Is Consent the Foundation of Fair Information Practices? Canada's Experience Under Pipeda

Lisa M. Austin

Version Post-print/accepted manuscript

Citation (published version) Austin, Lisa M., Is Consent the Foundation of Fair Information Practices? Canada's Experience Under Pipeda (November 1, 2005). (2006) 56 University of Toronto Law Journal 181.

Publisher's Statement Austin, Lisa M., Is Consent the Foundation of Fair Information Practices? Canada's Experience Under Pipeda (November 1, 2005). (2006) 56 University of Toronto Law Journal 181. Reprinted by permission of the University of Toronto Law Journal.
<http://dx.doi.org/10.2139/ssrn.864364>

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.

Is Consent the Foundation of Fair Information Practices? Canada's Experience Under PIPEDA*

Lisa M. Austin
Assistant Professor
University of Toronto Faculty of Law

1. Introduction

In January 2001, the federal government put in place an important new component of data protection law: *The Personal Information Protection and Electronic Documents Act* (PIPEDA).¹ PIPEDA regulates the collection, use and disclosure of personal information within the private sector. This Act takes its place alongside the federal *Privacy Act* and *Access to Information Act*, which regulate the public sector, together creating a fairly comprehensive federal regime regarding data protection and implementing what have come to be known internationally as “fair information practices.” Fair information practices involve a number of core entitlements that seek to place limits on information processing practices as well as to ensure the transparency and accountability of these practices. Within this model of data protection, privacy is often seen to be the core interest protected and individual consent the central vehicle through which this protection is accomplished. This certainly characterizes the rhetoric surrounding PIPEDA.

* I would like to thank Joe Murray, Hudson Janisch, David Dyzenhaus and Wendy Adams for their helpful comments on earlier drafts of this paper. All errors, of course, remain mine. An initial version of this argument was presented at the conference *Privacy and Security: the Next Wave*, Toronto, Ontario, sponsored by the Centre for Innovation Law and Policy, the Office of the Information & Privacy Commissioner (Ontario), et al., November 7, 2003.

¹ *The Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.5 [Hereinafter PIPEDA].

Initially, PIPEDA applied only to the federally-regulated private sector as well as to organizations engaged in collecting, using or disclosing information outside of the province or country. However, PIPEDA's staggered implementation schedule was completed as of January 2004 and it now applies to all organizations engaged in commercial activity *within* a province unless that province has enacted "substantially similar" legislation.² To date, Quebec, British Columbia and Alberta have all enacted legislation that has been deemed to be substantially similar.³ This paper argues that two of these initiatives raise interesting questions regarding the relationship between consent and privacy and suggest that derogations from consent are not necessarily derogations from privacy. That is, they call into question the claimed centrality of consent to fair information practices and the data protection regimes modeled upon them.

The privacy legislation of both British Columbia and Alberta permit employers to collect, use and disclose personal information about employees without employee consent so long as employees are notified prior to the collection, use and disclosure and "the collection [use and disclosure] is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the

² Pursuant to s. 26(2)(b), the Governor in Council is empowered to order an exemption from PIPEDA if the legislation of a province is "substantially similar" to Part 1 of PIPEDA. Part 2 applies to electronic documents and is not about privacy protection. This power of the Governor in Council raises important federalism concerns, which are beyond the scope of this paper. Quebec is intending to challenge the federal legislation on the grounds that the federal government has exceeded its jurisdiction. See Quebec Court of Appeal, Order No. 1368-2003 (December 17, 2003) allowing Quebec to proceed with a constitutional challenge to PIPEDA.

³ *Personal Information Protection Act*, S.B.C. 2003, c.63 (British Columbia) [Hereinafter B.C. Act]; *Personal Information Protection Act*, S.A. 2003, c. P-6.5 (Alberta) [Hereinafter Alberta Act]; *An Act respecting the protection of personal information in the private sector*, R.S.Q., c.P-39.1 (Quebec). See also *Organizations in the Province of Quebec Exemption Order*, P.C. 2003-1842, C. Gaz.2003.I.1842; *Organizations in the Province of British Columbia Exemption Order*, P.C. 2004-1164, C.Gaz.2004.I.1178; *Organizations in the Province of Alberta Exemption Order*, P.C. 2004-1163, C.Gaz.2004.I.1174.

individual.”⁴ When first introduced, these provisions received strong criticism from some privacy advocates. For example, former Privacy Commissioner George Radwanski argued that the B.C. Act “is clearly inferior” to PIPEDA with respect to protecting employee privacy and that the “reasonable” test that the Act does provide is “meager consolation for employees or prospective employees concerned about privacy.”⁵ Nonetheless, these Acts have been found to provide “substantially similar” protection to that of PIPEDA, although the basis for this finding in relation to employee privacy has not been articulated. The most straightforward reason would be that even if PIPEDA applied to activity within the provinces of B.C. and Alberta, it would not apply to employees but only commercial activities; PIPEDA only applies to employee information within the federally-regulated sector.⁶ In other words, the B.C. and Alberta Acts provide privacy protection for employees superior to that of PIPEDA because PIPEDA only applies to a narrow category of employees. A much different reason would be that the kind of privacy protection that PIPEDA offers to employees in federally-regulated industries is equivalent to the privacy protection offered to employees generally under the B.C. and Alberta Acts. According to this line of reasoning, a regime of notice and reasonableness provides the same level of privacy protection as a regime of notice, reasonableness and consent.

⁴ B.C. Act, *ibid.* at ss. 13(2)(a) and (3), 16 and 19; Alberta Act, *ibid.* at ss. 15, 18 and 21.

⁵ Privacy Commissioner of Canada, News Release (May 8, 2003); he made similar criticisms of Alberta’s legislation: Privacy Commissioner of Canada, News Release (May 27, 2003).

⁶ PIPEDA, *supra* note 1 at ss. 4(1)(b) and 30; see Office of the Privacy Commissioner of Canada, “What is Not Covered by the Act” in *Your Privacy Responsibilities: A Guide for Businesses and Organizations to the Personal Information Protection and Electronic Documents Act* (<http://www.privcom.gc.ca/information/guide.asp>).

This paper argues that this second line of reasoning is in fact persuasive. Moreover, it argues that this line of reasoning is persuasive even outside of the employment relationship. Its central claim is that the alleged centrality of consent to the protection of privacy is misplaced: all derogations from consent are not necessarily derogations from privacy.

A number of reasons support this claim. First, while consent-based privacy regimes are attractive both in terms of the individual empowerment they seem to provide and the manner in which they appear to evade the definitional difficulties that plague other regimes, they suffer from a number of important defects. These defects, enumerated in subsequent sections of this paper, suggest that individual consent is neither necessary nor sufficient for the adequate protection of privacy. Therefore there are strong theoretical reasons for skepticism regarding any claims to the centrality of consent to the protection of privacy. Second, a close examination of several articulations of fair information practices suggest that consent is not the only norm operating to limit the collection, use and disclosure of personal information. Some of these other norms, like the “reasonable purpose” standard included within PIPEDA, can potentially offer a great deal of privacy protection. Third, the decisions rendered under PIPEDA so far in fact confirm the conceptual primacy of reasonableness over consent. In these cases, where individuals are properly notified regarding the purposes for the collection of their personal information and that collection is found to be reasonable, a finding of consent follows. In other words, it is the test for “reasonable purposes” and not the consent provisions that drives the analysis. This suggests that it is “reasonable purposes” that

holds out the most promise for strong privacy protection and is therefore deserving of much greater attention by the privacy community.

However, this paper also argues that the decisions under PIPEDA indicate that the promise that “reasonable purposes” holds for the protection of privacy remains largely unfulfilled. If consent is seen as providing central protection for privacy, then “reasonable purposes” too easily becomes a site for the consideration of countervailing values, such as business interests. In this way, misunderstanding the relative roles of consent and reasonable purposes threatens to undermine privacy rather than protect it. What is needed instead is a shift in focus away from consent and towards a more nuanced and normative approach to privacy that is then incorporated into a test for “reasonable purposes.”

2. The Relationship Between Consent and Privacy

(a) The Promise of Consent

A regime of privacy protection centered around individual consent, particularly in the context of e-commerce, is attractive for a number of reasons. It has the potential to shift the balance of power away from businesses who have strong reasons to collect personal information towards the individuals who might have strong reasons to prevent this. In this way, a baseline entitlement to consent can give individuals greater bargaining power within the market to force businesses to be more responsive to privacy. Indeed, PIPEDA was introduced, in part, as one prong of the federal government’s E-Com

Strategy, responding to consumer concerns that shopping on-line put their privacy at risk.⁷

But a consent-based privacy regime is attractive for reasons beyond its perceived individual empowerment. Another attraction, less obvious to consumers but important for legal policy, is that such regimes appear to avoid some of the definitional difficulties surrounding the idea of privacy. Privacy is a notoriously elusive concept and adequately defining it has been one of the central problems plaguing any legal regime purporting to protect it. For example, after surveying the extensive American experience with the tort of invasion of privacy, William Prosser famously argued that the tort protected not one, but four separate interests and should be considered as four separate actions.⁸ This is indeed how the tort is currently treated in American law; there is no general tort of invasion of privacy but rather intrusions upon seclusion, publication of private facts, false light publicity and misappropriation of name or likeness.⁹ Such difficulties with defining privacy within tort law have led some other jurisdictions to reject recognition of such a tort, confining the protection of privacy to what may be accomplished under breach of confidentiality.¹⁰ Canada occupies a middle ground, with a few lower court decisions

⁷ William Charnetski, Patrick Flaherty, Jeremy Robinson, *The Personal Information Protection and Electronic Documents Act: A Comprehensive Guide* (Aurora: Canada Law Book, 2001) at 6.

⁸ William Prosser, "Privacy" (1960) 48 Cal. L. Rev. 338.

⁹ *American Restatement (Second) of Torts* § 652A (1977).

¹⁰ See *Wainright v. Home Office*, [2003] 3 W.L.R. 1137 (H.L.); *Campbell v. MGN Ltd.*, [2004] E.M.L.R. 15 (H.L.).

endorsing the recognition of the tort¹¹, others embracing privacy under the rubric of nuisance law¹², and a few provinces creating a statute-based tort.¹³

The definitional difficulties that plague the private law are also present in constitutional jurisprudence regarding privacy. Canada's Charter has been held to protect a "reasonable expectation of privacy." However, this test suffers from an important ambiguity resulting from the fact that "reasonable" refers to two very different kinds of inquiries with respect to privacy.¹⁴ One sense of "reasonable" refers to the outcome of a balancing of privacy with other interests such as law enforcement. This is the sense in which "reasonable" is invoked in the first major Charter decision interpreting s.8: *Hunter v. Southam*.¹⁵ There is a point at which an individual's privacy interest must give way to other important state interests. *Hunter v. Southam* held that, in the context of law enforcement, that point was articulated by the standard of reasonable and probable cause. The second sense of "reasonable" refers to the threshold question of whether a sufficient privacy interest is at stake to engage the *Charter*. This threshold question is therefore unconcerned with the question of the interests that might weigh against privacy in a particular context and instead asks about the nature of the privacy interest at stake.

¹¹ See e.g.: *Saccone v. Orr* (1981), 34 O.R. (2d) 317 (Co.Ct.). But also see *Weingerl v. Seo* [2003] O.J. No. 4277 (Ont. Sup. Ct. Jus.) for a more limited reading of this case.

¹² *Motherwell v. Motherwell* (1976), 73 D.L.R. (3d) 62 (A.C.A.); *Roth v. Roth* (1991), 4 O.R. (3d) 740; *Ontario (Attorney General) v. Dieleman* (1994), 20 O.R. (3d) 229; *Saelman v. Hill*, [2004] O.J. No. 2122.

¹³ See *An Act Respecting the Protection of Personal Privacy*, R.S.N. 1990, c. P-22 (Newfoundland); *The Privacy Act*, R.S.M. 1987, c.P125 (Manitoba); *An Act Respecting the Protection of Privacy*, R.S.S. 1978, c.P-24 (Saskatchewan); *Privacy Act*, R.S.B.C. 1979, c.336 (British Columbia); *Civil Code of Québec*, C.C.Q., Book 1 ss. 35-41; *The Québec Charter of Human Rights and Freedoms*, R.S.Q. C-12, s.5.

¹⁴ For a more detailed version of this argument, see Lisa Austin, "Privacy and the Question of Technology" (2003) 22 Law & Phil. 119.

¹⁵ *Hunter v. Southam*, [1984] 2 S.C.R. 145.

Although the threshold question and the balancing question are distinct, the jurisprudence is replete with examples where the two questions have been conflated. This is problematic when considerations of the kinds of interests that might outweigh privacy in some contexts are invoked in order to define the nature of the privacy interest at stake in the threshold analysis. In this way, privacy is discounted prior to the balancing exercise where those countervailing interests are properly considered. This “double-counting” of the interests that are to balance against privacy then has the very real potential to undermine privacy protection.¹⁶

Another important defect of the reasonable expectation of privacy test is that it often is interpreted as a kind of descriptive inquiry into social expectations of privacy rather than a normative, purposive inquiry into why privacy is important in a free and democratic society and how those values are engaged in any particular context. That is, instead of asking whether surreptitious video cameras in hotel rooms are consistent with a free and democratic society, many judges instead ask “well, in the circumstances, what did you expect?”¹⁷ However, in the context of new and emerging information practices where social practices and expectations are not settled, the question should not be “what did you expect?” but rather “what *should* you expect?” The latter question is one that requires an inquiry into the value of privacy.¹⁸ Even in cases where a more normative approach may be discerned, what is appealed to are a confusing mix of norms arising out

¹⁶ Examples of this approach include *R. v. Wise*, [1992] 1 S.C.R. 527 and *R.v. M. (M.R.)*, [1998] 3 S.C.R. 393.

¹⁷ See *R. v. Duarte*, [1990] 1 S.C.R. 3, for the contrast between LaForest J. and Lamer C.J. (as he then was) on this point.

¹⁸ See, for e.g., *R. v. Dyment*, [1988] 2 S.C.R. 417; *R. v. Mills*, [1999] 3 S.C.R. 668.

of considerations such as property, bodily integrity, decisional autonomy and confidentiality, with little analysis linking these strands together.¹⁹

These definitional difficulties present in legal regimes protecting privacy are present in the literature regarding privacy as well. In pointing to the general lament of theorists regarding the ability to reach a satisfying account of privacy, Solove notes that privacy definitions currently encompass “(among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations.”²⁰ This is not a recent phenomenon. More than 20 years ago, Gavison surveyed the terrain and argued that various accounts of privacy have included practices as various as:

the collection, storage, and computerization of information; the dissemination of information about individuals; intruding or entering “private” places; drawing attention to individuals; required testing of individuals; and forced disclosure of information. ... exposure to unpleasant noises, smells and sights; prohibitions of such conduct as abortions, use of contraceptives, and “unnatural” sexual intercourse; insulting, harassing, or persecuting behaviour; presenting individuals in a “false light”; unsolicited mail and unwanted phone calls; regulation of the way familial obligations should be discharged; and commercial exploitation.

It is difficult to offer a theory or definition that is able to coherently account for the inclusion of such diverse practices under the rubric of privacy.

¹⁹ For a discussion of the relationship between privacy and confidentiality under s.8, see Lisa Austin, “One Step Forward or Two Steps Back? *R. v. Tessling* and the Privacy Consequences for Information Held by Third Parties” (2004) 49 *Crim. L.Q.* 22; *R. v. Edwards*, [1996] 1 S.C.R. 128, provides a clear example of the privacy understood in terms of the norms of private property; *R. v. Dymnt*, *supra* note 18, discusses blood both in terms of bodily integrity and informational privacy without any clear statements regarding the differences between them.

²⁰ Daniel Solove, “Conceptualizing Privacy.” (2002) 90 *California Law Review* 1087 at 1088.

Given these difficulties, a consent-based privacy regime has much to recommend. Such regimes often implicitly rely upon a definition of privacy as control over personal information; consent is the manner in which this control is operationalized. Many privacy advocates and theorists define privacy in precisely this way. For example, Alan Westin 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.”²¹ 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.”²² One could therefore argue that a consent-based privacy regime clears away definitional difficulties by endorsing one particular definition.

Another way to characterize a consent-based privacy regime is to view it as a model of individual choice. According to this model, it is individuals who both define privacy for themselves and decide what level of privacy they wish to enjoy. In this way, this model does not depend upon a definition of privacy as control over information; an individual choice model would largely allow for a plurality of such definitions—each individual may choose not only according to his or her own privacy preference levels but also according to his or her own definition of privacy. Moreover, individuals make their own decisions with respect to the trade-off between privacy and other values.

A consent-based regime of privacy protection therefore appears to get beyond many of the definitional difficulties inherent in other types of privacy regimes by either

²¹ Alan Westin, *Privacy and Freedom* (New York: Ateneum, 1967), 7.

²² Charles Fried, “Privacy” *Yale L. J.* 77 (1968), 482.

implicitly endorsing a definition of privacy as control over personal information or by leaving the question of definition up to the individual. Furthermore, according to both iterations of a consent-based regime, derogations from consent are derogations from privacy. If privacy is defined as control over personal information then a lack of consent is easily construed as a lack of control and therefore a lack of privacy. Derogations from consent can still be generally understood as derogations from privacy if one moves from a privacy-as-control model to an individual choice model. The only additional premise that is needed is the claim that in those circumstances where consent is diminished that individuals would in fact have chosen to preserve their privacy rather than give it up; if they would choose to give it up, then there is the possibility that derogations from consent provide the same level of privacy protection. Both privacy-as-control and privacy-as-individual-choice therefore capture the pervasive view that consent is centrally linked to privacy protection.

However, despite the promise of consent-based privacy regimes, the next section argued that there are in fact strong reasons to be skeptical of this claimed connection between consent and the protection of privacy. As will be outlined, the case can be made that derogations from consent are not necessarily derogations from privacy.

(b) The Case for Skepticism

While the promise of consent-based approaches to privacy lies in their seeming ability to empower individuals within the marketplace as well as to circumvent problems

regarding the definition of privacy, the case for skepticism is rooted in the many ways this individual empowerment remains elusive and these definitional problems reappear.

For example, control-based accounts of privacy are susceptible to a number of criticisms that show how they do not really overcome the definitional dilemma of privacy. One of their defects is that they cannot answer the question: control over what? Without an answer to this question, we are left with the value of control itself, which would make privacy indistinguishable from liberty or autonomy. Instead, privacy must be defined in relation to what an individual is *entitled* to control rather than to the norm of control itself.

This concern lies at the root of two prevalent criticism of control-based theories of privacy: that control is neither necessary nor sufficient for the protection of privacy.²³ For example, W. A. Parent provides the example of an individual who “invents a fantastic X-ray device”, allowing him to look through the walls of my home. I thereby lose control over the disclosure of information regarding the activities taking place within my home even if nobody actually uses the X-ray device.²⁴ Nonetheless, my privacy is only lost if someone actually uses the X-ray to look into my home. Similarly, if I lose my personal diary and another finds it but does not read it and does not show it to anyone else I might want to say that my privacy has been respected even though I have no control over my personal information. In this way, control is not a necessary condition for

²³ See Lisa M. Austin, “Privacy and the Question of Technology” [cite] for a fuller treatment of this debate.

²⁴ W.A. Parent, “Recent Work on the Concept of Privacy” (1983) 20 Am. Phil. Q. 344. See also W. A. Parent, “Privacy, Morality, and the Law” (1983) 12 Phil. & Publ. Aff. 272-4.

privacy; I may have no control over the collection, use and disclosure of personal information and still suffer no loss of privacy.

One might still want to point to Parent's example and argue that even if privacy is not lost until someone actually uses the X-ray, it is nonetheless threatened because it is subject to the whim of the X-ray inventor. But even here, a complete account of this threat cannot come from the idea of the control that the X-ray inventor has. That someone controls some aspect of my life is troubling—even wrongful—but does not tell us why we should label that aspect "privacy." The fact that we consider the X-ray use a threat to privacy rather than to some other value depends upon the sense of the privacy of the home that we already have, and which operates in the example independently of the idea of control.²⁵

But neither is control a sufficient condition for privacy. It is not sufficient, because it seems plausible—indeed, persuasive—to argue that one can consent to give up one's privacy.²⁶ That is, if an individual consents to a request that her personal diary be published on the internet we would want to say that the individual has consented to give up her privacy. Privacy therefore appears to be a concept that is, in some fundamental manner, independent of the notion of consent. Similarly, as Ruth Gavison points out, we often want to criticize individuals for not choosing privacy.²⁷ If such a criticism turns out to be of the nature: "you should not have chosen to give up control over that," then

²⁵ I may also control access to my home, but this is an idea of property, not privacy.

²⁶ Anita Allen, "Privacy-as-Data Control: Conceptual, Practical and Moral Limits of the Paradigm" (2000) 32 Conn. L. Rev. 861.

²⁷ Ruth Gavison, "Privacy and the Limits of Law" *Yale L. J.* 89 (1980): 428. Reiman, "Driving to the Panopticon," 30-31, similarly points out that there are activities that we consider private and which we are not permitted to choose to perform in public, such as excretory functions. To explain this, our concept of privacy must be independent of the concept of control.

privacy looks more like autonomy, where we are concerned that adults make their own choices and retain the ability to do so. But if such a criticism rests on a different understanding of impropriety than simply the giving up of control, then we need an account of this. In other words, we need a definition of privacy that can identify a loss of privacy independently of identifying a loss of control.

To argue that control is neither necessary nor sufficient for the protection of privacy is not to argue that control is not in some way deeply connected to the protection of privacy. Privacy may in fact be well protected in many instances by providing individuals with control over their information. Control may also protect other important and related values, such as autonomy. What this argument does suggest is that privacy is not adequately *defined* as control over information. And this suggestion opens the possibility that some derogations from a consent-based model of privacy protection do not actually represent a lower level of privacy protection.

The case for skepticism also holds once one moves from a privacy-as-control model to an individual choice model. Although the connection between consent and privacy is less direct on this model, derogations from consent can still be generally understood as derogations from privacy. The only additional premise that is needed is the claim that in those circumstances where consent is diminished that individuals would in fact have chosen to preserve their privacy rather than give it up; if they would choose to give it up, then there is the possibility that derogations from consent provide the same level of privacy protection. Assuming that this latter suggestion is unlikely, there are

nonetheless two major difficulties with an individual choice model of privacy protection. First, individual choice may in some cases provide illusory protection. Second, sometimes individual choices regarding privacy have negative externalities so that it is the individual who benefits from the collection of personal information but it is others who, at least partially, bear the privacy costs. Third, an individual choice model can sometimes overprotect privacy. These problems are outlined in further detail below and call into question strong assertions that derogations from individual consent must lead to derogations from privacy. In fact, if such derogations address these issues then they could potentially lead to stronger privacy protection.

As many of the concerns surrounding the new provincial privacy legislation in British Columbia and Alberta focus on derogations from a consent model within the employment relationship, it is important to note that there are good reasons to question employee consent as a source of protection for employee interests. Employment contracts are one area where it is widely agreed that reliance upon freedom of contract will not protect employee interests. The differential bargaining power of employers and employees has led to a number of legal responses. Collective bargaining regimes are one such response to this power imbalance. Other responses that operate within the individual contractual paradigm include legislated employment standards that cannot be contracted out of, such as minimum wage laws. Another significant feature of employment contracts is that they purport to regulate a relationship rather than a discrete transaction.²⁸ Because it is difficult to specify in advance all of the further details of this relationship, courts have been willing to import implied terms. Some of these are implied terms of fact,

²⁸ O. Kahn-Freud, "A Note on Status and Contract in British Labour Law" (1967) 30 Mod. L. Rev. 635.

which purport to reflect the intentions of the parties. However, many of these are implied terms of law and are best understood as reflecting policy determinations as to what the employment relationship *should* look like.²⁹ Considerations arising out of our experience with employment contracts in general therefore counsel caution in accepting the proposition that a consent-based privacy regime will in fact protect individual interests, particularly within the context of relationships analogous to the employer-employee relationship. Moreover, the move towards implied terms of law suggests that a determination of privacy must reflect a sense of what is reasonable within a particular relationship and not a unilateral individual definition. This in turn reintroduces the definitional problem of privacy.

Focusing on these two issues of relationship and bargaining power as they arise in the employment context can help to highlight deficiencies in the individual choice model of privacy within the context of more traditional market transactions. Even if transactions do not take place within such a complex relationship as the employment relationship, some aspects of information collection, use and disclosure may raise analogous issues. For example, in some contexts it is difficult to specify in advance all of the ways in which personal information will be used and so fairly general language may be resorted to. Even if the language is fairly specific, individuals may not fully appreciate the potential effects of some information practices, especially if they involve the storage and future uses of information. Individual consent in such circumstances may be inadequate to fully protect individual interests. Furthermore, the personal information collected pursuant to any

²⁹ Geoffrey England, "Individual Employment Law" Irwin Law, 2000 at 28. Nonetheless, it is also important to note that these implied terms do not necessarily favour the employee's interest.

particular transaction may not be information to which an individual attaches a strong privacy interest. However, the cumulative effects of individual choices in many particular transactions with many different parties may result in a diminishment of privacy that is *not* desired by the individual. The effects of the aggregation of information are not well captured by a model that seeks to protect privacy at the level of individual transactions.

Another concern about an individual choice model is that consumers, as *individuals*, do not have a great deal of bargaining power within the market. An individual consumer can usually only choose from what is offered on the market rather than negotiate for goods or services; what is offered is dependent upon whether there are other consumers who are willing to pay for the goods or services. If enough people desire the same level of privacy protection as that individual, then the good or service will be offered in a manner that provides the desired level of privacy protection. In such a scenario, the individual's privacy interest may be protected through individual choice. However, if other people do not desire the same level of privacy protection then the service in question may only be offered with the undesirable privacy consequences, and the only choice available to the individual is between the service and his or her privacy.³⁰

An individual therefore has little recourse where his or her preferences differ from the majority of people. At best, he or she can pay more for this preference, but cannot pay the same for services that impinge less upon his or her privacy. In other words, unless many individuals desire the same high level of privacy, the choice may in fact not be

³⁰ Paul M. Schwartz refers to some of these problems as "the autonomy trap." See "Internet Privacy and the State" (2000) 32 Conn. L. Rev. 815 at 821 ff.

offered in a manner that is meaningful to the individual. But unless a meaningful choice is presented to consumers, then the fact that consumers can consent to the choice presented does not necessarily protect privacy in any rigorous manner. It will definitely not protect privacy if that protection actually imposes any additional costs on a business beyond the costs of obtaining consent.

The foregoing analysis also highlights one of the social aspects of privacy: the choices made by others can affect the choices available to any particular individual. There are two other elements to this social dimension of privacy that are important to mention. The first is that the choices made by other people may in fact provide others with indirect information about you. For example, this is how so-called “DNA dragnets” work in the context of investigations into some violent sexual crimes: police ask for voluntary DNA samples from individuals within a certain area in order to rule out potential suspects.³¹ Numerous concerns arise out of this practice, including the validity of individual consent in such circumstances and the retention of the samples. However, another concern is that when large numbers of individuals do comply with such requests, individuals who refuse become singled out as suspects. In this way, personal information that is voluntarily provided by a number of people leads to the drawing of inferences about another individual. Within this context provided by the choices of others, individuals who refuse because of privacy concerns look like they have something to hide. One could argue that in such circumstances an individual’s right to refuse consent in order to protect privacy in fact leads to the violation of privacy by singling out an

³¹ Examples of such “searches” include the recent Holly Jones murder investigation in Toronto.

individual for more intrusive surveillance. Consent in such circumstances does not provide meaningful privacy protection.

A second important social dimension of privacy arises out of the intersubjective nature of some information. An individual choice model depends upon the idea that personal information is information that is about that individual and over which that individual is entitled to exercise control. However, there are many kinds of information that may be about several individuals and the model of individual control will be inadequate. Health information in general, and genetic information in particular, is often thought to have this feature. Individual consent in such circumstances will not be able to protect, and balance, all of the interests at stake.

Finally, an individual control model encounters conceptual problems when seeking to define the circumstances where an individual is not to be provided with control over personal information. As Allen argues, “in so many policy contexts it is wrong to insist on individual control over personal data.”³² There are many circumstances where others require access to personal information that an individual might nonetheless object to. Under an individual choice model, we would expect to find exceptions to consent where we have strong reasons to suspect that individual choice would result in the wrong balance between privacy and competing values. Such cases would include where the social interest in the collection of personal information is in direct conflict with the individual’s interest in such collection—for example, the law enforcement context. In contrast, where the benefits of collection fall to the individual (for example, additional

³² Allen, *supra* note 26 at 841.

service features), it would appear appropriate to allow the individual to determine whether those benefits outweigh any disadvantages to his or her privacy.

However, there are many cases that fall between these extremes and which call for the need to adjudicate between an individual's decision regarding the right balance between individual privacy—informed by that individual's conception of privacy as well as desired level of privacy—and the needs of others. This would seem to either reintroduce the conceptual problems of defining privacy or introduce the risk of an individual choice model actually overprotect privacy to the detriment of other important social values.³³

These difficulties are apparent even in property-based articulations of personal information protection. For example, James Rule has argued that the commercial exploitation of personal information is best addressed through a proprietary right whereby all commercial uses of personal information must be subject to the explicit consent of the individual, who could also demand compensation for its collection and use.³⁴ However, he also indicates that the personal information “deemed ‘functionally necessary’ to initiate and sustain the individual’s access to the service or product ... sought” may be collected without consent.³⁵ Once one grants, as Rule does, that a commercial entity collecting information should not have the sole discretion to determine what is “functionally necessary” for the transaction, then an objective test has to be

³³ See Anita Allen, *Why Privacy Isn't Everything* (Maryland: Rowman & Littlefield Publishers, 2003).

³⁴ James B. Rule, “Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions” 54 U. Toronto L.J. 183.

³⁵ *Ibid.* at pp185-6.

developed. It is difficult to see how this could work without an appreciation and balancing of the costs and burdens of conducting a transaction in a more privacy-enhancing manner against the potential impact on an individual's privacy. Not only is a balancing exercise inevitable, it also calls out for more nuanced understanding of privacy than one that is based on an assertion of a proprietary right of control.³⁶

There are many reasons, therefore, to be skeptical of the claimed centrality of consent to the protection of privacy. Consent-based regimes of privacy protection rely upon either an understanding of privacy as control over personal information or as a matter of individual choice and definition. As the previous discussion has outlined, both approaches have serious defects that suggest that individual consent is not always necessary in order to provide adequate protection to individual privacy. This seems to be in direct contrast to much current rhetoric surrounding fair information practices that suggests that consent is the central vehicle through which the collection, use and disclosure of personal information is limited in a manner that protects privacy. However, the following discussion outlines how this rhetoric is not only in tension with the general theoretical concerns canvassed above but also with a number of articulations of fair information practices themselves. That is, even within the discourse of fair information practices one finds that consent is not the only norm operating to limit the collection, use and disclosure of personal information. Understanding this provides additional weight to the view that not all derogations from consent need to be construed as derogations from the protection of privacy—privacy might be protected in other ways.

³⁶ Rule also accepts the idea that some “sensitive data” should be removed from commercial exchange (*ibid.* at p. 224). This at least implicitly suggests that not all privacy concerns are captured by his proprietary notion of control.

3. Consent and Fair Information Practices

(a) OECD Guidelines

Fair information practices find their most influential articulation in the 1980 OECD Privacy Guidelines, which adopted the following eight principles: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability.³⁷ These principles still represent the international consensus regarding data protection and are considered minimum standards “which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.”³⁸ Canada has been a signatory to them since 1984 and they have deeply informed the development of Canadian data protection law.³⁹

Consent plays an important role in a number of the principles outlined in the OECD Guidelines that seek to place limits on the collection, use and disclosure of personal information. For example, the Collection Limitation Principle states: “There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.”⁴⁰ Therefore the requirement of consent (where appropriate) helps to limit

³⁷ *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Annex to Recommendation of the Council, September 23, 1980[Hereinafter OECD Guidelines].

³⁸ *Ibid.* at para. 6.

³⁹ Canada has tended to refer to these principles as protecting privacy rather than privacy and individual liberties.

⁴⁰ OECD Guidelines, *supra* note 37 at para. 7

the collection of personal information. Of course, as the Collection Limitation Principle also states, there are circumstances in which consent is not appropriate. The “Detailed Comments” section of the OECD Guidelines refers to “[c]riminal investigation activities and the routine up-dating of mailing lists” as examples of such situations.⁴¹

Consent also figures in the principles that speak to the subsequent uses and disclosure of information. For example, the Purpose Specification Principle states: “The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”⁴² Additionally, the Use Limitation Principle states: “Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle]” unless the “data subject” consents to this use or it is authorized by law.⁴³ Taken together, what these principles require is that if information is to be used or disclosed in a manner inconsistent with the purposes for which it was collected, then consent is required unless otherwise authorized by law. This is so even if the original collection of information did not require consent.

Although consent plays an important role in limiting the collection, use and disclosure of personal information, it is important to note that it is not the only norm that plays such a role. As already indicated, the Purpose Specification Principle limits the use

⁴¹ *Ibid.* at para. 52.

⁴² *Ibid.* at para. 9

⁴³ *Ibid.* at para. 10.

and disclosure of personal information to the purposes for which it was initially collected even if that collection did not require consent. Furthermore, under the Data Quality Principle, the collection of information is limited to information that is relevant to the specified purposes: “Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.”⁴⁴ The normative force of this kind of limit does not necessarily depend upon consent. If I consent to collection for specified purposes then one could argue that my consent is limited to information relevant to those purposes. However, the Data Quality Principle would limit information collection even in circumstances where consent is not required.

Apart from information collection, use and disclosure being limited by notions of purpose and relevancy, there is another sense of limits that does not piggy-back upon the notion of consent: we may think that some kinds of information should be protected from collection even if an individual consents to such collection. That is, we may want to argue that some kinds of information should not be collected for some kinds of purposes. This is also reflected in the Collection Limitation Principle. The “Detailed Comments” section of the OECD Guidelines states that the Collection Limitation Principle in fact deals with two issues:

(a) limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and (b) requirements concerning data collection methods. Different views are frequently put forward with respect to the first issue. It could be argued that it is both possible and desirable to enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited. ...On the other

⁴⁴ *Ibid.* at para. 8.

hand, it may be held that no data are intrinsically “private” or “sensitive” but may become so in view of their context and use.⁴⁵

Because the Expert Group could not agree on sensitivity criteria, they instead had the Collection Limitation Principle include the concept of limits in general.⁴⁶ The reference to consent in the Collection Limitation Principle would therefore appear to fall under “requirements concerning data collection methods” rather than “limits to the collection of data” that are considered sensitive. In other words, the OECD Guidelines reflect the idea that norms independent of consent might operate to limit the collection of information considered “specially sensitive.”

(b) CSA Code

The first national Canadian articulation of fair information practices was the Canadian Standards Association Model Code for the Protection of Personal Information (CSA Code)—a voluntary industry standard.⁴⁷ Although modeled upon the OECD Guidelines, the CSA Code outlined ten principles instead of eight: Accountability, Identifying Purposes, Consent, Limiting Collection, Limiting Use, Disclosure and Retention, Accuracy, Safeguards, Openness, Individual Access, and Challenging Compliance.

The principles outlined in the CSA Code differ from those in the OECD Guidelines in a number of ways that are important to the issue of limiting the collection,

⁴⁵ *Ibid.* at para. 50.

⁴⁶ *Ibid.*

⁴⁷ CAN/CSA-Q830-96 [Hereinafter CSA Code]. This was recognized as a national standard in 1996.

use and disclosure of personal information. First, the minimum standard of “knowledge or consent” except where inappropriate found in the OECD Guideline’s Collection Limitation Principle becomes the potentially more robust standard of “knowledge and consent” except where inappropriate in the CSA Code’s principle of Consent.⁴⁸

Second, the Limiting Collection Principle of the CSA Code can also be seen to build upon the OECD Guideline’s minimum standards. It states that “[t]he collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.” While this copies the “lawful and fair means” of the OECD Guideline’s Collection Limitation Principle, it also shifts from a standard of relevancy to purposes as found in the OECD Guideline’s Data Quality Principle to a standard of necessity—which is potentially far more stringent.

Third, the normative basis for understanding limits to the collection of information shifts in the CSA Code almost entirely towards a consent-model. That is, there is virtually no sense within the CSA Code that the collection of some information should be prohibited either because of its nature or the context of its collection. Instead, the “sensitivity” of the information is to be taken into account when determining the type of consent required under the principle of Consent. As the CSA Code states:

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive,

⁴⁸ *Ibid.* Principle 3, s.4.3, emphasis added.

depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.⁴⁹

Furthermore, when determining the form of consent, “the reasonable expectations of the individual are also relevant.”⁵⁰ The choice of the CSA Code, therefore, was to incorporate the OECD concerns regarding “specially sensitive” data into the consent provisions by ensuring that consent to the collection, use or disclosure of such information be explicit. However, the CSA Code does not provide for any further limits to information collection beyond the protection offered by an individual’s refusal to consent.

At tension with this move towards a consent-model, although also included within the full statement of the principle of Consent, is the refusal to deal clause: “An organization may 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.”⁵¹ The potential tension between this provision and the idea of consent lies in the word “legitimate.” If this means that individuals may not consent to purposes deemed “illegitimate” then it is not clear why this statement is part of the full elucidation of the principle of Consent – it would more appropriately be labeled as a limitation on the principle of Consent. However, this interpretation is unpersuasive given both the placement of the failure to deal clause in the Consent section of the model Code and the Code’s decision to protect “sensitive” information through consent itself and not some other idea of limitation. It is

⁴⁹ *Ibid.* s.4.3.4.

⁵⁰ *Ibid.* Principle 3, s. 4.3.5.

⁵¹ *Ibid.* s.4.3.3.

more likely that the idea of “legitimate purposes” is meant to ensure that businesses cannot avoid the protections of the Code simply by requiring consent to very broad purposes that may in fact contemplate information uses beyond those needed for the specific transaction in question. For example, a business may want to collect and use personal information for marketing purposes even if that information is not needed to complete a transaction for services. This principle would require the business to treat these as two separate transactions, each requiring a separate consent.

(c) PIPEDA and the British Columbia and Alberta Models

PIPEDA in some senses represents a departure from the OECD Guidelines in that it adopts the strengthened centrality of the consent provisions as provided for in the CSA Code. PIPEDA incorporates the CSA Code into its legislative structure: section 5(1) provides that, subject to a number of exemptions as outlined in the Act, every organization is required to comply with the obligations of the CSA Code, as outlined in Schedule 1 of the Act. Many of these exemptions deal with the question of when personal information may be collected, used or disclosed without consent. For example, under PIPEDA consent is not required for the collection of information where

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 laws of Canada or a province⁵²

⁵² PIPEDA, *supra* note 1 at s.7(1)(b).

There are similar provisions with respect to the use and disclosure of information without consent for law enforcement purposes.⁵³ Other exemptions for use and disclosure without consent include purposes such as research.⁵⁴ Such exceptions to consent can be characterized as derogations from privacy in order to meet other important objectives.⁵⁵

However, in another sense PIPEDA represents a return to the OECD Guidelines through recognizing potential limits to the collection of information that are not determined, directly or indirectly, through reference to the notion of consent. Importantly, s.5(3) of the Act provides that “[a]n organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.” This last provision was added at the behest of privacy advocates who were concerned that organizations be required to justify their purposes for the collection, use and disclosure of personal information.⁵⁶ In fact, when PIPEDA was originally introduced as Bill C-54 in 1998, it did not have this provision.

Both British Columbia’s *Personal Information Protection Act* and Alberta’s *Personal Information Protection Act* in many respects follow PIPEDA’s consent model

⁵³ *Ibid.* at s.7(2)(a), (3)(c), (c.1), (c.2), and (d). These provisions do raise the question of whether it is too easy for law enforcement agencies to get access to personal information and whether the Charter permits this. See Lisa M. Austin, “One Step Forward or Two Steps Back? *R. v. Tessling* and the Privacy Consequences for Information Held by Third Parties” *supra* note 19.

⁵⁴ PIPEDA, *supra* note 1 at s. 7(2)(c) and (3)(f).

⁵⁵ Some of these might be objectives pertaining to the individual’s best interest rather than the broader social interest. For example, s.7(1)(a) permits the collection of personal information without consent where “the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way”.

⁵⁶ Stephanie Perrin, Heather H. Black, David H Flaherty, and T. Murray Rankin Q.C., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin Law, 2001) at 61.

and, as stated earlier, have been deemed to be “substantially similar.”⁵⁷ Although neither explicitly incorporates the CSA Model Code into its structure, both adopt its framework in many respects as well as PIPEDA’s general framework for limitations on consent. In addition, both incorporate a general reasonable purpose standard in addition to consent in order to limit the collection, use and disclosure of personal information.⁵⁸

However, both the B.C. and the Alberta Act derogate from PIPEDA’s consent model in a number of ways. First, as outlined earlier, both Acts exempt the employment relationship from the consent provisions. However, the claim that this type of derogation from consent represents a derogation from privacy is not as clear as with the law enforcement exemptions outlined above. Information collection, use and disclosure within the employment relationship is still subject to the requirements of notification and reasonableness. If *both* the reasonableness provision and the consent provisions in PIPEDA are means to act as limits to the collection, use and disclosure of information then it does not necessarily follow that a regime of no consent but reasonableness will not adequately protect privacy. What is needed is a better sense of the role that each plays with respect to the protection of privacy.

This relationship between consent and reasonable purposes is also at stake in the second way in which the B.C. and Alberta Acts depart from the PIPEDA consent model. Neither Act follows PIPEDA’s clear statements regarding the need for explicit consent with

⁵⁷ Of course, both Acts also incorporate the many other important elements of fair information practices. However, a discussion of the adequacy of their compliance with these other components is beyond the scope of this paper.

⁵⁸ B.C. Act, *supra* note 3 at ss. 11, 14, 17; Alberta Act 3 ss. 11, 16, 19.

respect to sensitive information and instead outline the circumstances under which implicit consent will be found. For example, under the B.C. Act an individual is deemed to provide implicit consent where notified about the purposes for collection, use or disclosure, given the opportunity to decline, and “the collection, use or disclosure of personal information is reasonable having regard to the sensitivity of the personal information in the circumstances.”⁵⁹ The Alberta Act has virtually identical provisions.⁶⁰ It is not clear that these provisions will result in greater reliance on implicit consent than under PIPEDA. However, given that many privacy advocates view implicit consent as a very weak version of consent that should be limited, this shift in emphasis could be construed as a derogation from PIPEDA’s consent model. It is not difficult to see why: implicit or “deemed” consent is far from the question of actual consent and shifts the focus from the particular individual to a more objective inquiry which can potentially import considerations that stray far from a consent analysis.⁶¹ Nonetheless, the fact that implicit consent may only be found where a reasonableness standard has been met again raises the question regarding the relationship between reasonableness and consent. If reasonableness can also protect privacy, then is a derogation from a standard of explicit consent (if that is the standard) that preserves a reasonableness standard necessarily a derogation from privacy?

In sum, the real question raised by the new B.C. and Alberta legislation is the relationship between the role of consent and the role of a reasonable purpose standard in

⁵⁹ B.C. Act, *supra* note 3 at s.8(3).

⁶⁰ Alberta Act, *supra* note 3 at s. 8.

⁶¹ The experience with implied terms in contract law, which raise similar questions of whether the parties would have actually agreed to the terms or whether policy concerns operate to determine contractual obligations.

securing limitations on the collection, use and disclosure of personal information. If the reasonableness standard can be seen as a source of privacy protection, then it may not be the case that derogations from consent are necessarily derogations from privacy. This paper has already suggested that individual consent is not necessarily a source of privacy protection, indicating that a test for “reasonableness” could indeed provide a privacy-protective function depending upon how a concern for privacy is built into such a test.

The following section outlines the decisions that have been rendered under PIPEDA that have dealt with the relationship between reasonable purposes and consent and argues that these decisions in fact show that it is reasonableness that takes conceptual primacy over consent. As will be discussed in more detail below, where individuals have been properly informed of the purposes for the collection, use or disclosure of their personal information and these purposes have been found to be reasonable, a finding of consent follows. This holds true both within and outside of the employment context. However, this then raises the question of how “reasonableness” is to be determined in a manner that provides strong privacy protection. As will be discussed, the primacy of reasonableness over consent in practice suggests that the definitional difficulties plaguing other areas of privacy protection cannot be avoided in the context of fair information practices. If privacy is indeed to receive adequate levels of protection, such difficulties must be faced head-on rather than avoided through an over-reliance on consent that simply serves to obscure the role of “reasonableness.”

4. Decisions Under PIPEDA: The Priority of Reasonableness over Consent

(a) The Employment Context

PIPEDA applies to employees working in federally-regulated industries. A number of employment decisions under PIPEDA have dealt with the relationship between the principle of consent and s.5(3)'s requirement of reasonable purposes. An examination of these cases reveals that the reasonable purposes provision in fact deeply influences the consent analysis such that consent does not play a significant role. In other words, the employment decisions under PIPEDA would be decided the same way under the B.C. and Alberta Acts even though that legislation exempts the employment relationship from the requirement of consent.⁶²

The first employment case under PIPEDA was ambiguous concerning the respective roles played by consent and reasonable purposes. The case dealt with an employee who, pursuant to PIPEDA, had requested access to her personal information held by her employer. The employer sent copies of its response to union representatives without the consent of the employee.⁶³ The Commissioner agreed that there had been no implied consent to this disclosure to the union representatives and also indicated that under s.5(3) "he was satisfied that a reasonable person would have considered the

⁶² This is particularly interesting, given that most were made by former Privacy Commissioner George Radwanski, who so severely criticized the British Columbia legislation and who has argued on many occasions that "the concept of consent ... is at the heart of any statute purporting to protect privacy." See News Release, *supra* note 5.

⁶³ PIPED Act Case Summary #20 (2001). The employee also complained about a copy of the denial of access sent to an employee relations coordinator. However, that complaint was dealt with under Principle 4.5 (Limiting Use, Disclosure, and Retention) rather than 4.3 (Consent).

disclosure to the union representatives to be unacceptable.” What is not clear is whether the Commissioner’s decision regarding lack of consent in fact followed upon his determination of lack of reasonableness. Another way to put this is to ask whether, if the disclosure had been found to be reasonable under s. 5(3), the Commissioner would have found implied consent to the disclosure.⁶⁴

While this initial employment case is unclear regarding the relationship between these questions, subsequent cases strongly suggest that a finding of implied consent follows a finding of reasonableness, making reasonable purposes rather than consent the primary consideration. Consider a more recent employee case. Two former operators at a telecommunications company complained that their employer had collected information about their work (the volume, duration and type of calls received) without their consent and had used it to evaluate their job performance.⁶⁵ In evaluating this complaint, the Commissioner dealt with s. 5(3) first and found that such collection and use was reasonable under s. 5(3), for “it is appropriate for a company to monitor and evaluate the job performance of its employees and ... since, in this case, an operator’s main function is to answer customer calls, it is likewise appropriate for statistical information about these calls to be used to measure job performance.” The evidence also showed that the employees were informed of these purposes. Turning to the principle of consent, he held that “performance evaluation, an integral part of the employer-employee relationship, is a

⁶⁴ An application was made to the Federal Court where Pinard J. held that an arbitrator had exclusive jurisdiction over the dispute. He also held that the complaint was without merit as there was no disclosure of sensitive personal information that would require explicit consent. See *Diane L’Écuyer v. Aéroports de Montréal*, [2003] F.C.J. No. 573. For a different result regarding the question of jurisdiction see *Eastmond v. Canadian Pacific Railway*, [2004] F.C.J. No. 1043 [Hereinafter *Eastmond*].

⁶⁵ PIPED Act Case Summary #153 (2003).

condition of employment to which the complainants gave implicit consent when they agreed to work for the company.” In this case, therefore, the determination of the consent issue appears to follow the determination of the reasonable purpose question, making reasonableness rather than consent the threshold issue.

This relationship, whereby consent is subordinated to reasonableness, is even more striking in a number of cases that appeared to invite a strong consent-based analysis and yet were determined almost solely according to the reasonableness provision. For example, a complaint was brought by thirty-five employees of a particular company who alleged that their employer was requiring that they consent to a security check and threatening them with loss of employment or reassignment to another division of the company if they did not consent.⁶⁶ The basis for the complaint was that consent under such circumstances could not be considered voluntary. The Commissioner found that the complainants had a choice regarding whether or not to provide consent and so the consent *was* voluntary despite “the potential for negative consequences.” He argued that the pressure felt by the employees did not amount to “duress” and that the key question in the case was not consent but rather “whether the collection itself was reasonable.” With respect to this latter question, the Privacy Commissioner found that the collection was reasonable. The security checks concerned the nuclear products division of the company in question and that division required a license from the Canadian Nuclear Safety Commission (CNSC) in order to produce nuclear fuel. In response to concerns regarding terrorist attacks on nuclear facilities, the CNSC required the security checks in question as a condition of retaining a license. The Commissioner found that both CNSC’s

⁶⁶ PIPED Act Case Summary #65 (2002).

requirement for the collection of information and the company's compliance with this requirement were reasonable and that because of this the complaint of the employees was not well-founded. In this case, therefore, the analysis turned on the issue of reasonableness. The only opportunity for choice that consent provided to employees was the choice between accepting the collection of information or losing their jobs.

Similarly, a complaint was brought by an employee of a telecommunications company who alleged that his employer was forcing him to consent to a security check in order to work in a restricted area of an airport.⁶⁷ The Privacy Commissioner concluded that the complaint was not well-founded, arguing the complainant had a choice with respect to whether to consent to the security check and that the fact that failing to comply with this requirement could result in job loss did not make his consent involuntary. Importantly, the Commissioner "noted the fact that consent is often not unfettered and that it must be looked at in the context of the reasonable person test in section 5(3)." In other words, the Commissioner explicitly acknowledged that for him the protection offered through consent is intrinsically tied to the protection offered by reasonableness.

Even where the Commissioner found an employer to be in violation of PIPEDA, he chose to do so under reasonable purposes rather than under consent. For example, a complaint was brought by a commercial airline pilot who was being asked to sign a form broadly authorizing the U.S. government to obtain personal information as a condition of training on aircraft simulators in the U.S. The Commissioner held that this was unreasonable even though the cost of alternative training in Europe was quite

⁶⁷ PIPED Act Case Summary # 127 (2003).

considerable. Influencing this decision was the fact that the U.S. authorization form failed to meet the requirements of fair information principles and therefore was contrary to Canadian law. To be required to fulfill the request of a foreign government that was contrary to Canadian law when alternatives existed was unreasonable.⁶⁸

Similarly, an employee of a railway company complained to the Privacy Commissioner regarding the use of digital video surveillance cameras, which the company claimed were needed primarily to reduce vandalism, theft, potential liability for property damage, and improve employee safety.⁶⁹ The complaint is reported to be a complaint about the collection of personal information without consent. However, it was determined solely under s.5(3) where the use of the cameras was found to be unreasonable. The Commissioner determined that there was no evidence of a real and specific problem, that it was not clear that the system was effective, and that the company had not considered less privacy invasive alternatives.

On application to the Federal Court, the Court also determined the case primarily under s. 5(3). Lemieux J. disagreed with the privacy Commissioner and held that the use of the video camera was reasonable.⁷⁰ Importantly, he also determined that the first question to answer was the question of reasonableness and then the question regarding consent could be asked. However, he declined to answer the question of consent because “[t]he issue of implied consent was raised but not really argued.”⁷¹ Instead, he found the

⁶⁸ PIPED Act Case Summary #106 (2002).

⁶⁹ PIPED Act Case Summary #114 (2003).

⁷⁰ *Eastmond*, *supra* note 57.

⁷¹ *Ibid.* at para. 191.

collection of information to fall within s. 7(1)(b) of PIPEDA, which permits collection without consent where consent would compromise the availability of information for the purposes of an investigation.

The strong role that s.5(3) plays in influencing the issue of consent has even been explicitly confirmed in some decisions under PIPEDA. For example, the Assistant Privacy Commissioner has recently stated that “[i]n considering the issue of consent with respect to a job requirement that impinges on privacy, the purposes for introducing the measure must be looked at in the context of the reasonable person test outlined in subsection 5(3).”⁷²

There is one recent decision where the Assistant Privacy Commissioner upheld the employer’s information collection under s. 5(3) but held that the principle of consent was nonetheless violated.⁷³ The complainant did not want to consent to what he considered to be excessive claims by his employer for medical information. The Assistant Privacy Commissioner held that the employer’s purpose for collection was reasonable under s. 5(3) and found that the collection was limited to what was necessary for this purpose. However, she found that the principle of consent was violated when the employer sought some of this information directly from the complainant’s specialist rather than requesting the information from the complainant. In this way, this one case upholds the principle of consent as operating independently of s.5(3). However, it is important to be clear regarding what the actual wrong was in the case. The complainant

⁷² PIPED Act Case Summary #281 (2004). See also PIPED Act Case Summary #279 (2004).

⁷³ PIPED Act Case Summary # 287 (2005).

had no reason to object to the employer requiring the information but did have a reasonable objection to the manner in which it was collected. This is not necessarily upholding consent so much as the idea that information should be collected directly from an individual and collected with that individual's knowledge.

In all of these decisions, therefore, consent plays little role outside of the fact that one is held to consent to the employment relationship. Most of the cases turn on the question of whether the purposes for collection are reasonable within that relationship. In other words, they all exhibit the structure adopted by the B.C. and Alberta Acts with respect to the employment relationship. In this context, then, derogations from consent are not necessarily derogations from privacy given that consent plays no apparent role outside of the consent given to the general relationship. Even if these decisions had been made differently, the likely response of employers would be to make the collection, use and disclosure of personal information explicitly a part of the employment contract. Given the general experience with employment contracts, as discussed earlier, it is difficult to see how this would provide employees with more privacy protection than a finding that the collection, use and disclosure of personal information for reasonable employment purposes is an implied term of the employment contract.

Privacy protection in the employment context will come from a strong reading of reasonable purposes, not consent. Here, the concerns arising out of our experience with the reasonable expectation of privacy test are apposite. A reasonable purposes test will not protect employee privacy if it is strongly focused on employer interests rather than

employee privacy. The test cannot be whether, from the employer's perspective, the impugned practices make sense. That is, the reasonable purposes test should not simply weed out non-employment purposes from employment purposes. It must also inquire into the nature of the employee privacy interest at stake and the extent of the purported violation. Moreover, there must be some sense of an employer's obligation to accommodate employee privacy even if this imposes some burdens on the employer. The Privacy Commissioner's analysis in his decision regarding the airline pilot's complaint about U.S. information practices comes closest to meeting the requirements of this kind of analysis but many of the Commissioner's other decisions are disappointingly thin. Part of the difficulty is likely that the former Privacy Commissioner operated explicitly with a definition of privacy as control over information. Such a definition does not lend itself to the kind of balancing analysis required under reasonable purposes and, ironically, because of this can potentially undermine privacy.

Finally, it is important to note the role that notification plays. The B.C. and Alberta Acts require employers to notify employees about information collection, use and disclosure and in the cases under PIPEDA discussed above this was never in question. Even if notification is not tied to consent it is important in order to allow employees to contest the reasonableness of the information practices as well as to effectively exercise the rest of their rights under a fair information practices regime—including the ability to access personal information held about them as well as the right to correct inaccuracies.

(b) Outside the Employment Context

The foregoing analysis of the employment relationship raises a further question regarding the alleged centrality of consent to fair information practices more generally. If consent does not play a meaningful role in the employment context, is there any reason to think that this conclusion is limited to that context rather than signaling something of broader significance? Within the employment context, if an employee consents to the employment relationship and the information practices are known to the employees and considered reasonable within that relationship, then implicit consent is found. The question then is whether, outside of such a complex relationship, a similar structure of analysis ensues. If so, one would expect that where an individual consents to a particular transaction for goods or services, knows about the information practices associated with that transaction, and such information practices are considered to be reasonable, that implicit consent would be found. That is, the result would be the same as if there was simply a notice and reasonableness regime.⁷⁴ According to this analysis, consent would be required only in two types of cases. First, it would be required in those situations where the process of gaining explicit consent was important for ensuring that adequate notification actually occurred so that the consent to the transaction in question is fully informed. Second, it would be required where the information collection, use or disclosure itself amounted to a separate transaction rather than being tied to the initial transaction that was consented to.

⁷⁴ One could withdraw consent, but then it is understood that one is withdrawing from the transaction – i.e., canceling the goods or services.

One of the earliest cases under PIPEDA to demonstrate the purported strength of its consent provisions concerned Air Canada's use of "opt-out" consent for its Aeroplan Frequent Flyer Program.⁷⁵ After PIPEDA came into force, Air Canada distributed a brochure to some of its Aeroplan members outlining how their personal information was used in five different categories. Plan members were instructed to check off an opt-out box beside any of these categories if they did not consent to such use. Upon investigating a complaint brought by a number of Plan members, the Privacy Commissioner determined that the use of opt-out consent in such circumstances violated the consent provisions of PIPEDA. The Commissioner

expressed concern about the potential, in each of the five information-sharing situations, for use and disclosure of information customized according to individual plan members' purchasing habits and preferences. He determined that information of this kind is sufficiently sensitive to warrant obtaining positive or "opt-in" consent, as opposed to negative or "opt-out" consent, from the individuals concerned. Although in the Commissioner's view the practice of using plan members' information for purposes of advertising products, services, and special promotions remains unobjectionable in itself, he was satisfied that a reasonable person would not expect such practice to extend to the "tailoring" of information to the individual's potentially sensitive personal or professional interests, uses of or preferences for certain products and services, and financial status, without the positive consent of the individual.⁷⁶

There are several points to note about this decision. First, the determination of whether consent is to be explicit or implicit makes reference to the expectations of a reasonable person. Second, part of what concerned the Commissioner was the sensitivity of the professional and financial information involved, information that Air Canada collected from what it identified as "external sources" in order to better target consumers as well as to determine their eligibility for certain financial products and services. According to the

⁷⁵ PIPED Act Case Summary #42 (2002).

⁷⁶ *Ibid.*

analysis outlined above, sensitive information might call for explicit consent in order to ensure adequate notification of its collection, use and disclosure.

Third, it was the extension of the information collection, use and disclosure past basic advertising and promotions and into targeted marketing that the Commissioner determined required explicit consent. This also comports with the analysis offered above that explicit consent is required where the information collection, use and disclosure is best characterized as a separate transaction. Here, consumers collect air miles in order to redeem them for certain products and services. Therefore some information practices must be seen to be an intrinsic part of being part of the plan and if a consumer has knowledge of these practices and enrolls within the plan, then they implicitly consent to these practices. However, to the extent that information practices go beyond those needed to the transaction, a separate consent is required. The basis for determining this important cut-off is not consent, but reasonableness.

One of the strongest cases for illustrating the role of the consent provisions under PIPEDA can therefore be read as support for the proposition that the provisions of reasonableness and notification in fact do most of the work in protecting an individual's privacy. The case for such a interpretation of the primacy of reasonableness finds further support in an examination of the cases under PIPEDA that have quite explicitly dealt with the relationship between consent and reasonable purposes. If the application of the consent provisions in general under PIPEDA follow the same pattern as their application to the employment context, then we would expect to find that all the cases that pass

scrutiny under the reasonableness standard of s.5(3) also pass scrutiny under the principle of consent. If, on the contrary, the consent provisions do some independent normative work, than we would expect to find some cases where, despite passing s.5(3) scrutiny, the collection, use or disclosure of information violates the consent provisions of the Act. In fact, there are a few cases that exhibit this last structure. However, a close examination of them suggests that, rather than confirming the significance of consent, they in fact repeat the basic structure exhibited by the employment cases. In other words, consent does not appear to play the central role often claimed of it.

There are two very similar cases that exhibit the general structure of passing s.5(3) scrutiny but failing under Principle 4.3 but which, on closer examination, appear to be about the failure of notification rather than the failure of consent itself.

The first case exhibiting this pattern of complaint dealt with an individual who, in the course of seeking to have his cable service disconnected, was asked to provide his new address as well as his reasons for changing cable providers.⁷⁷ When the individual asked why the cable company required this information, he was told that it was needed to “fill in the screen.” The Privacy Commissioner found that “a reasonable person would view the purposed for collecting this information ... to be legitimate and in accordance with section 5(3).” However, despite passing this reasonable purpose threshold, the cable company was found to have contravened Principle 4.3.2. Principle 4.3.2, as a subsection of the general principle of consent, refers to the requirement of notice and consent. The

⁷⁷ PIPED Act Case Summary #152 (2003). There were other elements to the complaint as well, but only this aspect of the complaint exhibited the structure outlined.

Privacy Commissioner determined that Principle 4.3.2 was violated “because [the cable company] failed to inform the complainant, at the time of collection, of the true purposes for which this information was being collected, and thus did not obtain his valid consent.”⁷⁸ What the Commissioner’s finding turned on, therefore, was the lack of notification of the true (and reasonable) purposes rather than a lack of consent per se. If the cable company had provided such notification, then it does not appear that the Privacy Commissioner would have found a violation of Principle 4.3.2. In other words, his reasoning would have conformed to the pattern in the employment cases where a finding of implied consent followed a finding of reasonable purposes.

A second case dealing with reasonable purposes under s. 5(3) but a lack of consent under Principle 4.3.2 is also best characterized as a case about notice rather than consent. In this case, an individual was required to provide either two pieces of identification or a deposit in order to obtain telephone services.⁷⁹ She was told that the purpose for the identification was to “confirm her identity.” However, upon investigation, the Privacy Commissioner found that the true purpose of such collection in the case of new customers was in fact to run a credit check on the applicant.⁸⁰ While the Commissioner found this purpose to be reasonable under s. 5(3), he found that the telephone company nonetheless violated Principle 4.3.2 because “a reasonable person would conclude that the company did not explicitly state the purpose for its collection of

⁷⁸ For this reason, the cable provider also contravened principle 4.2.3, which requires that “[t]he identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.”

⁷⁹ PIPED Act Case Summary #24 (2001).

⁸⁰ Under CRTC regulations, the provision of telephone services is seen to be an extension of credit.

personal information with respect to first-time subscribers.”⁸¹ In other words, the case turned on the question of notice; if the telephone company had informed the individual of the true (and reasonable) purposes for the collection of her information then there would have been no violation of the consent provisions.

What these cases suggest is that if a consumer is notified about the purposes for the collection of the personal information in question, these purposes are reasonable, and the individual chooses to obtain services, then the individual implicitly consent to the collection of information. However, there is one PIPEDA decision where s. 5(3) is satisfied but principle 4.3 is violated but which cannot be as easily explained as a case about notification rather than consent. The case involved an application for long-distance services from a telecommunications company.⁸² When the complainant filled out his application form, he clearly indicated that he did not authorize a credit check. A company representative suggested to him that in order to avoid a credit check, he should opt for a pre-authorized payment plan, and the complainant did so. However, the company still did a credit check, arguing that “this procedure was mandatory to obtain services, as it serves to verify the credit standing and ensure the financial capacity of the new subscriber.” The Privacy Commissioner held that, although the credit check was reasonable, it was contrary to “the individual’s clear wishes opposing a credit check” and therefore violated Principle 4.3. This case therefore provides a stronger example of the role that consent may play, independent of an inquiry into reasonableness.

⁸¹ For this reason, the telephone company also was found to be in violation of principle 4.2.3.

⁸² PIPED Act Case Summary #193 (2003).

One may still argue that the real problem in the case was the misrepresentation to the individual that the pre-authorized payment plan did not involve a credit check and so the case is really best understood as a case about a failure of notification. More importantly, however, this case does not really answer the question of whether the telecommunications company is permitted, under PIPEDA, to only offer services that are tied to a credit check. While the Commissioner was drafting his findings, the company informed him that it changed its policy to allow for the option of a pre-authorized payment plan in order to avoid a credit check. But if the choice, prior to the official change in policy, had been accurately put to the individual—services with credit check or no services—would the company have been in violation of PIPEDA given that the individual did not wish to consent to a credit check? The Privacy Commissioner’s finding that the credit check was “reasonable” even in the context of a pre-authorized payment plan suggests that no violation of PIPEDA would have been found in such circumstances and that this finding would have been determined by reasonableness rather than consent.

(c) Reasonableness and the Protection of Privacy

As the previous discussion highlights, the analysis of reasonable purposes in fact drives the analysis of consent in decisions under PIPEDA; where the purposes are reasonable and the individual is properly notified of them, a finding of implied consent follows. In fact, it is not clear what independent work consent would do apart from this structure. Another way to describe this structure is to say that an individual consents to a particular transaction but needs to know the informational implications of that transaction. If notified, then the individual implicitly consents to these implications in

consenting to the transaction. When the informational practices are better understood to constitute a separate transaction, then consent to this separate transaction is required. Many of the concerns that motivated the widespread adoption of fair information practices are concerns regarding the way in which companies were collecting personal information that was not needed for the initial transaction and was being used for subsequent interactions such as targeted marketing. Requiring consent to this unnecessary collection of information seems like an appropriate response. However, consent does not help to determine the line between what is required by a particular transaction and what constitutes a separate transaction. Determining this line according to the idea of consent would mean that individuals would be able to unilaterally decide what they think is necessary in the context of a particular transaction and impose this upon businesses. This seems inappropriate. One way to read the previous cases is to argue that the recourse to reasonable purposes is a recognition of the need to balance individual privacy against the needs of businesses and employers to determine what kinds of information practices are required by certain transactions and relationships.

Another option for determining when information practices constitute a separate transaction, requiring a separate consent, would be to reinvigorate the so-called “refusal to deal” provisions. As outlined earlier, under the CSA Code and PIPEDA, a business can not refuse the provision of services to an individual who refuses to consent to the collection, use and disclosure of personal information beyond what is necessary to fulfill the purposes for the collection, use and disclosure.⁸³ One could therefore argue that it is this provision that is best suited to drawing the line between information collection that is

⁸³ PIPEDA, *supra* note 1 Principle 4.3.3.

properly tied to one transaction and information collection that is best construed as a separate transaction.⁸⁴ There are two problems with this approach. The first is that it is not really a balancing test and the concern is that it would not be interpreted in a manner that would recognize that business needs must be balanced against privacy and that business might in fact have a burden to change the way in which they provide goods and services in order to be more privacy friendly. The second is that a finding of necessity really depends on the construal of the purposes. For example, a credit check is necessary for many types of billing options but may not be necessary when considered in light of the broader purpose of payment for services. The question of whether alternative options should be made available seems better asked under reasonable purposes because this is more clearly a balancing test and targets the construal of the purposes directly.

The question then is how to ensure that the determination of reasonable purposes protects privacy rather than simply serving as a vehicle through which to override privacy in the name of other competing interests. One of the problems that have resulted from an over-emphasis on the notion of consent as the central vehicle through which to protect privacy is that a robust reasonable purposes test has not been developed. This can be seen by returning to the issue of credit checks and payment plans in relation to subscribing for certain kinds of services.

⁸⁴ James Rule proposes something similar to this when he argues that explicit consent should always be required unless the information collection is “functionally necessary.” I disagree with his proposal for many of the reasons outlined here (“Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions” *supra* note 34 at 185-6.)

A number of cases that deal with complaints regarding the collection of personal information needed to facilitate a credit check involve situations where an alternative payment plan is in fact available to consumers.⁸⁵ The availability of such an option informs the Commissioner's findings regarding consent and reasonable purposes. However, consider an earlier case, where an individual complained because she was only able to obtain the services in question if she agreed to one of two automatic payment options: the first involved providing information about her bank account, and the second involved providing information about her credit card.⁸⁶ She requested a third option—payment by certified cheque in advance. The company in question refused this request, arguing that they only allowed such prepayments for more expensive combined service packages because of the cost of processing the cheques. The division in question was found to not have a billing system capable of administering such a payment option and only offered it with their combined services package due to an arrangement they had with another division. On these facts, the Commissioner held that the company 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.”⁸⁷

This case is striking because the Privacy Commissioner never asked the question of whether the organization should have to provide a pre-payment option for the same services that did not require providing so much personal information. It is not clear why

⁸⁵ See, for e.g., PIPED Act Case Summary #94 (2002) and #104 (2002).

⁸⁶ PIPED Act Case Summary #48 (2002).

⁸⁷ The Privacy Commissioner also determined that, under Principle 4.3.3, that “processing payments for service” was “legitimate” under “legitimate purposes”. *Ibid.*

an organization should be able to determine its own billing options without taking into account the need to provide privacy-protective options or providing evidence as to why it could not do so. Perhaps the Privacy Commissioner was concerned not to place an undue burden on businesses to change their billing systems in order to accommodate the desires of a minority of individuals. However, if PIPEDA is to be a privacy-protective regime and not simply an enabler of electronic commerce, then it should require an organization to make privacy-protective choices available to individuals even if these choices do not represent the most cost-effective business practices possible. And this requires a robust reasonableness test that gives greater weight to the privacy interest at stake and requires evidence as to why a more minimally-intrusive option would place too heavy a burden on the business in question.

Another important issue that this case highlights is how important it is to place privacy obligations on companies prior to the setting up, or upgrading, of information systems. Because contemporary information-processing systems, including billing systems, rely upon information technology that is often expensive to set up and costly to change once set up, many decisions with important privacy implications are made prior to an individual being presented with any choices regarding services and transactions. Paying attention to how such systems are configured and the ways in which they enhance or further erode privacy is crucial. Indeed, this concern echoes one of Larry Lessig's central claims in his influential analysis of the internet: "Code is law."⁸⁸ That is, once built the architecture of cyberspace—the software and hardware that make it what it is—helps to shape the kind of interactions that may take place there. Regulating interactions

⁸⁸ Larry Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999) at 6.

after the important architectural decision have been made fails to see the important value choices that either deliberately or inadvertently get built into the technology.

Technologies and the specific value choices embedded in them come to function as a kind of legislation that is created outside of our normal political and legal institutions and are potentially quite difficult to alter after the fact. Similarly, a focus on the choices that a business makes available after their information systems have been set up fails to appreciate the need to require that privacy values be built into these systems from the outset.

What this might mean concretely is a far greater emphasis on the ability to engage in anonymous transactions or pre-payment plans than is currently the norm. Privacy advocates such as Roger Clarke have argued that ensuring anonymity is one of the most important emerging privacy challenges of the 21st century, and have expressed skepticism regarding the ability of fair information practices to meet this challenge without substantial revision.⁸⁹ What this paper suggests is that recognizing the work that “reasonable purpose” does in legislation like PIPEDA and ensuring that it does in fact provide a robust protection for privacy, rather than an excuse for its erosion, is the most promising manner through which to address these more systemic concerns.

What, then, should a test for “reasonable purposes” look like? The most promising test to emerge from the decisions of the Privacy Commissioner, and which was recently endorsed by the Federal Court in *Eastmond*, asks four questions:

⁸⁹ Roger Clarke, “Beyond the OECD Guidelines: Privacy Protection for the 21st Century” (<http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html>.)

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the benefit gained?
- Is there a less privacy-invasive way of achieving the same end?⁹⁰

These questions, particularly the last one, seem well-suited to address a number of the concerns that have emerged in this discussion. In particular, businesses should have to provide evidence as to why services cannot be provided in other, more minimally intrusive ways. However, this test will not adequately protect privacy unless it includes, as a first step, an inquiry into the nature and extent of the privacy interest at stake.

Without this, the test looks like a kind of orphaned Oakes test from *Charter* jurisprudence—defining when a right might be limited but missing the important initial step of defining the right in question and the manner in which it is being violated.

Because of this, the danger is that this test for reasonable purposes will become a test for limiting privacy rather than enhancing it. To counter this danger, what is needed is a return to the very difficult questions involved in defining privacy and its value. In other words, fair information practices must grapple with, rather than avoid, the same challenges facing other regimes of privacy protection such as constitutional law.

5. Conclusions

In sum, an examination of the decisions under PIPEDA indicates that “reasonable purposes” plays a large analytic role in PIPEDA’s articulation of fair information practices and in fact often drives the analysis of consent. The PIPEDA cases that deal with the relationship between consent and reasonable purposes reveal that consent is important in terms of consenting to the general transaction or relationship in question.

⁹⁰ *Eastmond*, *supra* note 64 at para. 13.

Notification provisions ensure that this consent is informed in the sense of alerting the individual to the informational consequences attached to the transaction or relationship. A separate consent to the information practices is important only where this might be necessary to ensure that proper notification occurred or where the information collection in question is better understood to form a separate transaction requiring its own consent rather than as part of the initial transaction. In this sense, consent can still safeguard some dimensions of choice. However, the question of whether the information collection, use or disclosure is appropriate within the particular transaction or relationship is dealt with under the reasonable purposes provision rather than consent. It is reasonable purposes, therefore, that holds out the promise of requiring meaningful choices to be presented to consumers. It is reasonable purposes that has the most potential for providing a high degree of privacy protection. Therefore derogations from consent that nonetheless preserve notification and reasonable purposes do not necessarily represent derogations from privacy.

However, what this further suggests is that much more attention needs to be paid to the interpretation of reasonable purposes so that it may fulfill its potential and provide strong privacy protection. What this requires is a return to the definitional difficulties that regularly surface in other regimes of privacy protection and an attempt to provide a workable understanding of privacy and its value, especially in the context of emerging technologies. To evade this responsibility through an over-emphasis on the value of individual consent is to provide inadequate and highly illusory protection for privacy.