

Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices

Lisa M. Austin

Version Publisher's version

Citation (published version) Austin, Lisa M., Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices (2006). Canadian Business Law Journal, Vol. 44, p. 21, 2006. Available at SSRN: <https://ssrn.com/abstract=1169162>

Publisher's Statement Reproduced from the Canadian Business Law Journal: "Austin, Lisa M., Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices (2006). Canadian Business Law Journal, Vol. 44, p. 21, 2006."
By permission of Thomson Reuters Canada Limited.

How to cite TSpace items

Always cite the published version, so the author(s) will receive recognition through services that track citation counts, e.g. Scopus. If you need to cite the page number of the **author manuscript from TSpace** because you cannot access the published version, then cite the TSpace version **in addition** to the published version using the permanent URI (handle) found on the record page.

This article was made openly accessible by U of T Faculty.
Please [tell us](#) how this access benefits you. Your story matters.



REVIEWING PIPEDA: CONTROL, PRIVACY AND THE LIMITS OF FAIR INFORMATION PRACTICES

*Lisa M. Austin**

I. INTRODUCTION

The federal Personal Information Protection and Electronic Documents Act (PIPEDA), introduced in 2001, provides individuals with a certain degree of control over their personal information by imposing a number of obligations on organizations that collect, use and disclose that information.¹ These obligations include informing individuals regarding the purposes for which their personal information is collected, used, or disclosed and requiring individuals to consent to these practices. Other obligations include requirements that the collection, use, disclosure and retention of personal information is limited, that its accuracy is ensured, and that this information is protected by appropriate security. Organizations are required to be transparent about their information management practices, to have an accountability structure in place, and to ensure that individuals can get access to this information and are able to challenge an organization's compliance with its obligations.² These obligations form the core of what are often referred to as "fair information practices" and are a crucial component of any contemporary legal response to the challenges posed by proliferating information and communications technology.

Parliament is scheduled to review PIPEDA in 2006 and determine whether any changes to its provisions or administration are warranted.³ In order to review the effectiveness of PIPEDA, this article will pose the

* Faculty of Law, University of Toronto. This paper was originally presented at the 35th Annual Workshop on Commercial and Consumer Law University of Toronto, October 22, 2005. Its redrafting has benefited from the comments of my co-panelists at the Workshop (Jennifer Stoddart, Drew McArthur, Ian Kerr and Mahmud Jamal) as well as from members of the audience and a number of helpful comments from Joe Murray.

1. S.C. 2000, c. 5 (hereafter PIPEDA).
2. *Ibid.*, Schedule 1.
3. *Ibid.*, s. 29.

following questions. First, what is the problem, or problems, that control over personal information is meant to solve? Second, does the model of data protection embodied in PIPEDA and administered and enforced through the Office of the Privacy Commissioner of Canada and the federal courts solve these problems?

In response to the first question, this article argues that control over personal information is meant to provide individuals with informational privacy. However, an examination of the relationship between control and privacy highlights the following issues: that control over personal information might protect a broader set of values than simply privacy; that individual informational privacy might be protected even in the absence of individual control; that determining the scope of the legal entitlement to control over personal information requires an understanding of the values that privacy is meant to protect and a balancing of these against legitimate claims of others in a principled manner; and that control will only provide meaningful privacy protection if individuals are presented with meaningful choices regarding privacy options.

Understanding these issues helps answer the second question, regarding the effectiveness of PIPEDA in solving the problem of privacy, for they permit a number of problems with PIPEDA to come into focus. These include the all-or-nothing approach to PIPEDA's Schedule 1 obligations; the need for a more nuanced approach to the scope of individual control over personal information and the role of implied consent in providing this; the desirability of an Ombudsman model; and whether PIPEDA's provisions can require that meaningful privacy choices be presented to individuals. After examining these problems in detail, through discussing the threshold issue of determining "personal information", the issue of implied consent, and the question of whether consumers should have to pay more for enhanced privacy, this article offers a number of recommendations regarding both the interpretation of the act as well as possible legislative amendments.

II. CONTROL AND PRIVACY

If the first question is what is the problem, or problems, that control over personal information is meant to solve, then the most straightforward answer is: the protection of informational privacy, which is under threat from proliferating information and communications technology and the data-mining practices that have ensued.

This answer is supported by the text of the act. For example, s. 3 states:

The purpose . . . is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

In other words, the legislation seeks to facilitate an organization's information practices in a manner that is protective of individual privacy. This answer is also supported by the public rhetoric surrounding the act, in which the principles of Schedule 1 are referred to as "privacy principles" and the legislation itself as "privacy legislation" which is enforced by the Privacy Commissioner of Canada.⁴

Nonetheless, despite this clear signal that control over personal information protects privacy, it should be kept in mind that the "privacy principles" that form the core obligations under the act are modeled on the "fair information practices" that found one of their earliest, and most influential, articulations in the 1980 Organization for Economic Co-operation and Development (OECD) Privacy Guidelines.⁵ These guidelines speak of protecting both privacy and "individual liberties".⁶ There is the possibility, therefore, that in constructing the answer to the first question by drawing a link between control over personal information and *only* privacy rather than both privacy and other values, we overlook important elements in our analysis of the effectiveness of PIPEDA. In fact, in later sections this article will argue that more attention needs to be paid to these other values in order to meet existing and emerging challenges.

Even if we take privacy as the answer to our question regarding the problem that control over personal information addresses, further refinements are required before answering the second question regarding the effectiveness of PIPEDA. Specifically, we need ask: *how* does the control over personal information protect privacy and what is the relationship between individual control over

4. See, for example, materials on the website of the Office of the Privacy Commissioner of Canada: <http://www.privcom.gc.ca/index_e.asp> (accessed October 2, 2006).

5. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Annex to Recommendation of the Council, September 23, 1980.

6. *Ibid.*, ss. 2, 3(b), 6.

personal information and the legitimate interests of others in using this information?

Many privacy theorists define privacy as control over personal information. For example, Alan Westin's influential work on privacy defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".⁷ Similarly, Charles Fried has argued that privacy "is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves".⁸ If one accepts such a definition, then it appears straightforward to argue that providing control over personal information ensures that individuals have informational privacy.

However, there are many problems with such definitions of privacy. I have outlined these in more detail in previous works, but will summarize some of the issues here briefly.⁹ Although control over personal information might in fact protect privacy in many circumstances, equating control with privacy as a definitional matter is unpersuasive. Control is not a sufficient condition for the protection of privacy, as individuals may be provided with control and consequently choose to give up their privacy.¹⁰ Because it makes sense to say that people can choose different levels of privacy, privacy must have some meaning that is independent of the notion of control. Neither is control a necessary condition for the protection of privacy, as there may be circumstances in which it makes sense to say that individuals do not have control over their personal information but their privacy is nonetheless respected.¹¹ For example, an organization might choose to limit its collection of personal information. This does not provide individuals with greater control over their information but does enhance their privacy. Therefore, providing control over personal information does not necessarily

7. Alan Westin, *Privacy and Freedom* (New York, Atheneum, 1967), p. 7.

8. Charles Fried, "Privacy" (1968), 77 *Yale L.J.* 475 at p. 482.

9. Lisa M. Austin, "Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA" (2006), 56 *U.T.L.J.* 181.

10. Anita Allen, "Privacy-as-Data Control: Conceptual, Practical and Moral Limits of the Paradigm" (2000), 32 *Conn. L. Rev.* 861. See also Ruth Gavison, "Privacy and the Limits of Law" (1980), 89 *Yale L.J.* 428.

11. See also W.A. Parent, "Recent Work on the Concept of Privacy" (1983), 20 *Am. Phil. Q.* 341 at p. 344 and W.A. Parent, "Privacy, Morality, and the Law" (1983), 12 *Phil. & Publ. Aff.* 269 at pp. 272-74.

ensure that individuals have informational privacy and providing no control does not necessarily entail a lack of informational privacy.

Even if we accept a definition of privacy as control over personal information, we are left with the question of when someone should be *entitled* to this control. That is, when is control over personal information justified not simply as a social or moral norm but as a matter of a legally enforceable right? Answering this question requires an understanding of why we value privacy, whether in its own right or because of the other types of interests that it promotes, what kinds of legitimate interests others might have in information about us, and how these are to be balanced in a principled manner.

Finally, control over personal information will only provide illusory privacy protection if individuals are not given meaningful choices with respect to their information. For example, if the only way that an individual can obtain some services is to provide information for a credit check, then the choice between services or no services is not one that provides an individual, in our society, with meaningful control over the use of their personal information. In particular, individuals must be given real opportunities to remain anonymous rather than to contribute to the ever-expanding trail of information that is recorded and stored regarding so many of our activities.

In summary, even if we accept that providing control over personal information is an important way to protect individual informational privacy, we need to be cognizant of four points. First, control over personal information might protect a broader set of values than simply privacy. Second, individual informational privacy might be protected even in the absence of individual control. Third, determining the scope of the legal entitlement to control over personal information requires an understanding of the values that control is meant to protect and a balancing of these against legitimate claims of others in a principled manner. Fourth, control will only provide meaningful privacy protection if individuals are presented with real choices regarding privacy options.

With this in mind, this article will argue that PIPEDA suffers from a number of defects, both interpretive and structural, that have their roots in these issues regarding the relationship between control and privacy. Understanding these defects, however, requires a brief overview of the act and the highlighting of some of its key features and their relation to these issues.

III. OVERVIEW OF PIPEDA

PIPEDA applies to private sector organizations that collect, use or disclose personal information in the course of commercial activities or where personal information is about an employee and is collected, used or disclosed in connection with the operation of a federal work, undertaking or business.¹² Personal information is defined as "information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization".¹³

If an organization is caught by these threshold questions regarding the applicability of the act, then s. 5(1) requires that it comply with the obligations set out in Schedule 1 of the act. This Schedule incorporates the CSA Model Code for the Protection of Personal Information (the Model Code).¹⁴ The Model Code includes ten principles: Accountability; Identifying Purposes; Consent; Limiting Collection; Limiting Use, Disclosure, and Retention; Accuracy; Safeguards; Openness; Individual Access; and Challenging Compliance.¹⁵ These obligations are further qualified by s. 5(3) of the act, which provides that "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."

There are a number of exemptions to the applicability of these obligations. For example, the act does not apply at all where personal information is collected for personal, domestic, journalistic, artistic or literary purposes.¹⁶ Even where the act does apply, personal information may be collected, used or disclosed without the knowledge or consent of the individual if the conditions of one of the exemptions outlined in s. 7 of the act are met. Under the provisions of s. 7, personal information may be collected without the knowledge or consent of an individual for a number of reasons, including law enforcement purposes, when the collection is in the

12. PIPEDA, *supra*, footnote 1, ss. 4(1)(a), 4(2)(a), 4(1)(b).

13. *Ibid.*, s. 2(1).

14. CAN/CSA-Q830-96. The schedule does not include the Model Code's overview or definitions. Drafters of the legislation made the unusual decision to incorporate this Model Code rather than translate it to conform more readily to the standards and conventions of legal drafting. For a discussion, and justification, of this decision, see Stephanie Perrin, Heather H. Black, David H. Flaherty, and T. Murray Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto, Irwin Law, 2001), p. 61.

15. PIPEDA, *supra*, footnote 1, Schedule 1.

16. *Ibid.*, ss. 4(2)(b) and (c).

best interests of the individual, when the collection is for journalistic, artistic or literary purposes, or where the information is publicly available.¹⁷ Personal information may be used without the knowledge or consent of an individual for similar purposes as in the case of its collection, as well as for the purposes of research if such research can only be undertaken with this information, it is impracticable to obtain consent, and the Privacy Commissioner is informed before the information is used.¹⁸ Finally, personal information may be disclosed without the knowledge or consent of an individual for a number of law enforcement and national security purposes, in order to collect debts, in emergency situations, and for research or archival purposes.¹⁹

The model of administration embraced by the act is largely an Ombudsman model, with the Privacy Commissioner of Canada as the ombudsman.²⁰ An individual may file a complaint with the Privacy Commissioner (the Commissioner) against an organization that may be contravening the act.²¹ The Commissioner attempts to resolve such complaints through negotiation and voluntary compliance but, if this is not successful, has a number of powers under the act including the power to summon witnesses, administer oaths, and compel the production of evidence.²² Within a year of filing of a complaint, the Commissioner is required to prepare a report outlining the Commissioner's findings. However, and notably, these findings are not binding on the parties and do not have any precedential value. Moreover, these findings are only partially made public: it has been the practice of the OPC only to issue publicly "summaries" of its findings and to do so without naming the parties involved. This practice appears to be rooted in s. 20 of the act, which requires the Commissioner to maintain confidentiality unless it is in the public interest to make public the personal information management practices of an organization.

17. *Ibid.*, s. 7(1)(a) to (d). Note that under s. 7(1)(d) information must be both publicly available and specified by the regulations.

18. *Ibid.*, s. 7(2)(a) to (d).

19. *Ibid.*, s. 7(3) (a) to (i).

20. The role of the Privacy Commissioner with respect to PIPEDA, in contrast to the Privacy Act, in some respects does not follow the classic legislative ombudsman model, which traditionally deals with citizen-government disputes. See Mary A. Marshall and Linda C. Reif, "The Ombudsman: Maladministration and Alternative Dispute Resolution" (1995), 34 *Alta. L. Rev.* 215.

21. PIPEDA, *supra*, footnote 1, at s. 11(1). The Commissioner may also initiate a complaint: s. 11(2).

22. *Ibid.*, at s. 12.

After receiving a report from the Privacy Commissioner, an individual may apply to the Federal Court for a hearing.²³ It is the court that has the power to order remedies, including ordering an organization to comply with the act and to award damages to the complainant.²⁴

From this brief overview, and in light of the previous discussion regarding the relationship between control and privacy, a number of potential problems can be identified. Two of the issues identified above were that control over personal information might protect a broader set of values than simply privacy and that individual informational privacy might be protected even in the absence of individual control. These raise questions regarding the all-or-nothing approach that PIPEDA takes with respect to engaging the obligations found in Schedule 1. That is, once an organization meets the threshold requirements for engaging the act, it is required to comply with all ten principles. However, as will be outlined below, there are circumstances in which it makes sense to require compliance with only a subset of these principles where compliance with the entire schedule is seen as inappropriate and yet compliance with none of it is inadequate. This more limited compliance might be appropriate in order to protect values other than privacy or in instances where privacy is adequately protected through adherence to some of the obligations but overprotected by adherence to all of the obligations.

Another issue identified with respect to the relationship between control and privacy is that the idea of control does not provide the conceptual resources with which to determine the scope of the legal entitlement of control. As consent is seen to be at the core of what it means to give individuals control, the question of the scope of control is often a question of when consent is required and what form this consent should take. PIPEDA ostensibly answers this question by providing individuals with the right to consent to the collection, use and disclosure of their personal information when it is used in commercial contexts, unless one of the statutory exemptions found in s. 7 is met. However, there may be a number of contexts, not covered by the exemptions in s. 7, in which it is nevertheless not appropriate to require explicit consent. As the following sections argue, there is a need for a more nuanced

23. *Ibid.*, at s. 14.

24. *Ibid.*, at s. 16.

balancing between individual privacy interests and the legitimate needs of organizations in their information management practices than the explicit structure of PIPEDA permits. Because of this, a number of problematic interpretations of key provisions of the act have emerged in an effort, often implicit, to get around the consent provisions. In some decisions this has resulted in restrictive interpretations of important threshold questions such as the meaning of "personal information". In other decisions, it has resulted in the avoidance of the requirement of consent through problematic interpretations of the consent provisions themselves. Later sections of this article will outline these decisions in more detail.

A test for implied consent could accommodate this demand for a more nuanced balancing. However, as this article will argue, the leading Federal Court jurisprudence on PIPEDA has so far taken a restrictive approach to the question of implied consent. In contrast, the Office of the Privacy Commissioner of Canada (OPC) has utilized s. 5(3)'s requirement that information practices be "reasonable" to develop a *de facto* balancing test and then has used this to determine whether there has been implied consent. This practice, while promising, raises another set of concerns, given the Ombudsman model of dispute resolution under the act. As will be argued further in later sections of this article, a test for "reasonable" only provides parties with a clear sense of their rights and obligations where there is a stable body of precedent interpreting this standard. The current administrative structure of PIPEDA does not provide this, favouring instead a more flexible and informal dispute-resolution model.

Finally, as the previous section outlined, control will only provide informational privacy in a context where there are meaningful choices regarding the collection, use and disclosure of personal information. PIPEDA does not necessarily accommodate this concern. For example, PIPEDA permits asking whether individuals know of and consent to particular information practices, and whether these practices are reasonable. But an organization that offers services under two different plans where the more privacy-protective plan costs more does not necessarily violate these provisions of PIPEDA even if it makes the protection of privacy, for practical purposes, more difficult for individuals. Part of the problem is that it may in fact cost an organization more to offer the privacy-protective plan — making the practice appear reasonable — but this might in turn

result from an underlying technical and administrative infrastructure that has been built without due regard to privacy issues, making the subsequent protection of privacy expensive. This will be discussed in more detail in a later section.

In summary, the issues raised in the previous section regarding the relationship between control and privacy raise questions regarding the adequacy of a number of features of PIPEDA, including its all-or-nothing approach to Schedule 1 obligations; the need for a more nuanced approach to the scope of individual control over personal information and the role of implied consent in providing this; the desirability of an Ombudsman model; and whether PIPEDA's provisions can require that meaningful privacy choices be presented to individuals. The remaining sections of this article will discuss in more detail how these problems are manifesting themselves.

IV. THRESHOLD QUESTIONS

1. "Personal Information" vs. "Work Product"

The issue of whether or not something is "personal information" comprises one of the key threshold questions under PIPEDA. If an organization is found to be collecting personal information within the meaning of the act, then it will be bound by the obligations found in Schedule 1 of the act, including the consent provisions. It is important to note that "personal information" is defined broadly as "information about an identifiable individual". This is quite different from other regimes that protect informational privacy. For example, s. 8 of the Charter has been held to protect informational privacy only insofar as the information in question falls within a "biographical core" of information that one would seek to keep secret from the state.²⁵ PIPEDA leaves the question of nuances between different types of personal information to the later issue of what kind of consent to provide rather than as a way of restricting protection at the outset. For example, under Schedule 1, the requirements of consent vary according to how "sensitive" the information is.²⁶ Nonetheless, as this section will argue, the all-or-nothing approach to engaging the obligations under Schedule 1 puts pressure

25. *R. v. Plant*, [1993] 3 S.C.R. 281 at p. 293, 84 C.C.C. (3d) 203, [1993] 8 W.W.R. 287.

See also *R. v. Tessling*, [2004] 3 S.C.R. 432, 244 D.L.R. (4th) 541, 189 C.C.C. (3d) 129.

26. PIPEDA, *supra*, footnote 1, at Schedule 1, Principle 4.3.4.

on the determination of "personal information" to play a stronger gate-keeping function than it is currently drafted to provide.

The key illustration of this potential problem is the decision of the former Privacy Commissioner, George Radwanski (the Commissioner), concerning the question of whether physician prescribing patterns are personal information under the act. The Commissioner concluded that they are not, arguing that they are a "work product" that is excluded from the definition of personal information. He wrote:²⁷

It is certainly difficult to discern how an individual prescription can constitute personal information about the physician who wrote it. While it can be revealing with regard to the patient — the nature of an illness or condition, for instance, and perhaps its severity — it discloses little or nothing about the physician as an individual. Indeed, a prescription is not normally treated as personal information about himself or herself by the prescribing physician. The patient is not enjoined to secrecy, remaining entirely free to show it to anyone at will or to leave it unattended in a public place

This is not surprising, because the prescription is not, in any meaningful sense, "about" the physician. It does not tell us how he goes about his activities, whether he is casual or formal, whether he works mornings or afternoons, whom he meets, where he goes, what views he holds, or any of the other myriad details that might constitute personal information. Rather, a prescription is the outcome of the professional interaction between the physician and the patient: the physician meets the patient, carries out an examination, perhaps reviews the results of tests, and then issues the prescription. Hence, the prescription can perhaps most appropriately be regarded as a "work product." I find it to be information not about the physician, but about something once removed, namely the professional process that led to its issuance.

Although "personal information" for the purposes of PIPEDA is very broad in scope, here the Commissioner infuses it with considerations that seem more at home in traditional privacy determinations — is this information traditionally considered secret? Does it go to one's biographical core? Moreover, the definition of personal information in the act says nothing of the distinction between information about someone in their professional capacity rather than their personal capacity, except to exclude "the name, title or business address or telephone number of an employee of an organization".²⁸ And, despite the Privacy Commissioner's assertion that prescription information provides little information about the physician, it is important to understand that pharmaceutical companies seek this information in part because they think that it does. They

27. PIPED Act Case Summary #15.

28. PIPEDA, *supra*, footnote 1, at s. 2(1).

use this information to compile personalized physician prescribing patterns that they can then use for purposes of targeted marketing — a practice that many physicians object to if it is done without their knowledge or consent.²⁹

The motivating concern of the Commissioner seems to be the potential consequences arising from a finding that information about how one undertakes professional duties might be subject to the consent provisions of the act and thereby preclude important commercial consumer reporting. For example, he wrote in the same case summary:

Does the chef in a restaurant predominantly focus on cooking fish, does she have a heavy hand with the tarragon or use very little salt? Does a contractor tend to use the very newest roofing materials, or does he predominantly stick with what was in vogue 10 years ago? Does a garage mechanic tend to fix only the problem that was reported, or is there a pattern of discovering other purported problems that run up the bill?

He went on to express concern that if personal information could encompass “work products” in this manner, then employees covered by PIPEDA would be able to invoke its provisions with respect to such things as “letters written by employees in the course of their employment, legal opinions, or reports prepared by employees for use by management”.

However, it is difficult to square this interpretation with the language of the act, which suggests that such “work products” are indeed “personal information”. Decisions like the “work product” decision are in fact engaged in a balancing for which there is no statutory support: the legitimate needs of others in the information is seen as a reason not to engage the obligations of the act even though the act contains no such balancing language as a threshold matter. A way around this might be to deal with such concerns through implied consent rather than as a threshold matter. For example, to invoke one of the Commissioner’s examples, a contractor has no right to restrict the dissemination of information about the quality of his work, as this information is of vital importance to the consumer. But could we not argue that, although this is indeed personal information, the contractor has himself put it in issue as part of his professional reputation and so consent to the dissemination of accurate information about his work is implied? The issue of implied consent will be taken up in more detail in a subsequent section.

29. Zoutman *et al.*, “A Call for the Regulation of Prescription Data Mining” (2000), 163 *Canadian Medical Association Journal* 1146.

There are other potential avenues within PIPEDA that could address these concerns, without invoking the awkward carve-out of “work product”. For example, there is an exemption for journalistic purposes that would seem able to accommodate consumer reporting.³⁰ Second, it is not clear that such reporting would necessarily fit within the “commercial activity” necessary to engage the act in the first place.³¹ The same might be said for other attempts to collect, use or disclose other types of work products.

This “work product” decision does point to the potential desirability of revisiting the statutory language of PIPEDA. For example, it is useful to compare the treatment of this issue with treatment of a similar dilemma under public sector data protection law. The key question here is how to strike a balance between the public’s legitimate interest in the disclosure of certain types of information and an individual’s interest in keeping that information private. Under the federal Access to Information Act, “personal information” shall not be disclosed unless the public interest in the disclosure outweighs the potential invasion to privacy.³² Personal information in this context does not include information relating to the position or function of a government employee.³³ Recently, the Supreme Court of Canada indicated that, in interpreting these provisions, the relevant line is not between information about an individual and information about the position or function of the employee. Rather, the question is whether the information, which will always be information about an individual, is related to the general characteristics of the position. In other words, the court did not attempt to say that this was not information about an identifiable individual. Instead, it sought to balance the privacy concerns of an individual against the concerns that engage the purposes of the ATIA: governance, participation, accountability. It is clear that citizens need some access to information about government employees, so the line is drawn at a certain level of generality about those positions. Similarly, in the context of PIPEDA, it would be preferable to acknowledge that work products are indeed personal information but that at a certain

30. PIPEDA, *supra*, footnote 1, s. 4(2)(c).

31. *Ibid.*, s. 4(1)(a).

32. Access to Information Act, R.S.C. 1985, c. A-1, ss. 19(1), 9(2); Privacy Act, R.S.C. 1985, c. P-21, s. 3.

33. Privacy Act, *ibid.*, s. 3(j).

level of generality, the disclosure of information about how one undertakes one's professional duties might be of sufficient public interest.³⁴ An amendment to PIPEDA could make this clearer.

The other issue overlooked by the Privacy Commissioner's "work product" decision is that even if we think that physician prescribing patterns may be collected without consent, we still might think that other obligations that are traditionally part of fair information practices should apply. For example, the principle of openness would ensure that both physicians and the public are aware of the targeted marketing practices of drug companies and enable a degree of vigilance regarding whether such practices unduly influence physician prescription habits. However, PIPEDA's all-or-nothing approach to the obligations of Schedule 1 precludes this. Only legislative amendments to the structure of PIPEDA could accomplish this.

2. Anonymous Information and the "Identifiable Individual"

As outlined in the previous section, "personal information" is defined as "information about an identifiable individual".³⁵ This raises another important threshold question, which is: what is the meaning of "identifiable"? This question is important because if information is considered to be identifiable, and therefore personal information, then the obligations outlined in the act will apply. As discussed earlier, these obligations include compliance with the principle of knowledge and consent, which can impose considerable costs and burdens upon organizations.

Consider the following two cases, which are in tension with one another. The first, PIPED Act Case Summary #4, concerned an organization that collected information regarding the entertainment budget of various establishments in order to determine copyright dues. The budget included information regarding salaries. The complaint was that the particular establishment only had one musician, so it would be easy to determine his salary. The Privacy Commissioner determined that this was not personal information about an identifiable individual, but provided no reasoning for this conclusion.

34. For an overview of arguments regarding the public interest in access to physician prescribing patterns, see Christopher Jones, T. Murray Rankin, Q.C., and James Rowan, "Do Physicians Have a Privacy Right Over the Prescriptions they Write?" (2000-2001), 14 *Can. J. Admin. L. Prac.* 225.

35. PIPEDA, *supra*, footnote 1, s. 2.

Contrast this with PIPED Act Case Summary #25, which concerned a website that was attempting to collect Network Basic Input/Output System (NETBIOS) information from computers accessing the site. This information could be used to trace an Internet protocol address, which in turn could "allow access to information such as Web sites visited by the computer's user or recent passwords used in obtaining access to secure accounts".³⁶ The organization at issue indicated that this collection was inadvertent and deactivated the features of its network that enabled this. The Privacy Commissioner, in finding a breach of PIPEDA, reasoned that "in some circumstances, notably the complainant's, a NETBIOS might be used to obtain information traceable to an identifiable individual". In this latter case, then, the Privacy Commissioner invoked a standard of "might be" to determine "identifiable", which is in strong contrast with the earlier case, which easily would have met a "might be" test.

The major problem with a "might be" test is that many experts dispute the idea that information can ever truly be anonymous. For example, Latanya Sweeny has argued that anonymity is in the eye of the beholder because someone who obtains deidentified information from an organization might have further information allowing them to identify individuals, and the organization releasing the original data may not know this.³⁷ Sweeny argues that for much of the adult population in the United States, local census information can be used to reidentify deidentified data because other personal characteristics, such as gender, date of birth and ZIP code often combine uniquely to identify individuals. Furthermore, "[a]ny single uniquely occurring value or group of values can be used to identify an individual". For example, if hospital maternity records contain only one patient who gave birth to triplets, then this could identify an individual even if there is no additional data regarding age, residence, etc. Therefore, Sweeny's provocative contention is that information is *always* about an identifiable individual.

What are the implications of the impossibility of anonymous information? If "might be identifiable" is the test for "personal information" under PIPEDA, then potentially all information meets this test and any organization dealing with seemingly deidentified information will be caught by the obligations of Schedule 1.

36. PIPED Act Case Summary #25.

37. Latanya Sweeny, "Weaving Technology and Policy Together to Maintain Confidentiality" (1997), 25 *The Journal of Law, Medicine and Ethics* 98.

However, there are two compelling reasons to reject this result. The first concerns statutory interpretation: "personal information" needs to mean something. If *all* information is caught by the act then the initial threshold of "personal information", albeit already broad, is rendered meaningless. The second is practical: requiring all organizations who deal with such a broad category of information to comply with all of the obligations set out in Schedule 1 seems unnecessarily onerous to meet privacy concerns.

A better test for whether or not information is "personal information" should depend on the presence of risk factors for its reidentification. These factors would include the likelihood of reidentification as well as the potential harmful consequences of reidentification.

Such an approach would suggest that the obligations regarding the disclosure of deidentified data should be different from the obligations regarding the collection and use of deidentified data. For example, if an organization is using information in a manner that would not reasonably lead to its reidentification, then there seems to be little reason to impose a strict interpretation of "identifiable" and its ensuing obligations. However, if an organization is *disclosing* deidentified data, then there is reason to impose a stricter interpretation, given that once information is generally disclosed, it can exist in the public domain for a long period of time and potentially be reidentified.

Utilizing a reidentification risk approach, the two cases already discussed can be shown to be rightly decided. In the case regarding the single musician's salary, although the organization collects information regarding entertainment budgets and could fairly easily deduce the musician's salary, it does not itself have any interest in identifying the musician and it does not release this information to any third parties.³⁸ Therefore, based on what is known of the information practices of the organization in question, the risk of identification is quite low even if it could meet a "might be" test. The same might be said regarding the NETBIOS case, as there was no indication that the organization was going to identify the individual or disclose this information to others. However, it is unlike the musician's case as the information collection at issue was inadvertent, which suggests sloppy information practices rather than trustworthy organizational policies. Moreover, the information at issue

38. PIPED Act Case Summary #4.

was more sensitive than in the previous case and, if linked to an identified individual, more intrusive of their privacy. Therefore, even though the organization's practices meant that there was a relatively low likelihood of reidentification, the organization was less trustworthy in its practices and the consequences of reidentification were more severe.

Even if the interpretation of "personal information" can be improved to take into account the challenges of anonymity by adopting a reidentification risk approach as just outlined, this does not address all problems associated with anonymous information under PIPEDA. Other problems might require statutory amendment rather than a particular interpretive test. In particular, the all-or-nothing approach to engaging the obligations of Schedule 1 does not admit of the kind of tailoring that would be advisable in some situations. For example, the principle of knowledge and consent might be too onerous to impose in some circumstances where principles such as safeguards are entirely appropriate. This might vary with the type of information at issue and the risks and consequences of its reidentification: an organization that collects and uses deidentified financial data should be held to high standards of security and transparency even if the data was scrubbed according to rigorous standards and, using a reidentification risk approach, did not meet the test for "identifiable". Even if the organization itself was not going to disclose this data except perhaps in aggregate form, hackers could gain access to it if it was not properly secured. They could then use other information to reidentify the data, with serious repercussions for informational privacy.

V. CONSENT

1. Control, Consent and Other Legitimate Interests

If providing individuals with control over their personal information is held to protect informational privacy, then consent is the central entitlement through which this control is operationalized. Under PIPEDA, individuals are granted control through their right to consent to the collection, use and disclosure of their personal information. Therefore questions regarding the proper scope of the legal entitlement to control are connected to questions regarding the requirements of consent and the exceptions to consent found in the act.

There are good reasons to argue that more flexibility is required in determining the scope of consent than what is currently found in Schedule 1 and s. 7 of the act. As discussed above, privacy theorists have had great difficulty dealing with the question of when an individual is entitled to control over their personal information in the face of other legitimate interests. Moreover, there are good reasons to hold that consent is not always required in order to protect privacy. Furthermore, the overall purpose of the act is to promote both privacy and legitimate business concerns. All of these considerations suggest that a greater flexibility is desirable in determining the requirement of consent as well as its exceptions.

Without such flexibility, potentially problematic interpretations of PIPEDA will flourish as organizations seek to avoid the consent obligations. The "work product" decision discussed above is one such example. There are further examples. Consider the following workplace complaint regarding the use of digital video cameras. As part of its security system, the organization in question had installed video cameras at areas of access to its facilities. The complainant filed a grievance alleging that the manager of security services deliberately hit him with the turnstile gate at the main ramp. In the course of investigating this complaint, the organization viewed video footage from the security cameras. While this footage did not indicate an assault as alleged, it did show the complainant walking on the vehicle ramp, which was in violation of company policy. The organization then further reviewed the videotapes for a 30-day period and determined that the complainant had violated this policy on other occasions as well. The organization disciplined the employee, and the employee complained about a breach of PIPEDA.

Upon investigation, the Privacy Commissioner held that there was no requirement of consent for the recording of the complainant walking down a ramp.³⁹ The reason given was twofold: first, that the purpose of the recording was not to collect personal information; second, that there was no reasonable expectation of privacy at the entrance/exit of the workplace. However, neither of these reasons is well supported by the text of the legislation itself. The purpose of the collection of information is not relevant to the question of when consent is required. The threshold for engaging the obligations found in Schedule 1 is whether personal information is being collected, not whether it was *intended* to be collected. Nor is the

39. PIPED Act Case Summary #264.

reasonable expectation of privacy relevant to the question of consent. Under the express language of the act, reasonable expectations go to the question of whether consent is implied or express — not to undermining the requirement of consent entirely.⁴⁰ This decision promotes an interpretation of PIPEDA in which the requirement of consent could be avoided entirely and for reasons that have little textual legitimacy.

At the same time, the result in this case looks correct: it does not seem reasonable to require individual employee consent to the videotaping at issue. The installation of the video cameras was recommended by a Labour Canada investigator for safety reasons, and agreed to by the union. Employees were notified about this security system and were given ongoing opportunities to raise their concerns. However, rather than finding that there is no requirement of consent, based upon a problematic interpretation of PIPEDA, it would be better to invoke the concept of implied consent. One could argue that an employee, in such circumstances, impliedly consented to the videotaping.

Of course, if implied consent is to work in this manner, then a test for implied consent needs to be developed that can properly balance individual informational privacy and the legitimate information practices and needs of others. Implied consent is promising because it offers a place to introduce more nuances in determining the scope of consent and control without necessarily requiring legislative amendment. However, as the following section will outline, the leading judicial decisions interpreting PIPEDA have yet to appreciate this challenge and formulate a workable test. The OPC has been utilizing s. 5(3) to develop a test for reasonableness that can be used to determine implied consent, but its practice is not yet transparent enough and leads to other problems, which will be discussed below.

2. Judicial Decisions

The leading judicial decision interpreting PIPEDA, and dealing with the issue of consent, is the Federal Court of Appeal decision in *Englander v. Telus Communications Inc.*⁴¹ TELUS uses and discloses customer listing information (name, address and telephone number) for a number of primary and secondary purposes. Its practice had

40. PIPEDA, *supra*, footnote 1, Schedule 1, Principle 4.3.5.

41. (2004), 247 D.L.R. (4th) 275, 36 C.P.R. (4th) 385, 1 B.L.R. (4th) 119 (F.C.A.).

been to discuss privacy concerns and options only if the customer herself expressed an interest in not having her listing information published.⁴² The Federal Court of Appeal held that this practice was inadequate and that TELUS had failed to obtain valid consent with respect to *both* the primary and secondary purposes for which a consumer's personal information was collected, used and disclosed.

Décary J.A.'s reasons with respect to the secondary purposes are unsurprising and find ample statutory support in PIPEDA's requirements for notifying individuals of the purposes for which their information is being collected, used and disclosed.⁴³ He held that TELUS needed to identify its secondary purposes to a new customer at the time of enrolment, something that it made no effort to do unless prompted by the customer. These purposes include use of the personal information in an Internet directory assistance service called "People Finder", and its use in services such as TELUS's Directory File Service, its Basic Listing Interchange File, and its CD-ROM service. Through these latter services, TELUS provides listing information, for a fee, to certain organizations. Not only were these services not identified, Décary J.A. also held that "there is no evidence that they were so connected with the primary purposes of telephone directories that a new customer would reasonably consider them appropriate".⁴⁴

More surprising, and with less explicit statutory basis, Décary J.A. also held that TELUS did not obtain valid consent for its primary purposes, namely publishing customer listing information in a phone directory. The trial judge accepted the evidence that TELUS customer service representatives informed first-time customers that telephone service would include a listing in their directories. Furthermore, the judge held that there was a long-established industry practice of including listing information in directories unless the customer requested an unlisted number. This would appear to fulfil the requirement that customers be informed of the purposes for which their information is being collected, used and disclosed. However, Décary J.A. held that it was not enough to inform individuals of this primary purpose — they also had to be informed of the option to opt out of a directory listing by choosing an unlisted number. In other

42. *Ibid.*, at para. 63.

43. See PIPEDA, *supra*, footnote 1, Schedule 1, Principle 4.2 (Principle 2 — Identifying Purposes) and 4.3 (Principle 3 — Consent), especially Principle 4.3.2.

44. *Englander v. Telus Communications Inc.*, *supra*, footnote 41, at para. 65.

words, proper notification included not just notification of purposes but notification of *choices*. According to Décary J.A., "A consent is not informed if the person allegedly giving it is not aware at the time of giving it that he or she had the possibility to opt out."⁴⁵ TELUS needed to take positive steps to tell its customers about their privacy options at the time of seeking service and not wait until the customer had herself, unprompted, expressed an interest in an unlisted number.

Décary J.A. based this interpretation on his overall approach to interpreting PIPEDA. As he stated,

even though Part 1 and Schedule 1 of the Act purport to protect the right of privacy, they also purport to facilitate the collection, use and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests. Furthermore, because of its non-legal drafting, Schedule 1 does not lend itself to typical rigorous construction. In these circumstances, flexibility, common sense and pragmatism will best guide the Court.⁴⁶

In adopting such a "flexible" interpretation, Décary J.A. held that Schedule 1, taken as a whole, required informed consent and informed consent requires understanding the possibility of opting out by choosing not to be listed. Moreover, this result was "a fair compromise between one's right to privacy and the industry's needs".⁴⁷

However, it is important to note that this decision appears to leave little room for the role of implied consent. Consumers can only give valid consent to their listing information being published in a directory if they know about both the fact of the listing and the possibility of obtaining an unlisted number. Décary J.A. could have held that customers have tacit knowledge of the possibility of obtaining an unlisted number, given widespread industry practice. To say that it is not reasonable to expect most telephone customers to know this is to seriously limit the scope for implied consent based upon any contention of the common knowledge of the practices of a particular industry. A better basis for Décary J.A.'s result would have been to argue that the information in question should be considered sensitive, given the potential for unwanted contact and even harassment that can result from a public listing in an

45. *Ibid.*, at para. 67.

46. *Ibid.*, at para. 46.

47. *Ibid.*, at para. 67.

information age, and that on this basis implied consent was inappropriate. This line of reasoning would not undercut the role of implied consent in future cases to the same extent.

If the *Englander* decision expands the requirement of notification beyond the text of the act, and leaves a reduced scope for implied consent, the decision in *Eastmond* avoids the issue of implied consent entirely.⁴⁸ Lemieux J. declined discussing implied consent as the issue “was raised but really not argued [and] is better left to a determination in another case”.⁴⁹ Moreover, the *Eastmond* decision is more clearly rooted in the text of the legislation but nonetheless appears rigid with respect to its interpretation of consent and its exceptions.

In *Eastmond*, an employee complained about the railway’s installation and use of six security cameras without employee consent. These cameras were placed in areas of general access and parking and were intended to help reduce vandalism and deter theft, reduce liability for property damage and enhance staff security. These cameras were fixed — that is, did not move or have zoom capabilities — and would automatically tape for 48 hours. However, the tapes would only be looked at if there was an incident to investigate.

Most of the analysis in the case concerned the interpretation of s. 5(3) — was the use of the security cameras “for purposes that a reasonable person would consider are appropriate in the circumstances”? Lemieux J. concluded that they were, as the privacy loss at issue was minimal: the cameras were not surreptitious, the collection of information was not continuous, the cameras were unsuited to monitoring employee productivity, they were in public places, and the tapes would only be looked at when an incident was reported.⁵⁰ Additionally, Lemieux J. found the employer’s interests to be persuasive, as there had been past incidents of vandalism, the cameras would deter future incidents (and there had been none since their installation) and other alternatives were not as cost-effective.⁵¹

However, the second question that Lemieux J. addressed was whether, even if the collection of information was reasonable,

48. *Eastmond v. Canadian Pacific Railway* (2004), 33 C.P.R. (4th) 1, 16 Admin. L.R. (4th) 275, 254 F.T.R. 169.

49. *Ibid.*, at para. 191.

50. *Ibid.*, at paras. 180-81.

51. *Ibid.*, at para. 177.

consent for the collection was required. He held that the collection of personal information can be made without the knowledge and consent of an individual only when this collection fits within one of the exemptions outlined in s. 7 of the act.⁵² He held that the collection in this case fit within the exemption of s. 7(1)(b), which provides that information may be collected without the knowledge or consent of the individual if:

it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the law of Canada or a province.

According to Lemieux J., the

collection of the person’s information takes place when CP officials view the recording to investigate an incident. Assuming the recording captured an individual committing an act of theft asking for his/her permission to collect the information would compromise the availability of the information for the purpose of investigation.⁵³

He further argued that this interpretation “does not does not strain the purposes of the exemption in paragraph 7(1)(b)”.⁵⁴

However, Lemieux J.’s interpretation does strain the overall purposes of the act, for this reasoning would permit a great deal of surveillance. Organizations could “collect” large amounts of personal information outside of the purview of the act and then retain this data for long periods of time so long as they only looked at the data in the context of one of the exemptions outlined in s. 7. Given the nature of the law enforcement and national security exemptions, this interpretation of s. 7 is quite worrisome from the perspective of protecting individual privacy.

A better approach would have been to take up the challenge of implied consent. As will be outlined next, the practice of the OPC has already laid the foundation of such an approach that does not strain either the language or the purpose of the act. However, as will also be argued, fully utilizing such an approach raises serious questions regarding the use and appropriateness of the current Ombudsman model for administering the act.

52. *Ibid.*, at para. 186.

53. *Ibid.*, at para. 189.

54. *Ibid.*, at para. 190.

3. OPC Practice and the Role of s. 5(3)

The most promising basis upon which to introduce interpretive flexibility into PIPEDA is to utilize s. 5(3), which states: "An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances." As this section will outline, s. 5(3) can be used to create a test for implied consent as well as to temper the interpretation of the exceptions to consent found in s. 7. Such an approach is already implicit in the practices of the OPC. However, making it more explicit raises a number of further questions regarding the emphasis, following from the Ombudsman model of enforcement, on alternative dispute resolution, rather than on the establishment of a body of binding case law.

As I argue in detail in another article,⁵⁵ in a number of cases where individuals are properly notified regarding the purposes for the collection of their personal information and that collection, use or disclosure is found to be reasonable under s. 5(3), the OPC has made a finding of implied consent — even in cases where the very complaint was that information was being collected without the complainant's consent. This practice suggests the following approach to the question of implied consent: a finding of implicit consent should be made where an individual consents to a particular transaction for goods or services (or, as in the context of employment, consents to a particular kind of relationship), knows about the information practices associated with that transaction, and where such information practices are considered to be reasonable. Explicit consent would only be required in two types of cases: first, where the process of gaining consent is important for ensuring that notification has actually occurred for some categories of sensitive information; second, when the information collection, use or disclosure itself amounts to a separate transaction and is not simply tied to the original transaction that is consented to (as when the sale of goods is used as an opportunity to collect information to be used in future targeted marketing campaigns).

Even in cases where implied consent is not appropriate but the exceptions to consent found in s. 7 are utilized, some of the potential excesses of the s. 7 provisions could be tempered by this section and s. 5(3) together. For example, in a case involving video

55. Austin, *supra*, footnote 9.

surveillance in the workplace, the Privacy Commissioner interpreted the exemption found in s. 7(1)(b) in light of the reasonableness requirement in s. 5(3): in the absence of evidence of a problem, and where the employer could use less intrusive means to deal with the issue, then s. 7(1)(b) is not available as a means around the consent issue.⁵⁶ This approach has also been reiterated in subsequent cases.⁵⁷

For such an approach to implied consent to work, a test for the reasonableness of the information practices in question must be developed that is rigorous and properly interprets and protects privacy interests. Otherwise it will simply function as a means to undercut privacy through an appeal to business interests. One such test has often been invoked by the Office of the Privacy Commissioner — although not in all cases involving s. 5(3) and not necessarily consistently. The Federal Court in *Eastmond*⁵⁸ approved of this test, which involves asking four questions, somewhat reminiscent of the *Oakes* test⁵⁹ in Charter jurisprudence:

1. Are the measures necessary to meet a specific need?
2. Are the measures likely to be effective in meeting that need?
3. Is the loss of privacy proportional to the benefit gained?
4. Is there a less privacy-invasive way of achieving the same end?

Because this is a balancing test, taking into account both privacy interests and the legitimate interests of others, it is well suited to temper the consent provisions and their exceptions.

However, utilizing this test raises two further issues. First, developing this test in a rigorous manner, especially when answering questions three and four regarding proportionality and tailoring, requires an understanding of the nature and scope of privacy that goes beyond the language of the legislation. To undertake the balancing demanded by this test in a way that does not simply vindicate business needs calls for a fuller appreciation of the value of privacy, when consent is important for its protection, and when privacy may be protected even in the absence of consent. The text of PIPEDA provides little guidance for this interpretive exercise.

56. PIPED Act Case Summary #265.

57. PIPED Act Case Summary #269.

58. *Supra*, footnote 48.

59. *R. v. Oakes*, [1986] 1 S.C.R. 103.

The second issue concerns the current Ombudsman model for administration of the act. As outlined above, to develop fully a test for reasonableness requires us to move beyond the text of the legislation and to make a number of determinations regarding privacy, its value, and how it is to be balanced against competing concerns. These issues are all controversial. To reduce controversy, PIPEDA requires a body of precedent interpreting these questions. Federal Court jurisprudence could provide such precedents, but few cases make it to this level and, as has been shown, to date the court has been reluctant to take on the issue of implied consent. For the most part, interpretation of the act has, quite properly, fallen to the OPC. However, the OPC must follow an Ombudsman model that relies heavily on encouraging negotiation and voluntary compliance.⁶⁰ Consequently, the findings of the OPC do not form a body of binding precedent that can provide firm guidance in developing a s. 5(3) case law. Indeed, the OPC's practice is to only publish a summary of its findings in individual cases and to protect the identity of both complainant and organization so that even their value as non-binding precedent is limited. If s. 5(3) ends up being as important to the OPC practice as current case summaries suggest, then interpretation of the act becomes too much a matter of individual discretion with the result that those affected by the act will be unable to determine clearly their rights and liabilities.

Several alternatives follow from this. First, Parliament could change the model of administration of the act so that the findings of the OPC would resemble more closely the common law model of case precedent. Second, the OPC could attempt to develop at least a body of principles, or interpretive guide, regarding privacy and make this publicly available as a source of guidance.⁶¹ Third, PIPEDA could be amended to provide more statutory guidance.

VI. FURTHER QUESTIONS: PRIVACY-ENHANCING TECHNOLOGICAL DESIGN

If one of the strongest motivating factors behind the introduction of PIPEDA was concern regarding proliferating information and

60. Roberta Jamieson has referred to the Ombudsman role as "willing listener, vigorous investigator, master persuader, and skilful mediator seeking balanced resolution". See Roberta Jamieson, "The Ombudsman: Learning from other Cultures" (1993), 25 *Ottawa L. Rev.* 629.

61. This option was suggested by Lorne Sossin at the 35th Annual Workshop on Commercial and Consumer Law.

communications technology and its effects on individual privacy, then in assessing the effectiveness of PIPEDA, it is crucial to look at whether it promotes the adoption of privacy-enhancing technologies. That is, does PIPEDA simply regulate how we can use the technology that we have, or may come to have, or does it also affect how we go about building that technology in the first place?

It is important to see why this is such a crucial question. Philosophers of technology like Langdon Winner argue that "If the experience of modern society shows us anything . . . it is that technologies are not merely aids to human activity, but also powerful forces acting to reshape that activity and its meaning."⁶² In particular, Winner's focus is on the manner in which technological artifacts can be said to have "politics", in that they "can embody specific forms of power and authority".⁶³ A focus on these aspects of technologies can highlight how, apart from questions of economics, health and safety, and environmental concerns, "choices about technology have important consequences for the form and quality of human associations".⁶⁴ One fairly obvious example he offers of the political nature of some technologies is the low-hanging overpasses on Long Island, designed by Robert Moses.⁶⁵ The twelve-foot tall buses used in public transit could not handle the overpasses, whereas cars — driven predominantly by the white middle and upper classes — could handle them easily. In this way a technological design quite deliberately kept a segment of the population off the parkways, ensuring that social inequality became embedded in the very landscape in a manner that is very difficult to later undo. As Winner argues more generally:

Consciously or unconsciously, deliberately or inadvertently, societies choose structures for technologies that influence how people are going to work, communicate, travel, consume, and so forth over a very long time. In the process by which structuring decisions are made, different people are situated differently and possess unequal degrees of power as well as unequal levels of awareness. By far the greatest latitude of choice exists the very first time a particular instrument, system, or technique is introduced. Because choices tend to become strongly fixed in material equipment, economic investment, and social habit, the original flexibility vanishes for all practical purposes once the initial commitments are made. In that sense technological innovations

62. Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (Chicago, The University of Chicago Press, 1986), p. 6.

63. *Ibid.*, at p. 19.

64. *Ibid.*, at p. 33.

65. *Ibid.*, at p. 23.

are similar to legislative acts or political foundations that establish a framework for public order that will endure over many generations. For that reason the same careful attention one would give to the rules, roles, and relationships of politics must also be given to such things as the building of highways, the creation of television networks, and the tailoring of seemingly insignificant features on new machines. The issues that divide or unite people in society are settled not only in the institutions and practices of politics proper, but also, and less obviously, in tangible arrangements of steel and concrete, wires and semiconductors, nuts and bolts.⁶⁶

Given the different ways in which technological artifacts can be said to have politics, Winner argues that we need to ask: "What forms of technology are compatible with the kind of society we want to build?"⁶⁷

Winner's argument is strikingly similar to Larry Lessig's claims regarding the need to pay attention to the law-making function of "code". One of Lessig's concerns is understanding the role that the architecture of the Internet plays in protecting or impeding certain fundamental values. As he argues, "In real space we recognize how laws regulate — through constitutions, statutes, and other legal codes. In cyberspace we must understand how code regulates — how the software and hardware that make cyberspace what it is *regulate* cyberspace as it is . . . *Code is law*."⁶⁸ "Code" is not neutral. That is, once built in a particular way it helps to shape the kind of interactions that may take place in cyberspace. Lessig acknowledges that the problems of cyberspace include ones of substance — will privacy prevail, for example. However, he believes that many of these substantive concerns will be solved if we solve the structural concerns relating to how cyberspace is constructed and who owns this architecture. Therefore for Lessig it is not enough to focus simply on the traditional broad rules of law; the architecture of the Internet — its code — influences how we can and cannot interact in cyberspace and we need to understand the relationship between this architecture and legal regulation.

Regulating interactions after the important architectural decisions have been made overlooks the important value choices that are either deliberately or inadvertently built into the technology. Technologies and the specific value choices embedded in them

66. *Ibid.*, at pp. 28-29.

67. *Ibid.*, at p. 52.

68. Larry Lessig, *Code and Other Laws of Cyberspace* (New York, Basic Books, 1999), p. 6, emphasis in original.

come to function as a kind of legislation that is created outside of our normal political and legal institutions and that is potentially quite difficult to alter after the fact. Although it may be impossible to understand all of the important social implications of our built world prior to its building, it is by no means impossible to bring to the surface many of these issues in a manner that can influence technological design. Indeed, the movement towards the greater adoption of Privacy Enhancing Technologies (PETs) is premised on the idea that information systems can be built in a manner that protects privacy from the outset rather than requiring a later trade-off between privacy and system functionality.⁶⁹

The challenge for law is to impose obligations regarding how information and communications technology should be built and implemented. Otherwise there may be no meaningful privacy protective choices available to individuals. Unfortunately, one of the problems with PIPEDA is that it is difficult to ask this important question of technological design.

Consider PIPED Act Case Summary #48. An individual complained to the Privacy Commissioner that an organization was not permitting her to pay for their services by certified cheque. Instead, the organization asked her to choose between two automatic payment options, which involved providing bank account or credit card information. The organization in question only permitted prepayments by certified cheque if a customer signed on for a more expensive combined services package. The organizational division in question was found not to have a billing system capable of administering such a payment option and only offered it with their combined services package under an arrangement they had with another division. The Commissioner held that the organization was in compliance with s. 5(3) because "a reasonable person would consider the processing of payments for service to be an appropriate purpose for the collection and would expect the organization to determine its own billing options".⁷⁰ However, the billing options in this case were closely tied to the technological and administrative capabilities of the organization. It is not clear why such options are to be entirely left to the discretion of the organization. The Privacy

69. See Philip E. Agre, "Beyond the Mirror World: Privacy and the Representational Practices of Computing", in *Technology and Privacy: The New Landscape*, Philip E. Agre and Marc Rotenberg, eds. (Cambridge, Massachusetts, The MIT Press, 1998), p. 29.

70. PIPED Act Case Summary #48.

Commissioner's reasoning would permit an organization to adopt an administrative structure that then makes the provision of privacy-protective choices difficult and costly. Asking the question of appropriate billing options after such a structure is in place is asking the question too late: many important decisions regarding privacy will have already been made and seemingly placed beyond the purview of the legal obligations found in PIPEDA.

One response to such a case is to argue for a stronger test under s. 5(3) of the act. If the reasonable purposes provision were given more teeth, then it might be possible to ask whether the balance between privacy on the one hand, and administrative cost and convenience on the other hand, was properly struck. Of course, invoking s. 5(3) in this manner would lead to the same implied consent problems discussed earlier: if s. 5(3) must do the heavy lifting under PIPEDA without further clarifying statutory language or a system of binding precedent and well-publicized full reasons, individuals and organizations will find it difficult to understand their rights and obligations.

In addition, s. 5(3) would not catch all of the cases where the issue of technological design might arise. One way to approach the issue of technological design is to ask who should bear the costs, or burdens, of ensuring that meaningful privacy-protective choices are made available to individuals. The *Englander* decision can be interpreted in this light. Part of Englander's complaint was that he should not have to pay more in order to protect his privacy by paying a fee for an unlisted number. The inappropriateness of charging this fee is difficult to articulate using s. 5(3) and Englander argued, instead, that TELUS had violated Principle 4.3.3 of the act, which states:

An 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 fulfill the explicitly specified, and legitimate purposes.

However, Principle 4.3.3 is also an awkward fit. A 4.3.3 argument is that one should not be required to consent to the disclosure of personal information as a condition of service. But in this case, such disclosure was not a requirement of service. As Décary J.A. stated:

I find no provision in the PIPED Act which expressly prohibits the imposition of fees and clause 4.3.3 of Schedule 1, on which the appellant relies, can by no means be interpreted as he suggests. The "service" referred to in that

clause is the telephone service and the clause prevents TELUS from seeking from its customers a consent wider than is necessary for the supply of that service.⁷¹

The problem is that to get service without disclosing personal information, one would have to pay more for that service. This is a different issue that is not easily articulated within the language of the obligations as set out in Schedule 1.⁷²

The essential question is whether asking the consumer to pay for enhanced privacy is an acceptable burden. Furthermore, in answering this question, one must consider whether too much emphasis is given to existing technological and administrative structures that were put in place without enough attention to privacy issues. If so, then the question of privacy gets asked too late, after many important decisions have already been made and implemented. One could argue that this in fact happened with respect to unlisted fees, which are approved by the CRTC. Although Englander had contested having to pay any fee, other privacy advocates have argued that the only reasonable payment is for the actual cost of providing the service. The CRTC rejected a cost-based rate because it "would fail to take adequate account of considerations such as the usefulness of a reasonably complete directory and the revenue impact of reduced rates".⁷³ In other words, because getting an unlisted number reduces the usefulness of the telephone directory by making it incomplete, individuals requesting an unlisted number could be expected to partially compensate service providers for this. Moving to a cost-based fee would also mean that service providers would lose revenue from the higher prices. By taking these factors into account in rejecting a cost-based fee, past revenue structures and business models that either did not take privacy into account or did so in a very different context now partially govern existing practices. However, leaving aside the adequacy of the CRTC's finding, it is important to note that the CRTC could at least ask the question of the adequacy of this fee

71. *Englander v. Telus Communications Inc*, *supra*, footnote 41, at para. 83.

72. One of the complications in *Englander* is that the court had to deal with the interaction between PIPEDA and the Telecommunications Act, and the jurisdiction of the Privacy Commissioner and the CRTC. As Décary J.A. argued, "No one argued before us that it was not a 'just and reasonable rate' within the meaning of section 27 of the Telecommunications Act, an argument the Court would have in any event declined to hear because that issue is within the exclusive domain of the CRTC." (*ibid.*, at para. 85). Leaving aside such jurisdictional questions, the issue still remains as to whether, in other circumstances, PIPEDA can address such issues.

73. *Ibid.*, at para. 31.

directly. In the context of PIPEDA, this type of question does not easily fit within the existing structure of the act.

VII. CONCLUSIONS AND RECOMMENDATIONS

This article has argued that PIPEDA provides individuals with control over their personal information in order to protect informational privacy while permitting organizations to collect, use and disclose personal information for legitimate and reasonable purposes. However, in determining whether such control is effective in protecting privacy, a number of issues emerged as important: control over personal information can protect a broader set of values than simply privacy; individual informational privacy can be protected even in the absence of individual consent; determining the scope of the legal entitlement to control over personal information requires an understanding of the values that privacy is meant to protect and a balancing of these against legitimate claims of others in a principled manner; and control will only protect privacy if individuals are presented with meaningful choices regarding privacy options. These issues then helped to pinpoint a number of PIPEDA's weaknesses, including its all-or-nothing approach to Schedule 1 obligations; the scope of individual control over personal information provided and the role of implied consent; the desirability of an Ombudsman model; and whether PIPEDA's provisions can require that privacy be taken into account at the stage of administrative and technological design.

This analysis has led to the following conclusions and recommendations. With respect to threshold questions, it is argued that "personal information" should receive a broad interpretation and the question of when information is "identifiable" should be answered utilizing a reidentification of risk approach. Both of these are matters of statutory interpretation. Potential legislative amendments include permitting the collection, use and disclosure of personal information that is of a professional nature where the public interest outweighs individual privacy interests. In addition, the all-or-nothing approach to engaging Schedule 1 obligations should be revisited to ensure that in some contexts, such as where organizations collect, use or disclose financial or health information but where the threshold of "personal information" has not been met, an organization must adhere to a subset of Schedule 1 obligations such as the principles of security and openness.

With respect to the issue of consent, there are good reasons to develop a test for implied consent, utilizing s. 5(3) of the act, in order to better balance privacy interests and the legitimate interests of others. The result of this need not be lesser privacy protection, as consent is neither a necessary nor a sufficient condition for the protection of privacy. Moreover, without such a test, problematic interpretations of PIPEDA will ensue that undercut privacy in order to create more flexibility in the act. However, if such a test is to be developed and followed in a manner that provides individuals and organizations with stable guidance regarding their rights and responsibilities, then the current Ombudsman model of administration requires rethinking so that the interpretation of s. 5(3)'s reasonableness requirement admits of some stability and predictability. This predictability could be achieved by allowing case findings to play a more precedent-setting role, creating an interpretive guide, or by amending the legislation to provide more textual guidance.

PIPEDA could provide a framework capable of meeting the challenges of privacy protection in an information age with rapidly changing information and communications technology. But to do this it must impose obligations upon organizations to take privacy into account when developing and implementing their administrative and technological infrastructures — even, up to a point, where this makes such infrastructures more costly. While s. 5(3)'s reasonableness requirement can be made to take this into account in some contexts, legislative amendments may need to be considered to address this issue properly.