to apply to the federal public sector. Section 4(2) of *PIPA* states that *PIPA* does not apply to "any government institution to which the *Privacy Act* applies."

[8] S. 30(1). Under ss. 30(1.1) and 30(2.1), there is a further one year delay with respect to personal health information.

[9] S. 30(2).

[10] S. 26(2)*(b)*.

[11] Section 26(2)*(b)* allows for this fragmented application by providing that where the Governor in Council is satisfied "that legislation of a province that is substantially similar to this Part applies to an organization, a class of organizations, an activity or a class of activities," the Governor in Council may "exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province."

[12] S.Q. 1993, c. 17.

[13] Canada, Privacy Commissioner of Canada, "A Guide to the New Private Sector Data Protection Bill" (Ottawa), online: <http://www.privcom.gc.ca/english/02_06_02b_e.htm> (date accessed: 17 November 2000). In its Consultation Paper on proposed private sector privacy legislation, the Ontario Ministry of Consumer and Commercial Relations adopts an approach to

not apply to the Quebec private sector. The Ontario government is currently contemplating its own private sector legislation.[14] What has the potential to be a confusing patchwork of concurrent and not necessarily identical regimes is the result of federal treading around thorny division of powers questions.[15] Similarly, the limitation of the application of *PIPA* to information collected "in the course of commercial activities" and its potential for ensuing interpretive difficulty[16] is also a product of the need to fit this legislation within the somewhat uncertain scope of the general trade and commerce power.

Where *PIPA* is in effect, it will capture virtually all commercial activity. "Organization" is defined as including "an association, a partnership, a person and a trade union,"[17] and organizations carrying out commercial activities under federal and provincial jurisdictions are likely to include every conceivable form of business undertaking in Canada. *PIPA* is therefore intended to apply equally to banks, insurance companies, utilities, drug stores, grocery stores, video rental outlets and online e-commerce businesses, to give but a few examples.

B. *Normative Vagueness in* PIPA

The breadth of application of *PIPA* serves to exacerbate interpretive problems for those affected by this legislation. While private sector privacy legislation must, of necessity, seek a certain level of generality,[18] *PIPA* has two main problems in this

---

personal information protection that would be quite similar to that in *PIPA*, noting: "The similarity of the proposed Ontario Privacy Act and federal legislation would avoid occasional overlap becoming a source of conflict or confusion": Ontario, Ministry of Consumer and Commercial Relations, *A Consultation Paper: Proposed Ontario Privacy Act* (July 2000), online: <http://www.ccr.gov.on.ca/pdf/PrivacyPaper.pdf> (date accessed: 17 November 2000) [hereinafter *Consultation Paper*].

[14] It is the objective of the Ontario government to produce legislation that would be considered equivalent to *PIPA*, and therefore apply in Ontario instead of *PIPA* (*Consultation Paper*, *ibid.* at 4).

[15] See, *e.g.* the testimony of Roger Tassé on Bill C-6, Ottawa, Senate of Canada, Standing Committee on Social Affairs, Science and Technology, in *Proceedings*, (6 December 1999), online: <http://www.parl.gc.ca/36/2/parlbus/commbus/senate/com-e/soci-e/06ev-e.htm> (date accessed: 17 November 2000).

[16] The extension of the application of *PIPA* to the health care sector has exacerbated this difficulty. See, *e.g.* Ottawa, Senate of Canada, Standing Senate Committee on Social Affairs, Science and Technology, in *Proceedings*, (29 November 1999), online: <http://www.parl.gc.ca/36/2/parlbus/commbus/senate/com-e/soci-e/02ev-e.htm> (date accessed: 17 November 2000). In the Standing Committee hearings on Bill C-6, questions were repeatedly raised about determining how and when medical services constituted commercial activity for the purposes of the legislation. In proposing its own legislation, the Ontario Ministry of Consumer and Commercial Relations notes that "[a]n Ontario Privacy Act could also broaden privacy protection by applying to more than simply 'commercial' activities, as would be the case if Ontario does not act, and the federal legislation applies alone": *Consultation Paper*, *supra* note 13 at 3.

[17] S. 2(1).

[18] For example, in recommending the enactment of privacy legislation in the United States, the U.S. Federal Trade Commission noted the requirement that "any legislation be phrased in general terms and be technologically neutral. Thus, the definitions of fair information practices set forth in the statute should be broad enough to provide flexibility to the implementing agency

regard. First, it is not a model in which more detailed or sector-specific, formalized elaboration of the law is provided for, either through regulation-making or through the mechanism of formal approval of sectoral codes. Second, the incorporation of the Canadian Standards Association (CSA) Code in its entirety introduced into the law a further level of generality.

The normative provisions of the legislation are contained in Schedule 1 of the *Act*, and consist essentially of a reproduction *in toto* of the Canadian Standards Association's *Model Code on the Protection of Personal Information.* Using the Organization of Economic Co-operation and Development (OECD) guidelines on personal data protection[19] as a departure point, the CSA Code was the product of deliberations by representatives from a range of sectors and interest groups which included "the public sector, industries (including transportation, telecommunications, information technology, insurance, health and banking), consumer advocacy groups, unions and other general-interest groups."[20] Following its development and publication as a model code, the CSA Code was adopted by the Standards Council of Canada as a National Standard in 1996.[21]

It is clear that a consensus-based[22] voluntary code of this nature was never intended to provide the more strict normative guidance which one expects of legislation.[23] In fact, the difference between a code drafted as a model and legislation

---

in promulgating its rules or regulations": Canada, Federal Trade Commission, "Privacy Online: Fair Information Practices in the Electronic Marketplace: A Report to Congress" (May 2000), online: <http://www.ftc.gov/reports/privacy2000/privacy2000text.pdf> (last modified: 22 May 2000) [hereinafter "Privacy Online"].

[19] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (23 September 1980), online: OECD <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM> (date accessed: 17 November 2000) [hereinafter *Guidelines on the Protection of Privacy*].

[20] *Protection of Personal Information, supra* note 3 at 9.

[21] Pursuant to the *Standards Council of Canada Act*, R.S.C. 1970, (1st Supp.), c. 41, as am. by s. 4(2)(*e*).

[22] For a critique of the nature of the consensus, see Teresa Scassa, "Privacy and Electronic Commerce: Legislating Conflicting Interests" in *Perspectives on Legislation: Essays from the 1999 Legal Dimensions Initiative* (Ottawa: Law Commission of Canada, 1999) 233 at 237.

[23] Written as a study for the federal government predating the introduction of both Bill C-54 and Bill C-6, the report on *Regulating Privacy in Canada* downplays the normative function of the CSA Model Code:

> At first glance, the CSA Model Code might seem a Canadian version of the OECD Guidelines–a rearrangement and translation of the key principles into the Canadian context. At the moment, it is just that–a model that any organization can use and adapt to their specific circumstances. But it does represent a very important consensus, brokered among the major stakeholders. Moreover, it has doubtless been very valuable for participants in the process to think about the privacy protection problem from scratch and to grapple with these complex issues.

Canada, Industry Canada, *Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector* by C. J. Bennett, (1996), online: Strategis <http://e-com.ic.gc.ca/english/privacy/632d107.html> (last modified: 10 April 2000) [hereinafter *Regulating Privacy in Canada*].

should be quite pronounced. In New Zealand, where privacy law provides that sectoral codes may be given the force of law, the distinction between code and law is important:

> To be most useful, it is expected that codes might include practical examples. Sometimes this may take the form of a rule prescribing how the principle is to apply in such a case. However, in many cases, it will be inappropriate for those examples to be included in the formal code as issued as a legally binding document. Accordingly, it is suggested that a format be adopted whereby parts of the code intended only for illustrative purposes are distinguished from the operative parts of the code.[24]

In *PIPA*, the discursive elements of the CSA Code were incorporated into the legislation, along with the privacy principles, adding significantly to the potential complexities of interpreting the legislation. As the New Zealand Privacy Commission goes on to note: "Generally codes under the Act will need to be more detailed and precise than the more discursive codes found in some other areas and in other jurisdictions. This relates to the fact that *the code will have to be capable of legal interpretation.*"[25] In the case of *PIPA*, the wording of the norms, and the structure of the legislation in incorporating the norms, create a great deal of ambiguity about the precise standards required by law for the protection of personal information. Interestingly, the proposal for private sector personal information protection legislation in Ontario is gently critical of the incorporation of the entire CSA Code into the legislation, and suggests that such a route would not be followed in Ontario:

> The proposed Ontario Privacy Act would be based on the CSA Standard. However, although the CSA Standard is well suited to be applied as a voluntary code, not all of its elements may be well suited for legislation. Therefore, Ontario is considering each element of the CSA Standard and whether it would make an appropriate statutory requirement.
>
> In some cases, the CSA Standard relies on recommendations for information management processes. Ontario's proposed legislation would focus on outcomes, and what is clearly required, rather than processes. In other words, although key provisions of the CSA Standard would be adopted, certain provisions would not be used in the proposed Ontario Privacy Act.[26]

While a certain amount of generality is needed in all legislation in order to enable the law to be interpreted and applied to the variety of circumstances which may emerge over time, the generality of the normative provisions of *PIPA* is extreme. I will explore this generality and its consequences using the key consent principle as an illustration.

---

[24] New Zealand Privacy Commission, *Draft Guidance Note on Codes of Practice under Part VI of the Privacy Act*, online: <http://www.knowledge-basket.co.nz/privacy/comply/cops.html> (last modified: 30 August 1998).

[25] *Ibid.* (emphasis added).

[26] *Consultation Paper*, *supra* note 13 at 4-5. The Paper continues at 5 as follows: "This drafting approach differs from the federal legislation's design, however the proposed Act would closely resemble the federal legislation on the key elements of the CSA Standard. The proposed Act would be drafted similarly to Quebec's privacy legislation, which has been in place since 1994 and is working well."

C. *Consent*

Consent is fundamental to any legislation protecting personal information from unwarranted collection, use or disclosure. Under *PIPA*, as under similar pieces of legislation,[27] consent of the individual is required for the collection, use or disclosure of his or her personal information. Consent in law, however, is an inherently variable concept. Notions of express and implied consent add layers to the interpretation of adequate consent in areas such as tort and contract law. It is to be expected, therefore, that in any personal information protection legislation the notion of consent will be a flexible one. However, the normative provisions of *PIPA* render the notion of consent so mutable and context-specific as to raise concerns among businesses and consumers alike as to whether the appropriate consent is being sought in any given set of circumstances.

Consent in Schedule 1 of *PIPA* is described in paragraphs 4.3 to 4.3.8. Paragraph 4.3 begins with the concise statement of principle that "[t]he knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where appropriate." *PIPA* itself attempts to provide some certainty to the qualifier "except where appropriate" by setting out a series of circumstances in which information can be collected, used, or disclosed without the consent of the individual. These circumstances include some broadly worded allowances for the investigation of breaches of "an agreement or a contravention of the laws of Canada or a province,"[28] including, in some circumstances, anticipated breaches of the laws of Canada or a foreign jurisdiction.[29] Exceptions around disclosure are also legislated for medical emergencies, statistical or scholarly study or research, or for the more mundane purposes of collection on a debt, and communications with lawyers.[30]

---

[27] See, *e.g.* EC, *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*, [1995] O.J. L. 281/31 [hereinafter *Directive on Personal Data Protection*]; Quebec's privacy legislation *supra* note 12; and the federal *Privacy Act*, *supra* note 7.

[28] *PIPA*, *supra* note 1, s. 7(1)(*b*).

[29] See s. 7(2)(*a*). These qualifications are significant for the discussion that follows in that they elaborate contexts in which information validly collected for specific purposes can be used or disclosed for other purposes without the knowledge or consent of the individual. The legislation does not appear to require that the individual be informed of these possibilities, other than by the terms of the legislation. Thus, a business policy would not need to include them. Nonetheless, to the extent that a business has a particular practice or policy in place to deal with situations where such information is sought, it is not clear whether the business should make this policy known to individuals in order to allow them to give an informed consent. It is unlikely that the law requires such steps, though it might be a reasonable fair information practice, and arguably could become an industry standard or sectoral practice. Note, for example, that the Canadian Association of Internet Providers' (CAIP) Privacy Code, developed for its membership, provides that where members disclose personal information without consent when required by law, they should ensure that the demand for disclosure complies with the law, and strictly limit disclosure to what is required by law. Further, the policy states that "[a] member may notify users that an order has been received, if the law allows it": Canadian Association of Internet Providers, *Privacy Code* (1996), online: <http://www.caip.ca/privacy/privacy1.htm> (date accessed: 17 November 2000).

[30] S. 7(3).

As a general normative principle, the statement that "the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information" is not particularly strong. By contrast, the Quebec legislation provides that:

> 14. Consent to the communication or use of personal information must be *manifest, free and enlightened,* and must be given for specific purposes. Such consent is valid only for the length of time needed to achieve the purposes for which it was requested.[31]

In the *European Directive on Personal Data Protection*, data can only be processed where "the data subject has *unambiguously* given his consent."[32] Consent is further defined in the *Directive*, which provides, in art. 2(h) that:

> 'the data subject's consent' shall mean any *freely given specific and informed indication of his wishes* by which the data subject signifies his agreement to personal data relating to him being processed.[34]

Both the Quebec and the European standards are thus much more strictly worded than in *PIPA*, suggesting a higher threshold. This may raise questions as to whether the form or nature of consent required under *PIPA* is less rigorous than that required under comparable legislation.

The loosely worded consent principle in *PIPA* is made more problematic by the elaboration, in Schedule 1, of the notion of consent. Schedule 1 provides qualifications on the timing of obtaining consent, the effort required to ensure that the individual is advised of the purposes of information collection, the form of consent required, the relationship between consent and the reasonable expectations of individuals, the means of seeking consent, express and implied consent, and the ways in which consent can be given by individuals. While the general consent principle as stated would inevitably have been subject to interpretation had it formed the exclusive normative rule around consent, nevertheless these particular elaborations serve to so significantly muddy the understanding of consent as to undermine the general rule. They are also likely to leave the average entrepreneur or consumer wondering exactly what is required in any particular context for a valid consent to be given. The problem is compounded by the fact that the CSA Code was formulated and drafted before the rise of widespread online business-to-consumer commercial activity.[35] Thus, the wording

---

[31] *Supra* note 12 (emphasis added). In the *Avis de la Commission d'accès à l'information, supra* note 2 at 17, the Quebec Privacy Commission notes that "[l]e projet de loi C-54 est moins précis quant aux règles de validité du consentement."

[32] *Supra* note 27 at Art. 7(*a*) (emphasis added).

[34] *Ibid.* at Art. 2(h) (emphasis added).

[35] The Code was ratified in 1995.

around consent, which would be ambiguous in a non online context,[36] may provide virtually no guidance in online contexts.

1. *Objective Standard*

At several points in the elaboration of the principle of consent, Schedule 1 refers to objective standards for meeting the requirements of the *Act*. For example, an organization is required to make a "reasonable effort to ensure that the individual is advised of the purposes for which the information will be used."[37] While in many cases the reasonableness of the effort will be easy to assess, some situations may present greater difficulty. This is particularly likely to be the case in the online context. For example, a registration or application form for a product or service in a non online context may well contain the purposes for collection on the application form itself. This is likely to be considered a reasonable effort to inform the consumer. However, in the online context, many web sites locate such information in the privacy policy. These policies tend to be accessed from a link on the homepage, rather than at the point of information collection, which might be the registration form or order-entry window of the site. Whether this constitutes a reasonable effort to communicate the purposes of collection is open to discussion. The answer may depend on the location and size of the link to the privacy policy, or on other contextual factors such as emerging online practice.[38]

Another reference to a kind of "objective" standard appears in paragraph 4.3.5, which refers to the "reasonable expectations of the individual," and states that they are also relevant. However, it is unclear the degree to which the reasonable expectations of any given individual can be taken into account in the design of a company's privacy policy and consent-seeking methods. In an era of mass marketing, these individualized expectations are not likely to be known or assessed. In the online world, where face-to-face contact is absent, the individual is even more likely to merge into a composite consumer. Thus, to make sense, the paragraph must envisage a kind of "reasonable consumer" assessment of what is required in order to obtain a valid consent. For example, the paragraph uses the illustration of a person who subscribes to a magazine and states that they should "reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact

---

[36] Even the more strictly worded provision in the Quebec legislation has presented issues of interpretation. The Quebec Privacy Commission notes the following: "Au cours des dernières années, la Commission a été appelée à maintes reprises à évaluer la validité des consentements suite à des plaintes formulées par les citoyens. Les qualités du consentement décrites à l'article 14 de la loi québécoise l'ont grandement aidée à établir la validité ou non des consentements demandés par les entreprises établies au Québec." *Avis de la Commission d'accès à l'information*, *supra* note 2 at 17.

[37] *Supra* note 1 at para. 4.3.2.

[38] Significantly, emerging practice in e-business may well be leaning toward containing all such information in a separately located privacy statement. For example, many current commercial web sites follow a fairly typical format in terms of providing links to disclaimers and other legal notices from the homepage. The question remains whether the use of that format constitutes a "reasonable effort" to ensure that the consumer is aware of the purposes for which his or her personal information will be used. For further discussion of online practices, see below.

the person to solicit the renewal of the subscription."[39] A second illustration provided is that of the individual who provides information to a health care professional and could reasonably expect that this information would not be "given to a company selling health-care products, unless consent were obtained."[40] It would seem that the differences between these two examples rely less on the "reasonable expectations of the individual," which implies a subjective standard, and more on the more objective standard of the "reasonable individual" or "reasonable consumer."[41]

Finally, the Schedule leaves unclear who determines who the reasonable individual is, and how they relate to their information. Clearly, the answer might be different if the question were approached from a business rather than a consumer perspective. For example, from a business perspective, the reasonable individual might expect the business to use personal information to build an individualized profile in order to better assess the consumer's product likes and dislikes. The reasonable individual, on the other hand, might find such profiling activity to be an unacceptable invasion of their privacy. The legislation itself is highly ambiguous about the "perspective" it favours. While referencing protection of privacy as an important right in section 3, it does so in a context which immediately balances that right with the needs of business to collect, use and disclose such information. Further, the preamble of the *Act* does not refer explicitly to a privacy right, but rather indicates that the purpose of the legislation is to "support and promote electronic commerce by protecting personal information."[42] Perhaps recognizing a slant toward the business perspective, the Quebec Privacy Commission, in its comment on the legislation, took the view that "l'évaluation des attentes raisonnables d'une personne sera laissée à la discrétion de l'organisation."[43] It is interesting to note that Canada's Privacy Commissioner at the time of the enactment of the legislation, Bruce Phillips, identified himself as the "reasonable person" referred to in the legislation, stating, "I hope to function as a surrogate for that '*reasonable person.*'"[44] In attempting to describe the approach of the reasonable person to data collection he stated:

> A reasonable person will not take every business to task for collecting personal information. A reasonable person will welcome the collection of personal information in some situations, since it will serve the person in his or her dealings with that business. However, a reasonable person will challenge the excessive and persistent collection of information about them,

---

[39] *Supra* note 1 at para. 4.3.5.

[40] *Ibid.*

[41] It is not clear, therefore, how paragraph 4.3.5 with respect to the reasonable expectations of the individual is ultimately much different from paragraph 4.3.6, which states that "[t]he way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected." The clause goes on to state that express consent is generally appropriate where information is sensitive, but implied consent is acceptable for information which is "less sensitive."

[42] *Supra* note 1. For a more detailed discussion of the ambivalence in the legislation around privacy and electronic commerce, see Scassa, *supra* note 22 at 238-240.

[43] *Avis de la Commission d'accèss à l'information*, *supra* note 2 at 17.

[44] Bruce Phillips, "The Privacy Commissioner of Canada's approach to implementing the Act" (CENTRUM conference, 10 December 1999) [unpublished], online: <http://www.privcom.gc.ca/english/02_05_a_991210_e.htm> (date accessed: 17 November 2000).

> the indiscriminate or careless sharing of that information with others and the shrouding of that information-handling process in secrecy.[45]

It is not entirely clear why, in the face of enormous and widespread abuse of personal information by the private sector, the "reasonable person" would not be somewhat more militant in their stance regarding the collection, use and disclosure of personal information. It remains to be seen how interpretation will shape the key consent provision of the law.

2. *Degree of Sensitivity of the Information*

Paragraph 4.3.4 states that the form of the consent may vary depending on the type of information, and that "[i]n determining the form of consent to use, organizations shall take into account the sensitivity of the information." The paragraph goes on to explain that "some information (for example, medical records and income records) is almost always considered to be sensitive," yet that "any information can be sensitive, depending on the context." The example given distinguishes between the non-sensitive nature of the names and addresses of subscribers to a news magazine, and the potentially higher sensitivity of comparable information about subscribers to "some special-interest" magazines.

Apart from the unmanageably subjective nature of this kind of sensitivity (some individuals might be much more concerned than others about the privacy of their subscriptions to any variety of magazines), there are further problems with this approach. Fundamentally, linking the nature of consent to be sought to the sensitivity of the information is unworkable since the consent is obtained at the time of collection. Such an approach fails to recognize that sensitivity of information can vary according to context and the use that is made of the information. Thus, if a low level of consent is required because the information is considered less sensitive, the individual may nonetheless find their privacy substantially invaded by subsequent uses. For example, an individual who provides her name and address for a fairly innocuous magazine subscription, and does not notice the negative option check box on the subscription form which indicates that unless checked, information will be provided to third parties for direct marketing purposes, may find that her privacy is substantially invaded by the subsequent deluge of mass marketing appeals. Further, in the online context, apparently "non-sensitive" information, when linked with other information such as shopping preferences or surfing behavior, can be used to create a highly personal profile of an individual. Since consent is supposed to be given for particular uses, the degree of consent required should not be tied specifically to the nature of the information. This is certainly the approach in the Quebec legislation which requires a "manifest, free and enlightened" consent regardless of the circumstances. The linking of the form of consent to the nature of the information in *PIPA* is a further indication of the weakness and ambiguity of the consent principle. Needless to say, it also gives rise to further problems of interpretation.

Although the link between sensitivity and consent has its problems, the point that some kinds of information are more sensitive than others is not unimportant. In any

---

[45] *Ibid.* One can assume, of course, that subsequent Privacy Commissioners are not necessarily bound by this view or approach.

event, for someone attempting to interpret and apply this legislation, be they business or consumer, establishing some kind of spectrum of sensitivity is important. Nevertheless, both the Schedule and *PIPA* itself are quite unhelpful when it comes to determining what information should be considered sensitive. This in contrast with the *European Directive*, which specifically identifies categories of information that cannot be processed except in carefully delimited circumstances. This would include "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[46] In implementing the *European Directive*, Great Britain included in its *Data Protection Act 1998* a specific and detailed definition of sensitive data[47] as well as a separate Schedule to the *Act* regarding the processing of sensitive personal data.[48] In a similar vein, the Explanatory Memorandum to the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* states that:

> The Expert Group discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive. Consequently, Paragraph 7 merely contains a general statement that there should be limits to the collection of personal data. For one thing, this represents an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data. The nature of the limits is not spelt out but it is understood that the limits may relate to:
>
> . . .
>
> - "earmarking" of specially sensitive data according to traditions and attitudes in each Member country;
>
> . . .
>
> - civil rights concerns.[49]

PIPA does not come close to excluding or limiting the collection, use or disclosure of particular categories of information. Nonetheless, through the notion of "sensitivity" it suggests that some information must be handled more delicately than other kinds of data. What little guidance is provided, however, raises its own problems of interpretation. For example, paragraph 4 states that "income records" are almost always considered to be sensitive. It is not clear whether this would include the kind of marketing surveys that ask individuals to indicate the range within which their income falls; nor is it clear what it would mean for businesses which ask for postal codes, and which may make decisions or assumptions about income on the basis of the physical location of the individual's home.

---

[46] *Supra* note 27 at Art. 8(1).

[47] (U.K.), 1998, c. 29, s. 2. Section 2 includes information on race, ethnic origin, political opinion, religious beliefs, membership in a trade union, physical or mental health or condition, sex life, commission or alleged commission of any offence, or any proceedings related to any offence or alleged offence.

[48] *Ibid.* at Sch. 3.

[49] *Guidelines on the Protection of Privacy*, *supra* note 19 at para. 51.

The problem is further amplified by the wording of 4.3.6, which is largely repetitive of the ideas in 4.3.4, and which states that:

> the way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive.

What is particularly disturbing about this paragraph is the linking of "implied" consent to information considered to be less sensitive. This seems to suggest a very low threshold for much routine collection of the kind of personal information that many individuals nonetheless resent having disseminated. In addition, this "less sensitive" information, when matched with other information, can create a disturbingly vivid portrait of an individual. The Federal Trade Commission 2000 Survey of web sites found that most web sites "are capable of creating personal profiles of online consumers by tying any demographic, interest, purchasing behavior, or surfing behavior information they collect to personal identifying information."[50] Certainly, in the world of cookies and data mining, a standard revolving around the degree of sensitivity of particular pieces of information seems inadequate.[51]

Further problems arise with the linking of sensitivity with the notion of context: "any information can be sensitive depending on the context." No guidance is given as to what contextual elements are relevant. It is not clear, for example, whether the past practices of the particular industry might be relevant to the context. Thus, if information used to be provided without seeking express consent, (as has often been the case), is it then acceptable to continue to do so under *PIPA* using the argument that the information has not previously been treated as sensitive? Quite possibly, "context" would include the nature of the product being sold (as noted above, there are references to this concept in paragraph 4.3.4). Also alluded to are factors such as the consumer's vulnerability with respect to certain kinds of information, and the expectations of the individual. However, the subjectivity involved in the last two factors is likely to make such

---

[50] "Privacy Online", *supra* note 18 at 10.

[51] The TRUSTe certification program is sensitive to this issue. Its definition of personally identifiable information goes far beyond the equivalent definition in the CSA Code. Under TRUSTe: " 'Personally Identifiable Information' refers to any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other personally identifiable information can easily be derived, including, but not limited to, name, address, phone number, fax number, e-mail address, financial profiles, social security number, and credit card information. To the extent unique information (which by itself is not Personally Identifiable Information) such as a personal profile, unique identifier, biometric information, and IP address is associated with Personally Identifiable Information, then such unique information will also be considered Personally Identifiable Information. Personally Identifiable Information does not include information that is collected anonymously (i.e., without identification of the individual user) or demographic information not connected to an identified individual": Online: <http://www.etrust.com/webpublishers/pub_sitecoordinatorsguide.html>(last modified 20 November 2000).

"contextualization" unworkable for drafters of privacy policies, except in the roughest and most generic form.

3. *Minors and Others Incapable of Giving Consent*

One possible "contextual" factor might well be the age or capacity of the individual providing the information. However, *PIPA* is almost entirely silent as to what rules apply when information is being collected from minors or others incapable of giving consent. The only reference appears to be in paragraph 4.3.6. of the Schedule which states that "[c]onsent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney)." This statement leaves it unclear as to whether consent must be sought from such an individual in all cases where, for example, a child is involved, or whether this is simply an option for businesses. The position is certainly otherwise in the United States, where specific legislation has been enacted to deal with the gathering of information from children in the online environment.[52] A business governed by *PIPA* would have no guidance from the Canadian legislature as to the appropriate approach to dealing with the personal information of children.[53]

4. *Modes of Gathering Consent*

Paragraph 4.3.7 of *PIPA* illustrates some of the ways in which it is envisaged that individuals may give consent. The examples given are ones from the non-online business environment. For example, in 4.3.7(a) an application form is considered as being an acceptable means to "seek consent, collect information, and inform the individual of the use that will be made of the information." By completing and signing the form, the individual is considered to have given consent to the collection and the specified uses. Yet, as noted earlier, this example is not helpful in assessing the situation of the online business which has an application form, but which also has a link to a separate privacy policy setting out purposes for collection, and other relevant privacy information. The reference to a signed consent raises questions about online application forms which cannot be "signed," and about the contexts in which a signature is relevant for consent.

Paragraph 4.3.7(b) refers to the use of a check-off box. Individuals can request that their personal information not be given to other organizations by checking off a box. This negative option consent mechanism is inherently problematic; it would certainly seem to fly in the face of stricter standards of consent, such as those in the Quebec legislation and the European Directive. Even the Canadian Information Processing Society has expressed the view that:

> From a privacy perspective, this method of opting out is contentious. According to a major survey of Canadian privacy attitudes, the public does not want their personal information sold for direct marketing purposes. The

---

[52] *Children's Online Privacy Protection Act of 1998*, 15 U.S.C. SS 6501 *et seq.*

[53] It is worth noting that the Ontario proposal for personal information protection legislation indicates a desire to specifically address this issue. See *Consultation Paper*, *supra* note13 at 6.

> public view is that privacy should be the default condition and explicit consent should be obtained for secondary uses.
>
> The use of a checkoff box to opt out is analogous to the reverse-marketing option, where the onus is on the individual to opt out of new services for which he might be charged. The extent of public aversion to the reverse-marketing option can be gauged by the cable television example of a couple of years ago.[54]

The permissive reference to "reverse-option" consent suggests that the standard for consent in *PIPA* can be extremely low. In its recent survey of online privacy policies, the FTC was also critical of practices surrounding "negative option" consent. Its findings were as follows:

> Often, sites state that information will not be used to contact the consumer, or will not be shared with third parties, without the user's consent or agreement. In practice, however, such "consent" is obtained either through the provision of the information by the consumer (i.e., by providing the information the consumer implicitly agrees to these secondary uses) or by pre-checked "click-boxes" buried at the end of a registration form. In the latter case, a consumer may believe, based on the "consent" language, that he or she need not do anything to prevent the further use of the information. In reality, however, because a click-box had been pre-checked, the consumer is deemed to consent unless he or she unchecks the box. The use of ambiguous language regarding how consumers can exercise choice undercuts the value of offering such choice in the first instance.[55]

The prospect of pre-checked "click-boxes" online makes the permissiveness in *PIPA* towards this type of "reverse-option" consent even more problematic. Even if one accepts that negative option consent is ever acceptable, 4.3.7(b) offers no guidelines as to the limits on this approach.[56] Quite apart from not addressing pre-checked boxes, nothing seems to require that the box and accompanying text be at least the same size and font as the rest of the form. It is also not clear in what circumstances the negative option approach would not be acceptable, or what the parameters of any such approach would be. Some web sites currently note in their privacy policies that individuals who do not want their information used in particular ways should e-mail the company at a specified address.[57] This form of practice raises not only the problems associated with

---

[54] The External Liaison Committee of the Canadian Information Processing Society, "Privacy & Information Technology Paper: Implementation & Operational Guidelines," August 1997, approved by the CIPS National Board of Directors, October 1997 at 15 of 27, online: <http://www.cips.ca/it/position/privacy> (date accessed: 17 November 2000)

[55] "Privacy Online", *supra* note 18 at 26.

[56] The *Consultation Paper*, supra note 13, on the proposed Ontario Privacy Act recognizes the lack of guidance in *PIPA* when it states at 10 that "[t]he CSA Standard covers opt-out consent only in general terms. The proposed Ontario Privacy Act would clarify the use of opt-out consent, so as to avoid disputes."

[57] For example, 1-800-Flowers has the following wording in their policy: "If you prefer not to have us provide information about you to third parties, please let us know," and provides a regular mail and an e-mail address for this notification to take place. See online: <http://www.1800flowers.com/flowers/security/index.asp>. Similarly, the Airmiles privacy

"reverse option" consent, but also places an additional burden on consumers to take a further step (writing an e-mail) in order to protect their information privacy.[58]

To further illustrate the lack of real guidance provided in *PIPA*, paragraph 4.3.7(c) provides that consent may be given orally when information is collected over the telephone. This is obviously problematic, especially if no records are kept of the telephone solicitations that elicit the information. In this situation, where individuals may feel particularly pressured by the immediacy of the demand, the human voice attached to it, and the lack of time for reflection, problems of appropriate consent may be particularly acute.[59]

Finally, paragraph 4.3.7(d) states that consent may be given at the time that individuals use a product or service. This is a kind of click-wrap or shrink-wrap option, where, by use of the product or service, the consumer agrees to the attached terms and conditions. This may get dangerously close to requiring the provision of personal information in exchange for a product or service. Although paragraph 4.3.3 anticipates this, the statement that "[a]n organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes" does not seem to prohibit this activity. As long as the purposes of collection are legitimate and clearly specified, making access to a product or service contingent upon supplying personal information would seem to be permitted. This is in definite contrast to the Quebec legislation: "No person may refuse to respond to a request for goods or services or to a request relating to employment by reason of the applicant's refusal to disclose personal information" except in very clear and limited circumstances.[60]

---

policy reads, in part, as follows: "We respect your privacy when we promote products and services. If you do not wish to receive telephone calls or promotional mailings, other than AIR MILES Account Updates, simply inform us by writing" to the address provided: online: <https://secure2.airmiles.com/english/About/AboutPrivacy.asp>).

[58] The *Consultation Paper, supra* note 13 at 10 seems to take the position that "opt-out" consent provisions would be acceptable: "An 'opt-out' approach could be implemented through a document to which the individual would otherwise have to signify agreement or through providing clear notice setting out a straightforward (and cost free) means of exercising the opt-out. It would not be acceptable for an organization to simply have a policy of permitting opting out if asked, without ensuring individual are aware of their opportunity and have an easy means to use it."

[59] In the Member Notes on the *Draft Privacy Code for the Canadian Association of Internet Providers* the following comment is made: "The definition of 'consent' includes the option for a user to provide oral consent. We have left this option in our draft code because it exists in the national standards although we encourage CAIP members to rely primarily on electronic or written authorization given the uncertainties inherent in oral consent." Online: CAIP <http://www.caip.ca/privacy/privacy1.htm> (last modified: 20 November 2000). This highlights the problems of interpretation posed by the wordiness of Schedule 1 of *PIPA*, and the difficulties of translating a broadly worded standard into a functional and appropriate privacy code.

[60] *Supra* note 12 at s. 9. These circumstances include where "collection of that information is necessary for the conclusion or performance of a contract," where the collection is authorized by law, or where there exist reasonable grounds to believe that the request for goods or services is not lawful. Section 9 further clarifies the situation: "In case of doubt, personal information is considered to be non-necessary."

5. *Withdrawal of Consent*

Paragraph 4.3.8 of *PIPA* stipulates that "An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice." While important, the impact of this section may be greatly diminished by the reference to contractual restrictions. The withdrawal of consent provision might be easily circumvented by the use of "mini contracts" for the provision of personal information. Businesses concerned about the cost or the impact of consent withdrawal might choose, therefore, to use a contract model for collection information. In any event, programs which collect personal information in exchange for "rewards" are likely to be already on a kind of contract model. While a consumer may choose not to provide further information, they may not have a right to withdraw consent to the use of already collected information, for which the company has already provided "consideration" in the form of points or rewards.

III. TOOLS FOR CLARIFYING *PIPA* OBLIGATIONS

Given the uncertainty that accompanies the vagueness of the provisions of *PIPA*, businesses will be seeking some form of guidance as to how they can or should draft privacy policies. Similarly, consumers will be looking to define the boundaries of their right to information privacy. In this part of the paper I will consider some of the options available for elaborating the new legislation. Although I will begin by examining the role of the Privacy Commissioner, I will also look at past practice, existing legislation, sectoral codes, privacy seal programs, and technologically-enhanced protection measures such as the Platform for Privacy Preferences Project (P3P) and the OECD Privacy Policy Statement Generator. I will give particular, though not exclusive, attention to the e-business context.

In the earlier critique of the consent provisions of the *PIPA*, it should be clear that while some of the elaboration of the legislative norms will depend on context, much has to do with perspective. As noted earlier, what constitutes an appropriate consent in a given set of circumstances may depend very much on whether one is approaching the question from the point of view of seeking to facilitate the transfer of information, or whether one's perspective is influenced by the desire to carefully preserve personal privacy. In assessing the interpretive tools which follow, it is important to keep in mind the perspective or approach which they may favour, and the extent to which such approaches may affect the interpretation of *PIPA*.

A. *Privacy Commissioner*

The Privacy Commissioner has significant powers under *PIPA*. These powers include the handling of complaints,[61] including the initiation of complaints,[62] and powers of audit.[63] In addition, the Commissioner is empowered to enter into agreements with provincial counterparts "to ensure that personal information is protected in as consistent

---

[61] *PIPA*, *supra* note 1, ss. 11-13.
[62] S. 11(2).
[63] Ss. 18-19.

a manner as possible,"[64] to co-ordinate activities, to conduct research, and to "develop model contracts for the protection of personal information that is collected, used or disclosed interprovincially or internationally."[65] The Commissioner is also responsible for developing public information and education programs,[66] and is given the power to "encourage organizations to develop detailed policies and practices, including organizational codes of practice."[67] These latter powers are perhaps the most significant for the purposes of elaborating the law.

Although relatively open-ended,[68] the role of the Privacy Commissioner could be central to the process of elaborating the legislation. Clearly, the Commissioner's understanding of the law will be central to whether, on investigating a complaint, the Commissioner finds that one or more of the principles has been violated. The Commissioner's[69] interpretation of the principles will also be key to any decision to initiate an audit on the basis that s/he "has reasonable grounds to believe that the organization is contravening"[70] the law. The Commissioner's views on the law, disseminated through information programs, and formal and informal consultation on policies and practices, will be of crucial importance in shaping the interpretation of the fair information principles and their application in a variety of contexts.

The Privacy Commissioner is likely to be assisted by contacts with other jurisdictions where privacy legislation has been implemented. The ability to share expertise and experience across boundaries may be particularly vital in this area. In addition, other international initiatives may also be of use. For example, the OECD has recently developed a guide for online web privacy policy design that contains many useful suggestions that could be incorporated into a similar set of guidelines by the Privacy Commissioner.[71]

It is clear that the Privacy Commissioner will need to be guided by other views and sources relating to the interpretation of the information privacy principles. Of particular difficulty will be the application of the principles over a wide variety of commercial contexts. The legislation anticipates that the Privacy Commissioner will consult with other provinces on information privacy matters, and that s/he will work with organizations in the development of privacy policies. Significantly, however, the legislation does not provide any mechanism for public consultation or input. In fact, *PIPA* appears to contemplate a one-way flow of information from the Privacy Commissioner to the public, who will be on the receiving end of "information programs

---

[64] S. 23(1).

[65] S. 23(2).

[66] S. 24(*a*)(*b*).

[67] S. 24(*c*).

[68] This is by comparison with the Commissioner's counterparts in New Zealand and the U.K., who play a much clearer role with respect to the formalization of sectoral codes.

[69] Or his or her designate. The *Act* contains provisions allowing the Commissioner to delegate his or her powers of investigation and audit (ss. 12(3), 18(2)). More significantly, the Act envisages collaboration between the Commissioner and his or her counterparts under comparable provincial legislation (s. 23).

[70] S. 18(1).

[71] OECD, Group of Experts on Information Security and Privacy, *Practices to Implement the OECD Privacy Guidelines on Global Networks* (December 23, 1998), online: <http://appli1.oecd.org/olis/1998doc.nsf/linkto/dsti-iccp-reg(98)6-final> (date accessed: 17 November 2000) [hereinafter *Practices to Implement the OECD Privacy Guidelines*].

to foster public understanding, and recognition of the purposes"[72] of the *Act.* It could be argued that the legislation itself incorporates a slant towards an industry perspective. It will be interesting to see how the Privacy Commissioner handles the role of mediating between competing interests under *PIPA.*

B. *Past Practice*

It is unlikely that past practice will constitute a particularly useful reference point in assessing whether the privacy policy of a business or sector is in compliance with *PIPA.* Legislation is, after all, considered to serve a purpose, and it can be safely assumed that prior to the enactment of *PIPA* there was very little in the way of personal data protection in the private sector. Although the CSA Model Code existed prior to its incorporation into *PIPA,* it has only been available since 1995. While some businesses have addressed privacy issues by relying on the CSA Code,[73] this should not mean that their policies are in any way immune from scrutiny.

The lack of privacy policies for private sector businesses is particularly noticeable in online commercial activity. A recent report of the United States Federal Trade Commission notes that the number of websites in a random sample which provided any sort of privacy disclosure has jumped from 14% in 1998 to 88% in 2000.[74] Yet, in spite of these improved numbers, and in spite of publicity and efforts around self-regulation in the United States, the FTC report also notes that only 20% of sampled websites "implement, at least in part, the fair information practice principles of Notice, Choice, Access, and Security."[75] There is no reason to expect that results of a similar survey in Canada would be any better. A quick canvas of online e-businesses will reveal surprisingly few privacy policies, let alone ones which could be said to conform to the requirements of *PIPA.*

C. *Other Legislation*

In some industries, where the handling of personal information is considered particularly sensitive, or where it could bear significant consequences for the data subject, legislation is already in place to set minimum standards for data collection, use and disclosure. This is particularly the case in the financial services and credit reporting sectors. For example, s. 18(1) of the Alberta *Financial Consumers Act*[76] deals with information provided by consumers to those selling financial products. It stipulates that such information "can only be used for the purpose for which it is given unless the consumer specifically consents to another use." The conditions under which consent

---

[72] S. 24(*a*).

[73] For example, the Canadian Bankers Association Privacy Code is based upon the CSA Model Code.

[74] "Privacy Online", *supra* note 18 at 11. The Report notes, however, that these figures include even the most cursory privacy statements and "does not necessarily mean that a site follows any or all fair information practices"(*ibid.* at 11).

[75] *Ibid.* at 12.

[76] R.S.A. 1990, c. F-9.5.

may be given are also clearly spelled out in the legislation.[77] Similarly, credit reporting legislation places restrictions on the gathering of certain kinds of information, and on its disclosure, and may make provisions for consumer consent to the disclosure of the information.[78] Thus, in some jurisdictions, reporting agencies cannot provide any information except in a report to a person who will use the information for specific outlined purposes. They must ensure accuracy of their reports,[79] and they must not include a range of information including highly sensitive demographic information, or information not based on reliable evidence, or information based on events over six years old.[80]

Where such legislation is already in place, it would continue to apply to the targeted industries, and would provide a greater degree of certainty around the issue of appropriate consent for that industry. *PIPA* contemplates that the Governor in Council may create exemptions to the application of *PIPA* for "an organization, a class of organizations, an activity or a class of activities" governed by provincial legislation that is "substantially similar to this Part."[81] Nonetheless, because stricter provincial legislation dealing with particular industries would not necessarily be in conflict with *PIPA* (which, as noted earlier, is very general in its wording), there seems to be no reason to exempt these industries from *PIPA*. Rather, they could continue to meet the strict standards set out in legislation governing their operations, as well as the more general provisions of *PIPA,* for other data collection they may engage in which is not of such a core and highly sensitive nature.

The concurrent operation of *PIPA* and other legislation dealing with privacy issues in specific contexts could also lead to some uncertainty and confusion. It certainly risks making recourse more difficult for consumers who may be unaware of the different regimes and their differing modes of recourse. In considering whether to enact its own private sector privacy legislation, the Ontario Ministry of Consumer and Commercial Relations has indicated that Ontario would try to organize privacy norms under the umbrella of a single statute:

> Credit reporting is an example of an area that could be proposed as a sector code. There are already rules for the exchange of personal information used for credit reporting in the Consumer Reporting Act. It may make sense to address credit reporting as a sector under the proposed Ontario Privacy Act rather than under the current statute, so the laws do not overlap and are easier to oversee.[82]

This would be a desirable approach to privacy regulation. However, jurisdictional problems make it difficult, if not impossible, for the federal government to take this

---

[77] S. 18(2). Consent must be given in writing, it must be clear that it is consent which is being sought from the consumer, and the form must be explicit as to which information will be released, for what purposes, and to whom. Section 18(4) also clearly specifies that refusal to give such a consent cannot result in the rejection of an application by a consumer for an investment in a particular financial product.

[78] See *e.g.* the *Credit Reporting Act*, R.S.B.C. 1996, c. 81 or the *Consumer Reporting Act*, R.S.N.S. c. 93.

[79] *Credit Reporting Act, ibid.*, s. 11; *Consumer Reporting Act, ibid.*, s. 10.

[80] *Credit Reporting Act, ibid.*

[81] *PIPA, supra* note 1, s. 26(2).

[82] *Consultation Paper, supra* note13 at 16.

approach in the face of provincial statutes dealing with privacy on a sectoral basis. The main tool for dealing with such conflicts under *PIPA* is the use of exemptions, which is a much more complex option than that proposed in Ontario.

Standards legislated for particular industries might prove to be useful models for sectors or industries which deal with comparable kinds of information. Thus, while the legislation itself would have no actual effect outside the sector it regulates, it could be used to indicate the level of protection which should be available for certain kinds of information. Apart from legislation relating to credit reporting and to the financial sector, however, there is very little legislation of this kind. Although the *Bank Act* was amended in 1991 to empower the Governor in Council to make regulations regarding the privacy of customer information, and was again amended in 1997 to provide clearer guidance as to the contents of such regulations, no such regulations were ever enacted.[83]

In addition to specific legislation, some professions may also have ethical standards that deal in some way with personal information. For example, it would be unethical for a lawyer to disclose confidential information about his or her clients; it is even unethical to disclose the identities of those clients.[84] A breach of the ethical rules relating to confidentiality can lead to disciplinary action under the relevant legislation. Similarly, doctors operate under strict rules of confidentiality in their relationships with patients, as do numerous other health care professionals. These rules may be found in codes of conduct, legislation, or the common law,[85] or they may stem from a combination of these sources. These rules would continue to apply regardless of whether the services provided by any of these professionals constitutes "commercial activity." However, to the extent that the services fall within the scope of "commercial activity" the stricter norms would likely continue to operate alongside the rules set out in *PIPA*.[86]

Where such legislation exists, it will continue to set a higher standard for the protection of some forms of personal information, even after *PIPA* comes into effect. Thus in some sectors, the interpretation of *PIPA* will be supplemented or even superceded by pre-existing obligations with respect to personal information practices. It remains to be seen whether these rules relating to personal information will be considered too context-specific, or whether they can be used as a basis for fleshing out an understanding of the norms in *PIPA*.

It may be easier to interpret *PIPA* by looking at the interpretations of comparable legislation in other jurisdictions. Both Great Britain and New Zealand have private sector privacy legislation that predates *PIPA*. Although neither jurisdiction has

---

[83] The Canadian Bankers' Association has developed its own voluntary model code.

[84] *Canadian Bar Association's Code of Professional Conduct*, (adopted by Council August 1987). Chapter IV of the which forms the basis for the codes of conduct of provincial bar associations, sets out the basic rules regarding confidentiality in the solicitor-client relationship.

[85] See, *e.g. McInerney v. MacDonald*, [1992] 2 S.C.R. 138.

[86] *Supra* note 84 at 14. This may mean that some professionals will have to change how they approach their dealings with clients. For example, the legislation would seem to require explicit statements of certain norms and privacy practices in contexts where they were previously largely implicit. Thus, for example, assuming that the provision of legal services falls within the scope of "commercial activity," a law firm would need to be prepared, for instance, to "make readily available to individuals specific information about its policies and practices relating to the management of personal information," and must have designated an individual within the firm who is responsible for overseeing compliance with the legislation (*ibid.*).

an extensive track record with their legislation, it is possible that their experience in interpreting their own legislation may prove useful in the Canadian context. Further, Quebec's private sector privacy legislation has been in effect for more than six years, and past experience with this legislation may prove useful in interpreting *PIPA*.

D. *Sectoral Codes*

Sectoral codes are codes of practice designed to "provide detail and guidance on how legal requirements apply to a specific industry."[87] Their role in interpreting or elaborating the law may be an important one, particularly where the legislation gives them some recognition. The Task Force on Electronic Commerce, recognizing that smaller businesses were not likely to feel the need for a specific code, contemplated that larger businesses might find such devices useful: "other organizations, however, may prefer to draw on their own expertise to interpret the law as it relates directly to their line of business, and so may see value in developing sectoral codes which would supplement or replace the requirements of the law."[88] Of course, the extent to which such codes can "supplement or replace" legal requirements depends on how the law itself takes them into account.

In some jurisdictions, privacy legislation has recognized the role to be played by privacy codes developed for and tailored to the circumstances of particular industries or sectors. Where this is the case, the legislation may provide for formal recognition of these codes. Thus, in Great Britain, the *Data Protection Act of 1998* provides for approval by the Data Protection Commissioner, of codes of practice which have been proposed by trade associations.[89] Before approving a proposed code, the Commissioner is required by law to consult with persons who "represent data subjects." Following the consultative process, the Commissioner may approve the code of practice. The Commissioner also has the power, on his or her own initiative, or by direction from the Secretary of State, to draft codes of practice for particular sectors or industries, after appropriate consultation.[90] These codes of practice are meant to offer "guidance", and do not have the force of law.

In New Zealand, the *Privacy Act 1993*[91] also made allowances for the creation of codes of practice. That legislation specifically provides that, once approved, codes of practice become legally binding and enforceable documents. The codes allow for a more flexible application of the *Act* in the following manner:

> 46(2). A code of practice may –
>
> (a) Modify the application of any one or more of the information privacy principles by –
>
> (i) Prescribing standards that are more stringent or less stringent than the standards that are prescribed by any such principle;

---

[87] *Protection of Personal Information supra* note 3 at 15.
[88] *Ibid.*
[89] *Data Protection Act 1998*, (U.K.) 1998 c. 29, s. 51.
[90] *Ibid.*, s. 51(3).
[91] New Zealand *Privacy Act 1993.*

(ii) Exempting any action from any such principle, either unconditionally or subject to such conditions as are prescribed in the code;

(aa) Apply any one or more of the information privacy principles (but not all of those principles) without modification;

(b) Prescribe how any one or more of the information privacy principles are to be applied, or are to be complied with.

Thus, the legislation allows for the tailoring of the privacy principles to the needs or circumstances of particular sectors. In New Zealand, privacy codes developed in accordance with the legislation are given the force of law.[92]

Different ideas regarding sectoral codes were mooted around the time of the drafting of *PIPA*, including the possibility of some kind of approval mechanism whereby the Privacy Commissioner could sanction or adopt particular codes.[93] Prior to the drafting of *PIPA*, the Electronic Commerce Task Force noted the following:

> Privacy codes will obviously continue to play an important role within any legislated regime. The standards-registration process can relieve regulatory bodies of checking and verifying privacy code content. A system that mandates all organizations to develop privacy codes would be unnecessarily burdensome and expensive. Consequently, codes should continue to be developed as a result of market demand and consumer pressure but, only in special circumstances, in response to regulatory fiat.[94]

Even at an early stage, the preferred approach seemed to favour the voluntary drafting of sectoral codes, with a possible process for registration or approval.

Clearly the initial concept behind the CSA Model Code was that it was to be used as a model which could be followed or modified by sectors and industries as they saw fit. There is nothing to stop the development of voluntary codes which seek to adapt the principles in *PIPA* to a particular sector or industry. In fact, on a smaller scale, the *Act* specifically provides that the Commissioner shall "encourage organizations to develop detailed policies and practices, including organizational codes of practice, to comply with sections 5 to 10."[95] However, nothing in the *Act* requires the kind of public consultation which would be central to the development of a sectoral code under the British or New Zealand legislation, nor is there any provision for such a code to have a binding effect. Similarly, there is no provision for the Commissioner to actually approve or disapprove of such codes as they are drafted by particular sectors or organizations.[96]

---

[92] *Ibid.* at s. 53.

[93] *Protection of Personal Information, supra* note 3.

[94] *Regulation Privacy in Canada, supra* note 23.

[95] *PIPA, supra* note 1, s. 24(c). On the face of it, this provision seems only to be directed towards organizations, and not sectors.

[96] In *PIPA*, the Governor in Council does have a regulation-making power under s. 26(1)(*b*). The power is "for carrying out the purposes and provisions of this Part." It is unclear whether this would extend to approving sectoral codes, although to the extent that this would change the character of the legislation, it is unlikely such a power is to be contemplated.

Interestingly, the Ontario proposal for private sector privacy legislation specifically contemplates a power to develop and approve sectoral codes:

> The proposed Act would set out a rigorous and transparent process for developing or changing a sector code. The process would require participation from representatives of the sector, the public interest and experts, as necessary (such as legal, technical, academic). It would require the final approval of the government.[97]

Although not anticipating that many such codes would be drafted,[98] the proposal makes it clear that they would be a useful avenue to develop enforceable, context-specific rules "where necessary for the unique need of a sector or type of personal information."[99]

Given this situation, it is not clear what effect sectoral codes will have on the interpretation and application of *PIPA*. Possibly the degree of consultation involved, from a variety of interested parties, including the Privacy Commissioner and the general public, may have a real impact on the extent to which any such code would be allowed to set a standard for a particular sector. The Electronic Commerce Task Force certainly anticipated that sectoral codes could play a role in the interpretation and enforcement of privacy legislation. They noted:

> Privacy codes should be encouraged and they should use the CSA standard as a template. But under a legislated regime, they should not be given an official "seal of approval", nor the power to qualify the provisions of the law. However, compliance with a code approved by CSA may be taken into account by Commissioners and courts in determining whether there has been a breach of the privacy principles.[100]

This statement suggests that a body such as the CSA, rather than the privacy commissioner, should be the body which approves any sectoral codes. This may give some guidance as to what would be sufficient in order to allow a Code to have an impact on the interpretation of the legislation, and some sense of certainty to businesses which comply with CSA approved sectoral codes. However, there are no sectoral codes currently approved by CSA, and no indication that the CSA is interested in becoming involved in any kind of certification program around privacy. As one commentator has noted:

> no accredited Registrar in Canada currently has the expertise in the privacy issue to tackle the enormous variety of complex and highly technical problems that will inevitably arise. It would be necessary for the Standards Council of Canada to begin to accredit Registrars in privacy, as well as privacy auditors. Moreover, in no registration scheme can the Registrar offer the direct resolution or mediation of complaints.[101]

---

[97] *Consultation Paper*, *supra* note 13.
[98] *Ibid.*
[99] *Ibid.*
[100] *Regulating Privacy in Canada*, *supra* note 90.
[101] C. J. Bennett, "Implementing Privacy Codes of Practice" (1995) online: <http://www.privacyexchange.org/buscodes/standard/implementing.html> (last modified 22 August 2000).

Thus while sectoral codes may make good sense, there is currently no framework in place by which they can be vetted or measured against the requirements of the law. In any event, until such time as codes are drafted and approved other sources of guidance will be necessary. This is especially true for the many businesses or organizations, particularly e-businesses, for which sectoral codes are not a realistic option.

E. *Privacy Programs*

The spectre of uncontrolled personal information collection, use and disclosure in the online context was a key factor in bringing about the enactment of *PIPA*, and was also a significant factor behind calls for greater industry self-regulation in the United States. Electronic commerce is perceived by many as being a significant threat to personal privacy, and as a result, personal privacy concerns are seen as a significant threat to the success of electronic commerce.[102] In 1999, the FTC reported that:

> Eighty-seven percent of US respondents in a recent survey of experienced Internet users stated that they were somewhat or very concerned about threats to their privacy online. Seventy percent of the respondents in a recent national survey conducted for the National Consumers League reported that they were uncomfortable providing personal information to businesses online. Consumers are particularly concerned about potential transfers to third parties of the personal information they have given to online businesses.[103]

It is not surprising therefore, to see initiatives emerging which attempt to set certain standards for information privacy for online businesses. In the United States, initiatives range from guidelines such as those set by the Online Privacy Alliance,[104] to privacy policy drafting tools, and seal programs. Internationally, work is being done by the OECD to develop a privacy statement generator.[105] All of these initiatives use fair information practices as a baseline, and attempt to translate them into the online context.

---

[102] *The Protection of Personal Information*, *supra* note 3. See also U.S.A., *Self Regulation and Privacy Online: A Report to Congress* (Federal Trade Commission, 1999) (Chair: R. Pitofsky), online: Federal Trade Commission <http://www.ftc.gov/os/1999/9907/privacy99.pdf> (date accessed: 10 November 1999) [hereinafter *Self Regulation*].

[103] *Ibid.* at 2. In a recent study of commercial websites, the OECD Group of Experts on Information Security and Privacy found the following: "At least one third of the sites surveyed are not very explicit about the data collected, and over half do not address the question of clickstream data and the processing to which they are subject. Another third of the sites do not provide opt-out possibilities or a right of access. Lastly, almost one-quarter of the sites surveyed do not give any physical address permitting the visitor to know something about who he is dealing with in order to seek redress through traditional forms of communication, if necessary." *Supra* note 71 at 16.

[104] The Online Privacy Alliance (OPA) (Online: http://www.privacyalliance.org) is a coalition of industry groups which produced, in 1998, a set of guidelines for the online collection of personal information. The OPA does not offer a seal program. However, their guidelines have formed a basis for other seal programs. See *Self Regulation*, *supra* note 102 at 9-11.

[105] This tool was launched at the end of July 2000. Online: <http://www.oecd.org/scripts/PW/PWHome.ASP>.

For Canadian e-businesses, especially those with limited resources, the attraction of adaptable, pre-packaged privacy policies is obvious. First, *PIPA* provides only very general guidance, and is not well-tailored to the context of e-business. Private sector privacy initiatives would enable businesses to more easily create and adopt privacy policies tailored to their particular circumstances. Seal programs go a step further by offering a "stamp of approval" from a third party organization. However, because the American and OECD tools are not based on the specific provisions of *PIPA*, they may not fully satisfy the requirements of that law. Be that as it may, such models may be important in establishing certain consistent practices in the online environment which may in turn become relevant to the interpretation and application of *PIPA* in that context.

1. *Seal Programs*

A number of online privacy programs have emerged in the United States, largely because of the early decision to opt for self-regulation as opposed to legislation for privacy protection.[106] The most significant of these initiatives has been the use of seal programs, which set guidelines for privacy policies, review and monitor compliance with the guidelines and offer some form of seal or mark to identify "approved" sites.[107] TRUSTe[108] is one of the most well-known seal programs,[109]as is BBBOnLine,[110] but programs of this kind are also emerging tailored to the needs of specific sectors or industries.[111] Such programs may also provide private dispute resolution mechanisms.

---

[106] This may now be changing. In May 2000 the Federal Trade Commission, in its Report to Congress, recommended that, in light of widespread noncompliance with voluntary self-regulation, legislation be enacted to guarantee consumer privacy online. The FTC noted that "[o]ngoing consumer concerns regarding privacy online and the limited success of self-regulatory efforts to date make it time for government to act to protect consumers' privacy on the Internet. Accordingly, the Commission recommends that Congress enact legislation to ensure adequate protection of consumer privacy online. In doing so, however, the Commission recognizes that industry self-regulation, as well as consumer and business education, should still play important roles in any legislative framework, as they have in other contexts"; *supra* note 18 at 36.

[107] Even so, the May 2000 report of the Federal Trade Commission, notes that "[a]lthough the number of sites enrolled in these programs has increased in absolute terms since last year, the seal programs have yet to establish a significant presence on the Web": *supra* note 18 at 6. Further, in their 2000 survey of websites, the FTC found that "less than one-tenth, or approximately 8%, of sites in the Random Sample display a privacy seal": *ibid.* at 20. Perhaps more significantly, they found that not all of these seal-bearing sites actually implemented all four of the fair information practices identified by the FTC. *(ibid.)*.

[108] Online: TRUSTe Homepage <http://www.truste.org> (date accessed: 7 November 2000).

[109] Another example of a seal program is PriceWaterhouseCoopers BetterWeb program which can be found online at <http://www.pwcbetterweb.com/betterweb>.

[110]The Better Business Bureau Online Homepage Line Homepage can be found at <http://www.bbbonline.org/businesses/privacy/index.html>.

[111] CPA WebTrust has a privacy component to its program which is designed to assist Certified Public Accountants meet uniform standards around business practices, including information privacy (online: <http://www.cpawebtrust.org/>). The Entertainment Software Rating Board has also come up with its own privacy seal program for the entertainment software industry (online: <http://www.esrb.org>).

Begun by a small group of interested "pioneers" in e-commerce, TRUSTe began with a pilot program launched in 1996. It has since developed into a full blown privacy program.[112] TRUSTe is probably the highest profile[113] privacy certification site in the United States. Businesses seeking to be certified under the TRUSTe program must complete a self-assessment, draft a privacy statement according to a set of guidelines provided, and submit the materials to be reviewed by TRUSTe, along with their business web site. Upon review of the web site, TRUSTe may ask for changes to be made in order to comply with the guidelines. A business which is successful in having its statement approved will receive a TRUSTe trustmark and a "Click to Verify Seal." These marks will inform visitors to the site that the privacy policy and practices of the business have conformed to TRUSTe standards. TRUSTe also engages in third party monitoring and periodic reviews of licensed sites. These reviews can be quite extensive, and include reviews of changes to privacy statements as well as tracking of compliance with customer information-management requests.[114]

TRUSTe sets out privacy principles that are in many ways similar to those contained in *PIPA*. Disclosure of information gathering practices is required, as is information about what the information is used for and to whom it may be provided. Businesses must state whether information being collected must be provided, or can be provided at the user's option. Rather than refer to consent, TRUSTe refers to "choice." Users of the site must be informed of what choices they have regarding the collection, use and disclosure of their information. They must be given an opportunity to "opt-out" of any information collection or disclosure which is not directly necessary to the provision of the service.[115] The statement must also deal with issues such as correction of information, access to information, and security. There must also be provision made for notification of users of any changes in privacy policies.

In some ways, TRUSTe is a more useful tool than *PIPA* for online businesses. The TRUSTe guidelines address issues which were likely not even contemplated at the time the CSA Model Code was drafted. The definition of personally identifiable information is very broad (and much more explicit than that contained in *PIPA*).[116] As a result, it directly anticipates online modes of information gathering and the potential for creating personally identifiable information through processes such as online profiling. The statement addresses the use of cookies as a means of gathering

---

[112] Online: TRUSTe Homepage <http://www.truste.org/about/about_truste.html> (date accessed: 7 November 2000).

[113] The Federal Trade Commission notes that TRUSTe now has more than 1200 licensees across a range of industries. "Privacy Online," *supra* note 18 at 6.

[114] In spite of this, there have been criticisms of the effectiveness of seal programs. One critic notes that "it is procedurally quite difficult for consumers to bring a complaint against a web site, and have that complaint speedily resolved:" C. D. Hunter, "Recoding the Architecture of Cyberspace Privacy: Why Self-Regulation and Technology are not Enough," (February 2000), online: Christopher D. Hunter Homepage <http://www.asc.upenn.edu/usr/chunter/net_privacy_architecture.html> (date accessed: 10 November 2000). Further, the same source states that "even more troubling than this burdensome resolution process, is the fact that TRUSTe has repeatedly found ways to allow member websites to wiggle out of their contractual obligation to abide by their posted privacy policies,"(*ibid.*).

[115] This would seem to indicate that TRUSTe also accepts a negative option approach to information collection.

[116] The full text of the TRUSTe definition is reproduced *supra* note 51.

information, and requires disclosure about the use of cookies, and the ways in which information gathered through cookies will be used. The statement also addresses log files, frames, and co-branding of mirror sites, all issues which were likely not in the contemplation of the drafters of the CSA Code. Further, TRUSTe has specific requirements for sites which are directed at children under the age of thirteen.[117] TRUSTe provides a format for a privacy statement that suggests providing information about links to other sites, and the handling of information provided in chat rooms, forums and message boards. It also deals with the impact of mergers and acquisitions on personal information held by the merging companies.[118]

While TRUSTe provides a useful model for e-businesses (and certainly one which is more context-specific than *PIPA*), the extent to which it becomes an accepted model in Canada may raise concerns. It may well be that Canadian law should, in some circumstances, hold out for higher privacy standards than those set out in TRUSTe. For example, the guidelines require that "[t]he privacy statement must be one click away from the homepage."[119] This is required to avoid the "burying" of the statement within the site; however, it does not go so far as to require that the privacy statement be linked from the page or pages where information is gathered, which may be the better approach from a privacy perspective. *PIPA*, of course, is unclear on the subject. It requires that "[t]he purposes for which personal information is collected shall be identified by the organization at or before the time the information is requested." A privacy policy linked from the homepage could be said to provide the statement of purposes "before the time the information is requested"[120] In fact, principle 4.3.2 merely requires organizations to "make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used."

There are problems with having a privacy link from the homepage. Many privacy links placed on homepages are at the bottom of the page. It may be necessary to scroll down to see the link, even where it is possible to enter the site and begin shopping without scrolling down to the bottom of the page. Also, without font, colour and size restrictions, the visibility of any link to a privacy statement may also be an issue. Of course, to the extent that linking from the homepage becomes a more standard practice, there may be a growing consumer awareness of where to find privacy policies, thus rendering the issue less of a concern. Nevertheless, the question remains whether Canadian law should require greater visibility of privacy policies at the point of

---

[117] This is because the United States has legislation dealing specifically with this issue. See The *Children's Online Privacy Protection Act of 1998*, 15 U.S.C. SS 6501 *et. seq.* This law was enacted to deal specifically with the vulnerability of children's personal information in the online context.

[118] This issue is increasingly important, as many online businesses face mergers, acquisitions, or even bankruptcy, as fortunes shift in the volatile world of e-business. See B. McKenna, "E-tailer shakeout punctures privacy" *The Globe and Mail* (20 July 2000) T1.

[119] Online: TRUSTe Homepage <http://www.etrust.com/webpublishers/pub_sitecoordinatorsguide.html> (date accessed: 7 November 2000).

[120] However, the consent provision seems to require consent to collection or use to be sought at the time of collection (see paragraph 4.3.1.) As noted earlier, however, the consent principles are infinitely malleable, so it is far from clear whether they would require notice of purposes to be much more closely linked to the collection of the information in order for an informed consent to be deemed to have been given.

collection of information, rather than at a point potentially quite far removed from the collection. Certainly BBBOnLine takes a different approach than TRUSTe. In its sample privacy notice, it states: "[t]o make this notice easy to find, we make it available on our homepage and *at every point where personally identifiable information may be requested.*"[121] In addition, the FTC is of the view that "links to a privacy policy, as well as discrete and relevant information practice disclosures, should be prominently displayed on a site's homepage and *on every page on which personal information is collected.* Without clear and understandable information practice disclosures, it is unlikely that consumer concerns regarding online privacy will abate."[122]

Although not inconsistent with *PIPA*, this example of the privacy policy linked from the homepage illustrates the risk which exists with models such as TRUSTe. Acceptance of a recognized initiative such as TRUSTe may mean that having the only link to the privacy policy from the homepage may emerge as a standard which will influence the interpretation of *PIPA*. More thought needs to be given to whether this is an appropriate standard.[123] Nevertheless, the value of initiatives such as TRUSTe and BBBOnLine is clear, and they are likely to have an influence in developing standards of practice in online business. The leading seal programs are American, however, leaving the Canadian Privacy Commissioner and the provisions of *PIPA*, with little active role to play in the development of these particular norms for privacy in online commerce.

2. *Privacy Statement Generators*

Some technological devices aimed at assisting in the protection of online privacy are currently under development. The development of these software tools, which include the Platform for Privacy Preferences Project (P3P), and the OECD Privacy Statement Generator, is largely spurred by the absence of privacy legislation in, most significantly, the United States. The tools are thus aimed, in theory at least, at improving privacy by both encouraging businesses to develop and post privacy policies, and by raising consumer awareness of privacy issues.

(a) *Platform for Privacy Preferences Project*

---

[121] Sample Privacy Notice, online: BBBOnLine Homepage <http://www.bbbonline.org/privacy/sample_privacy.asp> (date accessed: 7 November 2000) (emphasis added).

[122] "Privacy Online," *supra* note 18 at 27-28 (emphasis added). The OECD in its Privacy Policy Statement Generator documentation recommends that: "In the absence of specific regulatory requirements, you may wish to consider creating a link between your homepage and your privacy statement, or between pages where you collect personal data and your privacy statement." (online: Organisation for Economic Co-Operation and Development Homepage <http://cs3-hq.oecd.org/scripts/pwv3/pwpart1.htm> (date accessed: 7 November 2000).

[123] In a recent report, the OECD Group of Experts on Information Security and Privacy found that the location of privacy policies on websites did present a serious issue. They found that locating a privacy policy "is easy on a little over half the sites looked at in the study, but it is more complicated on at least ten of them, where it takes a fairly long time to find the privacy statement. For some sites it is even necessary to be quite far advanced in a registration process or in a transaction–i.e. the user has to have started to transmit personal data–before a link with the site s provisions regarding personal data and privacy appears." *Practices to Implement the OECD Privacy Guidelines*, *supra* note 71 at 15.

The Platform for Privacy Preferences Project, or P3P, has been developed by the World Wide Web Consortium[124] to serve as "an industry standard providing a simple, automated way for users to gain more control over the use of personal information on Websites they visit."[125] Essentially, P3P is a standard designed to be implemented in web browsers. To operate successfully, it first requires that businesses draft their privacy policies using a standardized set of machine-readable fields. Users of browsers equipped with P3P would in turn configure their browsers to identify their privacy preferences.[126] When surfing the web, the user's browser would "read" the privacy policies of the sites which the user seeks to visit. The browser then informs the user of the basics of the privacy policy of the web site, and shows how they compare to the user's stated preferences.

P3P has been fairly extensively criticized.[127] Some critics argue that the framework results in a gross oversimplification of privacy policies. This oversimplification may mislead users as to the actual uses that will be made of their personal information.[128] Others are concerned that P3P may also give users a false sense of security, as it does not involve any form of oversight to ensure that companies actually comply with their stated policies.[129] Still other critics raise concerns that without widespread adoption of the technology by commercial websites and web users,

---

[124] The World Wide Web Consortium, or W3C, is a voluntary amalgamation of enterprises and organizations which are interested in standardizing WWW technologies." Rudiger Grimm & Alexander Rossnagel, P3P and the Privacy Legislation in Germany: Can P3P Help to Protect Privacy Worldwide?" Institute for Secure Telecooperation, (August 2000) at 1, online: Institute for Secured Telecooperation <http://sit.gmd.de/~grimm/texte/P3P-Germany-e.pdf> (last modified: August 2000).
The companies involved in the development of P3P include some of the major players in the software, hardware and Internet industries, such as Microsoft, Netscape, America Online, IBM and TRUSTe. While the group includes mostly corporations, the Ontario Office of the Information and Privacy Commissioner has participated, as has the Privacy Commission of Shleswig-Holstein in Germany.

[125] World Wide Web Consortium, Platform for Privacy Preferences (P3P) Project, "What is P3P?", online: <http://www.w3.org/P3P/> (last modified: 6 November 2000).

[126] The developers of P3P initially hoped that organizations such as the Better Business Bureau would develop recommended downloadable browser settings for P3P that users could adopt for their browsers. This may not happen as one commentator notes that: few or no organizations will have the resources to develop comprehensive and trusted privacy templates." (Hunter, *supra* note 114). Hunter goes on to suggest that perhaps companies like Microsoft and Netscape do have the resources to develop privacy templates, but states: considering that both of these companies generate significant revenue from online advertising, and have a less than stellar record with cookies (both browsers accept them by default), it is likely that their P3P templates would strongly favor industry interests, and therefore garner little trust among users"(*ibid.*).

[127] See *e.g.* Jason Catlett, Open Letter 9/13 to P3P Developers" (13 September 1999). Online: <http://www.junkbusters.com/standards.html> (date accessed: 8 November 2000).

[128] Some critics raise the concern that P3P merely codes industry's view of privacy, and thus actually makes it harder for users to protect themselves." (Hunter, *supra* note 114).

[129] Karen Coyle notes: It oversimplifies and quite possibly misrepresents the trust interaction, and always in favor of the web site that is asking for an individual s information." Karen Coyle, P3P: Pretty Poor Privacy?: A Social Analysis of the Platform for Privacy Preferences (P3P)" (June 1999), online: <http://www.kcoyle.net/p3p.html> (last modified: 1 November 2000).

it will not make a significant difference to the privacy practices of e-businesses.[130] Because the U.S. approach to date has been towards self-regulation, it is important to note that most of these criticisms come from a context where there are no legislated norms, no oversight mechanism, and no means by which rights can be enforced. Proponents of P3P stress that it should not be assessed as the sole form of privacy protection, but rather as one tool in a privacy framework that would include legislation.[131]

It is not clear whether P3P would have any impact at all on the interpretation of the privacy principles set out in *PIPA*. It is not even clear if P3P will be widely adopted. Assuming that it is, it would not supplant the obligations of Canadian web site operators to comply with the provisions of *PIPA*[132]. It is, conceivable, perhaps, that the implementation of P3P on a web site, would satisfy the requirement of openness.[133] However, it is less clear, should P3P become a widely used standard, whether a Canadian web site that did not adopt P3P would risk running afoul of the openness principle of *PIPA* on the basis that users would expect to be able to access privacy information in this manner.[134] While this is possible, it would certainly not be desirable, given some of the criticisms of P3P.[135] Although offering some potential benefits for Canadians engaging in out-of-country electronic commerce, P3P is not likely to have a significant effect in shaping the interpretation of Canada's privacy legislation.

(b) *OECD Privacy Policy Statement Generator*

---

[130] See Deirdre Mulligian, *et al.*, "P3P and Privacy: An Update for the Privacy Community." Center for Democracy & Technology, 28 March 2000. Online: <http://www.cdt.org/privacy/pet/P3pprivacy.shtml> (date accessed: 6 November 2000).

[131] For example, in Mulligan, *et al.*, *ibid.*, one source notes "[i]n our opinion, P3P does not protect privacy, in and of itself. It does, however, help create a framework for informed choice on the part of consumers. Any efficacy that P3P has is dependent upon the substantive privacy rules established through other processes, be they a result of regulatory, self-regulatory or public pressure."

[132] An assessment of the impact of P3P in Germany, which has private sector privacy legislation, is that P3P complements privacy protection law . . . P3P provides technical support to some but not all legal requirements." Grimm and Rossnagel, *supra* note 120 at 4.

[133] See *PIPA*, Sch. 1, para. 4.8. This principle requires that "[a]n organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."

[134] See *PIPA*, Sch. 1, para. 4.8.1 which states that [i]ndividuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable." One of the objectives of P3P is to make privacy information easily accessible, and in a simplified form. Arguably, if P3P were a widely used standard, this might be what web users would come to expect.

[135] The oversimplification of privacy information would most likely lead to a degrading of the level of personal information privacy offered to consumers. Of course, as noted earlier, the twin objectives of *PIPA*, to protect privacy and to promote electronic commerce, raise questions as to whether privacy protection principles would be interpreted with a view to facilitating or promoting electronic commerce.

The OECD's Privacy Policy Statement Generator (PPSG)[136] is a free, publicly accessible tool designed to assist online businesses in drafting privacy policies that comply with the OECD's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.*[137] Like P3P, PPSG is a technological tool aimed at facilitating the preparation of a privacy policy. Unlike PPSG, it does not have a user component that would make the generated policy machine readable. The PPSG provides a lengthy questionnaire about a company's privacy policies, as well as extensive background materials to assist web site developers in understanding and answering the questions. The questionnaire can be answered, for the most part, by simply clicking off check-boxes next to particular answers. Users are prompted if they fail to answer a question which is required to complete the privacy statement. Once the questionnaire is completed, the PPSG will generate a privacy policy in HTML which will presumably fit the needs and circumstances of the user. The policy generated will redline any answers which are inconsistent with the OECD Guidelines. This notification gives the user the opportunity to revise the statement in order to bring it into conformity with the privacy principles. Redlining, however, can be removed by the user, who can then post the policy without amendment.

The questionnaire format of the PPSG is likely to be useful in encouraging the creation and posting of web site privacy policies. However, it is a fairly rigid format, and it is still unclear whether sufficient flexibility will be built into the tool to make it widely useful. The statement generated is based on user answers, and may not conform to the OECD guidelines, let alone any relevant national laws. As a result, the OECD does not "certify" any statements created using PPSG, although statements generated in this way can refer to the OECD generator and link to it.

As with P3P, the PPSG is likely to be of limited usefulness in relation to interpreting and complying with *PIPA*. Although the CSA Model Code draws heavily on the OECD Guidelines, the provisions of that Code, incorporated into law, are nonetheless different in some respects. Canadian businesses would be expected to comply with the terms of *PIPA*, and not simply with the OECD guidelines. It is unclear at this point how many Canadian users would make use of the PPSG, and it is also unclear whether PPSG will have any significant role in shaping the understandings or expectations of either consumers or businesses in relation to online privacy.

IV. CONCLUSION

As a result of the way in which it has been drafted, with the adoption of the entire CSA Model Code as the normative heart of the legislation, *PIPA* is an unwieldy tool for the protection of personal information. Problems of interpretation are exacerbated by the fact that *PIPA* is also meant to apply across an almost impossibly broad range of commercial activity. Nevertheless, over the next few years it will become the law against which personal information protection in the private sector will be measured. Much work remains to be done in interpreting the legislation and applying its principles in a manageable and accessible way for both individuals and organizations.

---

[136] The Privacy Policy Statement Generator was released in late July 2000, and is available at: http://CS3_HQ.oecd.org/scripts/pwv3/pwhome.htm. The PPSG has been endorsed by the member countries of the OECD, of which Canada is one.

[137] *Supra*, note 19.

As diverse nations grapple with the twinned problems of protecting personal data and facilitating electronic commerce, different tools have emerged which may help shape approaches to understanding and applying the key provisions of *PIPA*. These range from more traditional legal sources such as similar legislation, to less formal sources such as sectoral codes. In addition, a range of new tools are emerging to grapple with personal privacy issues, particularly in the online context. Seal programs, and their guidelines for privacy protection, may play a role in shaping understandings of what is "reasonable" industry conduct, while P3P is an attempt to mediate between the desire of industry to obtain personal information and the attempts of individuals to maintain a certain level of personal privacy.

If there is one lesson to be learned from the range of other tools and instruments which address personal information privacy issues, it is that perspective is all important. Some tools, such as TRUSTe and P3P clearly adopt a business-oriented perspective to personal information. Other approaches, such as those in the British and New Zealand legislation, call for broader consultation and citizen involvement. The orientation of *PIPA* towards facilitating e-commerce, and the lack of public consultation mechanisms for the development of sectoral practices may raise concerns that the interpretation of *PIPA* will be unduly shaped by industry and commercial interests. In this respect, the role of the Privacy Commissioner as the "reasonable individual" will be crucial. Unfortunately, there is little room within the framework of the legislation for reasonable individuals to shape or influence the perspective of their official surrogate.