

**IS YOU IS OR IS YOU AIN'T:  
Making PIPEDA's Rights Language Meaningful By  
Re-Viewing Social Value**

*Penultimate Draft:  
Please do not cite, copy or quote without permission.*

jennifer barrigar  
January 2006

*It is the question: does one primarily protect people or does one protect data? Out of that polarity arise two essential climates or models from which I perceive that the discussion of your task has come.*

*First, there is the climate and the model of human rights. All the notions of privacy can trace back their origin and validity primarily to considerations of human rights. When human rights informs the language in which the discussion among you and the general public and Parliament takes place, you speak then, rightfully, about citizens and all that comes with that. On the other hand, if the emphasis is primarily on the protection of data one does look at a market model, one does look at an economic model, and all the things you've heard about the new economy. Then it is the language of the market that informs your discourse.*

*You talk then, and everybody who speaks with you speaks about consumers, about providers, about service. When those who primarily locate themselves in the human rights climate speak about citizens, about the relationship between groups and power, those who are in the market language speak primarily about stakeholders. And when one speaks about rights and obligations, others speak about binding contracts. When out of that human rights climate one derives instruments which require independent supervision those in the market climate will speak about functional analysis and choices. When one speaks about regulation and about the roots and moral and legal justification of law and regulation, the people on the economic model using the market language, will talk about monitoring and voluntary guides.*

*When the human rights approach looks at infrastructures that are appropriate for enforcement, the people in the market mentality and language think about correcting market failures. When the health and welfare data, for example, get into the wrong hands, our friends speak about correcting market failures, when I would speak about infringements of human rights. There are differences, and these indeed are the forces that are shaping the stormy and turbulent weather that is ahead of you.*

-Dr. Ursula Franklin, 1996-

A: Introduction

Canada's *Personal Information Protection and Electronic Documents Act*<sup>1</sup> speaks in its purpose clause of recognizing "the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."<sup>2</sup> No definition of privacy itself is provided.<sup>3</sup> Given the multiplicity of potential meanings of the term, in order to assess PIPEDA we must first explore the idea of privacy. After all, how we conceptualize a right has a powerful impact in assisting to "clarify our consideration of the degree of protection available, the nature of the derogations or exceptions, the priorities to be afforded to various rights, the question of whether a series of rights will be treated in hierarchical relationships, and similar problems."<sup>4</sup>

The language of the purpose clause contains within it an unresolved tension, one which is fundamental to the implementation of the Act. Is it a "right of privacy" which is being protected – an inherent, inviolable right – or is it a "right of privacy with respect to personal information" which is protected – privacy as control? Either way, the language of PIPEDA lies open to interpretation, providing an avenue for re-viewing privacy under PIPEDA without the necessity of amending the Act.

---

<sup>1</sup> *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [PIPEDA].

<sup>2</sup> PIPEDA *supra* note 1, s. 3.

<sup>3</sup> In fact, PIPEDA makes very few references to privacy at all. The term appears only five (5) times in the Act: twice in the s. 2 definition of "Commissioner" as the Privacy Commissioner appointed under the Privacy Act, once in the s. 3 purpose clause, and in references to the Privacy Act under s. 4(2)(a) and s. 26(2)(a).

<sup>4</sup> Jerome J. Shestack, "The Jurisprudence of Human Rights" in Theodor Meron, ed., *International Law of Human Rights*, vol. 1(Oxford: Clarendon Press, 1984) at 74.

The development of privacy protections pursuant to one of the other of these concepts has particular implications for the content of those protections and the social meaning of privacy in the legal landscape.

In order to explore this, I shall first re-view each of the concepts which are in tension in PIPEDA. By exploring the development and content of privacy as social value and of privacy as individual control, I will provide the necessary reference point(s) for a re-view of PIPEDA itself.

Second, I will explore the positioning of PIPEDA by looking both at the forces at work in the development of PIPEDA and at the structure of the Act itself.

Building on the structure of PIPEDA, I proceed to a review of PIPEDA in the employment context. Keying on the stages of consent, needs of organizations, and the interest balancing inherent in the appropriate purposes test, I review both how PIPEDA has been implemented to date and how it might be revitalized by a conceptualization of privacy as social value.

The history and development of PIPEDA has led, almost inevitably, to it being constructed as a data protection statute. This orientation has serious implications for the long-term meaningfulness of PIPEDA as a substantive privacy right. In order to re-dress this, it will be necessary to redefine the privacy right PIPEDA recognizes as one which transcends individual choice and instead key on notions of privacy as social control.

B: Concepts in TensionPrivacy as Social Value

Val Steeves speaks of privacy as “a fundamental human right that goes to the core of preserving freedom and autonomy, and is essential to the workings of a healthy democracy.”<sup>5</sup> Justice LaForest made a similar point when he wrote that “grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.”<sup>6</sup>

Understanding privacy as a right, then, must take account of different aspects of the right. While privacy is an individual right linked to individual dignity and autonomy, there is also a larger, social value to privacy which must not be overlooked.

Privacy has historically been conceptualized as a right and linked with notions of dignity and autonomy. In 1948, for instance, the United Nations included privacy protections as Article 12 of the Universal Declaration of Human Rights.<sup>7</sup> More meaningfully perhaps for Canada, since Canada did not directly implement the Universal Declaration, is the 1966 International

---

<sup>5</sup> Val Steeves, “A Better Road Map for the Information Highway: Critical Human Rights Issues in the Access and Privacy Field” (Paper presented at the Access & Privacy: the New Way of Doing Business conference held by Management Secretariat of the Government of Ontario, 12 September 1997 at 3. online: University of Ottawa Human Rights Research and Education Centre <<http://www.uottawa.ca/hrrec/publicat/mbs.html>> [Steeves, “Road Map”].

<sup>6</sup> *R v. Dymnt*, [1988] 2 S.C.R. 417 at 427.

<sup>7</sup> <http://www.un.org/Overview/rights.html>.

Covenant on Civil and Political Rights.<sup>8</sup> Article 17 of that instrument speaks similarly of privacy as such a right.<sup>9</sup>

In Canada, in 1977 Canada introduced data protection provisions into the Canadian Human Rights Act. These Provisions<sup>10</sup> covered information on natural persons which was held by the federal government and had been used in making decisions about the individual concerned. Although this Part of the Act is no longer in force, the decision to use the vehicle of the Canadian Human Rights Act is a significant one, underscoring notions of human dignity which are inextricably tied to privacy.

1982's *Canadian Charter of Rights and Freedoms*<sup>11</sup> does not explicitly include privacy in its protections, although some privacy interests have been found to be protected under section 7, 8 and 2(b) of the Charter.<sup>12</sup>

Under the Charter, it is clearly established that privacy protection inures to persons rather than to goods or places.<sup>13</sup> This should not be taken to mean, however, that privacy is of value only to individual persons or that privacy has no social value. Indeed, as Justice Gonthier noted, privacy is integral to the “preservation of a free and democratic society.”<sup>14</sup>

---

<sup>8</sup> <http://www.hrweb.org/legal/cpr.html>.

<sup>9</sup> Canada acceded to this in 19 May 1976.

<sup>10</sup> Part IV of the *Canadian Human Rights Act*, S.C. 1976-77, c. 33. Part IV of the *Canadian Human Rights Act* was repealed (S.C. 1980-81-82-83, c. 111 (Sch. IV, s. 3)) and replaced by the *Privacy Act* (S.C. 1980-81-82-83, c. 111, Sch. II).

<sup>11</sup> *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982.c. 11 [Charter].

<sup>12</sup> A.W. MacKay, “The Waves of Information Technology, the Ebbing of Privacy, and the Threat to Human Rights” (1999) 10:3 N.J.C.L. 411.

<sup>13</sup> *Hunter v. Southam*, [1984] 2 S.C.R. 145.

<sup>14</sup> *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773 at 789.

Priscilla Regan has argued that “privacy serves not just individual interests but also common, public and collective purposes.”<sup>15</sup>

In speaking of privacy as a common value, Regan is not merely asserting that all people in this society agree that privacy is of value or is a value. Rather, this is grounded in the recognition that all individuals value some degree of privacy. They may define it differently but there exists a common core that provides space in which they may define what they believe or what they wish to keep private.<sup>16</sup> Regan analogizes this to classical liberalism’s emphasis of the value to society of liberal freedoms in creating not only fullness of personal development but the usefulness to society of those developed individuals.<sup>17</sup> Thus “a prior commitment is made to an overarching concept of privacy from which we derive the meaning of privacy in particular circumstances.”<sup>18</sup>

Privacy may also be recognized as a public value. In part, this is what writers such as Val Steeves allude to when they speak of privacy as a foundational right upon which other human rights are built,<sup>19</sup> but that is only part of it. Privacy is not merely a procedural necessity for other rights – it is a right in itself. Regan suggests that “relating the importance of privacy to the ability of constructing a public, and to the development of trust and accountability, would expand the list of public functions that privacy performs and might make clearer that privacy itself is an essential element to a good society.”<sup>20</sup>

---

<sup>15</sup> Priscilla M. Regan, *Legislating Privacy: Technology, Social Value, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995) at 221 [Regan, “Legislating Privacy”].

<sup>16</sup> *Ibid* at 221.

<sup>17</sup> *Ibid* at 222.

<sup>18</sup> *Ibid* at 225.

<sup>19</sup> Val Steeves, “A Response to Professor Walter’s Article “Digitizing Technology, Transforming Ourselves”” (1999) 10 N.J.C.L. 445 at 448 [Steeves, “Response to Walter’s”].

<sup>20</sup> Regan, “Legislating Privacy” *supra* note 15 at 227.

Finally, Regan speaks of privacy as a collective value, recognizing that technology and market forces make it difficult for any one person to have privacy without all persons having some minimum level of privacy. Interests of third-party record holders – between patient, doctor, insurance company and employer, for example – the non-voluntary nature of many record-keeping relationships and the ever-growing abilities of computer and telecommunications technologies make individualized solutions to privacy difficult, if not impossible.<sup>21</sup>

David Flaherty writes that:

...privacy is and always has been under attack in the Western world from either surveillance ideology or technology or both... Thus, one of the goals of liberal democratic societies has been to legitimize concern for personal privacy by constitutional and legal means at points where the individual can no longer control his or her preservation of privacy because of competing goals.<sup>22</sup>

The way(s) in which this situation is addressed run the risk, however, of being threat- or issue-specific and neglecting to articulate or reinforce the larger social value of privacy.

#### Privacy as Control: Data Protection

As information technology developed and advanced in the 1960s and 70s, public and private organizations were able to process ever-increasing amounts of information about individuals.

---

<sup>21</sup> *Ibid* at 228.

<sup>22</sup> David H. Flaherty, "Visions of Privacy: Past, Present, and Future" in Colin J. Bennett and Rebecca Grant, eds. *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999) 19 at 27.

As people became increasingly concerned about their ability to protect their privacy, states began to recognize the necessity of, and attempting to govern such activities.<sup>23</sup>

As state- and country-specific data protection laws were enacted, concern arose that disparate national data protection schemes could hinder the free flow of information across borders, causing disruptions in important sectors of the economy. Accordingly, both the Council of Europe<sup>24</sup> and the Organization for Economic and Cultural Development (OECD)<sup>25</sup> created documents which set out fair information principles and attempted to harmonize transborder data flow issues by setting standards of cooperation, consultation and assistance. These principles were expected to form a template for national legislation.<sup>26</sup>

Both documents had in common a set of fair information principles, mandating:

1. public knowledge of personal record-keeping systems
2. rights of access and correction by individuals to their own data.
3. requirement that personal data should only be collected for legitimate and openly stated purposes.
4. that personal data should only be used (internally) in ways that are consistent with those purposes.
5. that personal data should only be disclosed (externally) in ways that are consistent with those purposes.
6. That there should be adequate and appropriate security safeguards.<sup>27</sup>

---

<sup>23</sup> Roger Clarke, "Beyond the OECD Guidelines: Privacy Protection for the 21<sup>st</sup> Century" online: <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html#ScopeDP> [Clarke] notes: "The first laws that expressly protected information privacy were passed in Europe in the early 1970s. The West German Land of Hesse passed its Datenschutzgesetz (Data Protection Act) in 1970, and that term quickly came to be used in virtually all discussions. Sweden's Data Act of 1973 was the first such legislation at national level. A succession of Continental countries followed, including Germany in 1977 and France in 1978."

<sup>24</sup> *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe Convention 108)* online: <http://www.coe.int/treaty/EN/cadreprincipal.htm>.

<sup>25</sup> *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* released 23 September 1980. Canada signed on June 1984. online:

[http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html).

<sup>26</sup> online: [http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_119820\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html).

<sup>27</sup> Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992) [Bennett, "Regulating Privacy"].

The OECD Guidelines were non-binding, and not all European nations ratified the Council of Europe Convention. Accordingly, in 1990 the European Union began working towards an EU Directive on data protection, and in 1995 the European Union formally adopted the *Directive on the Protection of Personal Data With Regard to the Processing of Personal Data and the Free Movement of Such Data (EU 95/46)*.<sup>28</sup> The EU Directive too was predicated on fair information principles.

At their most basic, then, data protection instruments consist of a series of procedural directions which are intended, if adhered to, to protect privacy by controlling the collection, use and disclosure of personal information. Data protection may be said to be concerned, then, with procedures for privacy rather than with privacy itself. Indeed, Raab and Bennett concede that “privacy as a goal has often been transmuted into data protection.”<sup>29</sup> We must recognize, however, that the two are not synonymous. Data protection presumes the use and disclosure of personal information, thus creating (if anything) a limited right of control over what organizations do with one’s personal information. There is little or no acknowledgement that one might wish to prevent anything being done with the information or, indeed, the information being collected in the first place. Instead, it focuses on reducing harm to the individual accruing from use or disclosure of the information.<sup>30</sup>

Also, although data protection schemes may be created in response to social issues or threats, the schemes themselves have an individual and transactional focus. This effectively isolates the threat rather than contextualizing it in the larger social value of privacy analysis.

---

<sup>28</sup> Online: [http://europa.eu.int/comm/internal\\_market/privacy/law\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/law_en.htm).

<sup>29</sup> Charles D. Raab and Colin J. Bennett, “Taking the Measure of Privacy: Can Data Protection Be Evaluated?” (1996) 62 Int’l. Rev. Admin. Sci.535 at 537 [Raab and Bennett].

<sup>30</sup> *Ibid* at 540.

Roger Clarke critiques fair information practice-based privacy regimes as “an official response which legitimated dataveillance measures in return for some limited procedural protections.”<sup>31</sup> Raab and Bennett have gone further, suggesting that not only do data protection schemes presume availability of information, thus implicitly authorizing its use but “the political reality has often been that reaping the commercial and administrative benefits that stem from information technology and data-usage, rather than privacy protection, has prompted the legislation in the first instance.”<sup>32</sup>

There is, then, a strong administrative and economic efficiency bias which seems to underlie data protection schemes, and this must be borne in mind when evaluating them.

### C: Positioning PIPEDA

#### Evolution of PIPEDA

Re-viewing the history of PIPEDA’s development and drafting, it is clear that there was an unusual amount of economic and business interest and involvement from the very beginning.

Although Canada had enacted the *Access to Information and Privacy Acts* in 1983 and signed on to the OECD Guidelines in June 1984, Colin Bennett suggests that “the agreements of the 1980s, chiefly the Council of Europe Convention and the OECD Guidelines had had a

---

<sup>31</sup> Clarke, *supra* note 23.

<sup>32</sup> Raab and Bennett *supra* note 29 at 540.

negligible impact on the personal data practices in Canada.”<sup>33</sup> While various private sectors articulated some form of fair information principles<sup>34</sup>, there was no substantial move towards them in Canada.

By the 1990s, however, it was clear that the proposed European Union Directive on the Protection of Personal Data would substantially change the landscape. Of particular concern to government and private industry were the standards imposed in that document regarding transborder flows of data. The draft of the Directive circulated in the mid-1990s stated that transfer of data to a third country is only allowed where that third country offers an adequate level of data protection. This raised fears of business relationships between European countries and Canada being blocked on the grounds that no adequate level of protection for personal data was provided. The draft also suggested that adequacy would be measured with regard to the nature of the data, the purpose and duration of the processing operation, the existence and scope of the general and sectoral data protection legislation in place, and any professional rules or Codes that applied.

This galvanized a move towards developing some form of private sector regulation.

In 1990, the Canadian Standards Association began to organize around the issue, considering the development of a standard for data protection, forming a committee made up of consumer representatives, business representatives, interested organizations such as

---

<sup>33</sup> Bennett, “Regulating Privacy” *supra* note 27 at 10.

<sup>34</sup> For instance, credit reporting legislation enacted in the 1980s, granted consumers the right to access and correct their credit information. In another sector, the Canadian Bankers Association adopted a model Privacy Code for individual customers in 1990 which was built on OECD Guidelines. A number of the chartered banks also developed their own individual codes.

labour unions and professional associations as well as representatives from federal and provincial government.<sup>35</sup> In 1991 they put forward a preliminary proposal to develop a national Model Privacy Code in order to establish common safeguards to protect the privacy of Canadian citizens and the confidentiality of personal information. The intent was to develop a national voluntary code which would become the cornerstone of a national voluntary compliance framework which would in turn guide and influence institutions to establish codes of standards particular to their own environments. The Model Code was successfully completed and released in 1996.

Christopher Berzins has suggested that the movement to develop the CSA Model Code was influenced by:

Two closely related considerations...The first was an attempt to respond to and assuage concerns repeatedly voiced in public opinion surveys about the increasing threats to privacy posed by the private sector's use of personal information. Flowing from this was the second consideration; voluntary privacy codes might pre-empt government regulation by demonstrating to politicians and the public alike that legislation to protect privacy in the private sector was unnecessary.<sup>36</sup>

In January 1998 Industry Canada and the Department of Justice released a consultation paper entitled "The Protection of Personal Information – Building Canada's Information Economy and Society." Berzins argues that this consultation paper was carefully focused in terms "most likely to mute business opposition."<sup>37</sup> Certainly it is true that at the end of the consultation process, Perrin et al claim that 5 requirements for the new private sector

---

<sup>35</sup> Stephanie Perrin *et al.*, *The Personal Information Protection and Electronic Documents Act : An Annotated Guide* (Toronto: Irwin, 2001) at xiii [Perrin].

<sup>36</sup> Christopher Berzins, "Protecting Personal Information in Canada's Private Sector : The Price of Consensus Building" (2002) 27 Queen's L.J. 609 at 619 [Berzins].

<sup>37</sup> *Ibid* at 625.

legislation had become evident: (1) that the law must be based on the CSA standard; (2) that the same rules must hold for the entire country; (3) that the law must not set up barriers to trade nor be so permissive as to allow data havens or offshore rivals; (4) the Privacy Commissioner should be responsible for oversight; and (5) the need for public education and awareness.<sup>38</sup> Note the inclusion of the CSA Code – developed with and by business – as the backbone of the law as well as the light enforcement model of the ombuds-man Privacy Commissioner.

PIPEDA received royal assent on 13 April 2000 and, as of 1 January 2004, is fully in force, applying to all personal information collected, used or disclosed in the course of commercial activities by all private sector organizations.<sup>39</sup> It also applies to the personal information of employees of federal works, undertakings or businesses (FWUBs).<sup>40</sup>

Understanding this history is absolutely integral to understanding PIPEDA. The recognition of the need for the law appears to have come (at least in part) from concern about maintaining and facilitating Canada's international trading relationship. The law was enacted under the federal trade and commerce power, and focuses primarily on commercial activities. Finally, the business involvement in the development of the CSA Code, which forms the backbone of PIPEDA<sup>41</sup> creates a situation with an extremely unusual degree of private sector involvement in the actual drafting of the law.

---

<sup>38</sup> Perrin *supra* note 35 at xiv.

<sup>39</sup> PIPEDA *supra* note 1, s. 4(1)(a). Except in provinces which have legislation in place which has been deemed substantially similar to PIPEDA.

<sup>40</sup> *Ibid*, s. 4(1)(b).

<sup>41</sup> PIPEDA, *supra* note 1, s. 5(1) provides that, subject to sections 6 through 9, every organization shall comply with the principles set out in Schedule 1 of the Act. Schedule 1 is the CSA Model Code for the Protection of Personal Information.

PIPEDA Structure

While on the whole the structure of PIPEDA is unexceptional,<sup>42</sup> there are factors in the structure and application of PIPEDA which seem to position PIPEDA as a data protection instrument.

First, the inclusion of the CSA Model Code as Schedule 1 of PIPEDA. It contains ten (10) Privacy Principles which form the core of PIPEDA, namely: accountability; identifying purposes; consent; limiting collection; limiting use, disclosure and retention; accuracy; safeguards; openness; individual access; and the need to provide recourse.<sup>43</sup>

---

<sup>42</sup> *Ibid.* Section 2 deals with definitions, section 3 with purpose and section 4 with scope and application. Section 11 deals with complaints to the Privacy Commissioner, section 12 with Commissioner investigations into complaints, and section 13 with the report of findings issued by the Commissioner at the conclusion of her investigation. Sections 14-17 address recourse to the Federal Court by complainant after the issuance of the Commissioner's report. Sections 18 and 19 deal with audits of the information management practices of an organization by the Privacy Commissioner, section 20-29 are general provisions and section 30 concerns transitional provisions.

<sup>43</sup> *Ibid.*, Schedule 1. The Principles, in full, are:

1. **Accountability:** an organization should: appoint an individual or individuals to be responsible for the organization's compliance; protect all personal information held by the organization or transferred to third parties for processing; and develop and implement personal information policies and practices.
2. **Identifying purposes:** An organization must identify the reasons for collecting personal information before or at the time of collection. Before or when any personal information is collected, they should inform the individual from whom the information is collected why it is needed, must identify any new purpose for the information and obtain the individual's consent to this new use before using it.
3. **Consent:** Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data; obtain the individual's consent before or at the time of collection, as well as if or when a new use is identified.
4. **Limiting collection:** Do not collect personal information indiscriminately; do not deceive or mislead individuals about the reasons for collecting personal information.
5. **Limiting use, disclosure, and retention:** Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act; keep personal information only as long as necessary to satisfy the purposes; put guidelines and procedures in place for retaining and destroying personal information; keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress; destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.
6. **Accuracy:** Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.

Section 5(1) of PIPEDA states that, subject to sections 6 through 9, every organization shall comply with the principles set out in Schedule 1. Section 7 sets out exceptions to the requirement for consent to the collection, use or disclosure of personal information. Section 8 sets out the process for requesting access, while section 9 sets out the legitimate exceptions to the requirement to provide access. What this means is that, with the limited exceptions set out in the text of the Act, private sector organizations in Canada are governed by the CSA Model Code – a code they themselves had a hand in drafting and which may be presumed, therefore, not to place an undue burden upon them. The approach – that of regulating the collection, use or disclosure of personal information via a set of procedural principles – is clearly grounded in the data protection stream. So too are the principles themselves, which are for the most part clear (re)articulations of fair information principles.

Second, we must consider the purpose of PIPEDA as set out in section 3. It reads:

- 
7. **Safeguards:** Protect personal information against loss or theft; safeguard the information from unauthorized access, disclosure, copying, use or modification; protect personal information regardless of the format in which it is held.
  8. **Openness:** Inform your customers, clients and employees that you have policies and practices for the management of personal information; make these policies and practices understandable and easily available.
  9. **Individual access:** When requested, inform individuals if you have any personal information about them; explain how it is or has been used and provide a list of any organizations to which it has been disclosed; give individuals access to their information; correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient; provide a copy of the information requested, or reasons for not providing access, subject to exception set out in Section 9 of the Act; an organization should note any disagreement on the file and advise third parties where appropriate.
  10. **Provide recourse:** Develop simple and easily accessible complaint procedures; inform complainants of avenues or recourse. These include your organization's own complaint procedures, those of industry associations, regulatory bodies and the Privacy Commissioner of Canada; investigate all complaints received; take appropriate measures to correct information handling practices and policies.

The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.<sup>44</sup>

Just as Raab and Bennett noted with regard to data protection schemes generally, the language of this clause specifically very clearly takes the circulation and exchange of information as a presumptive starting point.<sup>45</sup>

Although this clause speaks of a “right of privacy”, that right is a limited and finite one. It is a right of privacy only with respect to one’s personal information, not a more general right of privacy.<sup>46</sup>

Also, the already-limited “right of privacy of individuals with respect to their personal information” is then further balanced against “the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider

---

<sup>44</sup> PIPEDA, *supra* note 1, s. 3.

<sup>45</sup> Raab and Bennett, *supra* note 29 at 540.

<sup>46</sup> Clarke, *supra* note 23. In contrast, Roger Clarke has divided the right of privacy into:

- **privacy of the person.** This is concerned with the integrity of the individual's body. Issues include compulsory immunization, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilization;
- **privacy of personal behaviour.** This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places;
- **privacy of personal communications.** Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organizations; and
- **privacy of personal data.** Individuals claim that data about themselves should not be automatically available to other individuals and organizations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use.

appropriate in the circumstances.” In combination with the presumption of availability of data already discussed, this is reminiscent of Clarke’s comment that fair information-based regimes effectively legitimize “dataveillance” in return for limited procedural rights.<sup>47</sup>

Finally, even the “light flexible model”<sup>48</sup> of regulation corresponds to the interests of businesses.

On the other hand, there are some features of PIPEDA which seem to extend beyond the traditional data protection model.

Most remarkable of these is section 5(3) of PIPEDA, which provides that “an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.”<sup>49</sup> Perrin et al. wrote:

In the view of many privacy advocates, one of the major flaws of the code is that it does not contain a “justification principle” – that is, it does not oblige an organization to justify why it is collecting, using, or disclosing personal information. In the code, it is simply enough for an organization to state its purposes in collecting, using, and disclosing personal information. Subsection 5(3) attempts to closer that gap with a reasonable person test.<sup>50</sup>

In addition to addressing this concern, this clause may also hearken towards a conception of privacy as a common value beyond data protection. That is, by invoking the objective “reasonable person” standard, there is a suggestion of this corresponding existence of a reasonable, objective understanding of privacy which will inform such a determination.

---

<sup>47</sup> Clarke, *supra* note 23.

<sup>48</sup> Perrin, *supra* note 35 at xv. See also Berzins *supra* note ? at 629.

<sup>49</sup> PIPEDA *supra* note 1, s. 5(3).

<sup>50</sup> Perrin *supra* note 35 at 61.

In addition, the CSA Model Code contained, in addition to the 8 Fair Information Principles set out in the OECD Guidelines, an extra two (2) Principles which are incorporated into PIPEDA – Consent and Recourse.

Principle 4.3, the Consent Principle, has been referred to as the cornerstone of the Act.<sup>51</sup> Although there are problems with consent<sup>52</sup>, as will be discussed later in the paper, this Principle does contain the notion, in Principle 4.3.3 that an organization shall not make consent to the collection, use or disclosure of personal information (beyond that necessary to fulfill the explicitly specified and legitimate purposes) a condition for the supply of a product or service. This suggests an awareness of power dynamics which is out of character for data protection.

In addition, Principle 4.10, Challenging Compliance imbues the individual with agency. While previous Principles are inherently procedural, dictating the personal information management practices of organizations, Principle 4.10 empowers an individual to receive information about the information management practices of an organization and to complain about those policies and practices. Further, by mandating that the organization investigate all complaints and take appropriate measures where a complaint is justified, the Act bolsters the power of the individual to make an organization take notice.

#### D: PIPEDA In Practice

#### Re-Viewing through the Lens of Employment

---

<sup>51</sup> Commissioner speech references.

<sup>52</sup> See Allen, “Wanted Gaze”, *infra* note 59.

Teresa Scassa notes that “The legislation itself is highly ambiguous about the “perspective” it favours. While referencing protection of privacy as an important right in section 3, it does so in a context which immediately balances that right with the need of business to collect, use and disclose such information.”<sup>53</sup> Reading the legislation alone is not sufficient to provide an understanding of PIPEDA – we must place the analysis in context by looking at PIPEDA in action.

I choose the situation of employment information under PIPEDA as the lens through which I will explore the operation of PIPEDA and the effectiveness of its provisions in recognizing or protecting a right of privacy.<sup>54</sup> A recent Federal Court of Canada decision – *Turner et al v. Telus Communications Inc.*<sup>55</sup>—is of particular interest in exposing the tensions evident in PIPEDA and as such it and the Privacy Commissioner’s finding in the original complaint on which it is based<sup>56</sup> will provide a constant thread in the analysis.

The purpose clause of PIPEDA makes it clear that privacy does not stand alone. Balancing the right of individuals with respect to their personal information against the needs of businesses is built into the purpose of PIPEDA and the very articulation of the PIPEDA privacy right. Employment has long been an area where society recognizes some need to

---

<sup>53</sup> Teresa Scassa, “Text and Context: Making Sense of Canada’s New Personal Information Protection Legislation” (2001) 32 Ottawa L. Rev. 1 at 11.

<sup>54</sup> Of course, PIPEDA’s main coverage is commercial relationships, not employment relationships and it is positioned as a federal trade and commerce power rather than a provincial property and civil rights issue.

<sup>55</sup> *Turner et al. v. Telus Communications Inc.*, 2005 FC 1601 at para 51 [e.speak] online: Federal Court of Canada <http://decisions.fct-cf.gc.ca/fct/2005/2005fc1601.shtml>.

<sup>56</sup> See Summary #281 [OPC e.speak] online: Office of the Privacy Commissioner [http://www.privcom.gc.ca/cf-dc/2004/cf-dc\\_040903\\_e.asp](http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp). The case summary details a complaint by a group of employees who felt that their employer was forcing them to consent against their will to the collection of biometric information, namely a voice print.

limit or restrict rights in the interest of the larger social good, and as such it is perfectly placed for a PIPEDA assessment.

In addition, the Privacy Commissioner's findings under PIPEDA<sup>57</sup> reveal an astounding breadth of issues raised within the employment context, including health information and disability claims; surveillance inside and outside the workplace; consent to the collection of information; concerns about the appropriateness of use and disclosure of personal information of employees, analysis of the duty to inform and explain the collection, use or disclosure of personal information and more.

PIPEDA contains within it the requirement for a 5-year review of the Act. This review is due in 2006 and it is clear that the Privacy Commissioner is already beginning to muse over what areas of PIPEDA should be re-viewed. Indeed, in her 2004 *Annual Report to Parliament on the Personal Information Protection and Electronic Documents Act*, current Privacy Commissioner Jennifer Stoddart sets out some thoughts on the upcoming 2006 5-Year Review of PIPEDA. Interestingly, the very first issue she identifies is that of employment, asking “[d]oes PIPEDA deal effectively with employee information? Many of our complaints arise in the context of the employer/employee relationship. The current PIPEDA doesn't always fit that relationship. Both the B.C. and Alberta private sector legislation deal with employee information under a separate set of rules.”

Implicitly, it seems to me, the Privacy Commissioner is suggesting that when PIPEDA has trouble dealing effectively with the issue of employee information, the problem is with the

---

<sup>57</sup> Online: [http://www.privcom.gc.ca/cf-dc/index\\_e.asp](http://www.privcom.gc.ca/cf-dc/index_e.asp).

inclusion of the employment context, not with the general PIPEDA rules and principles. I include an analysis of this point in order to argue that the explicit removal of consent so proposed is analogous to the failure of consent to appropriately protect personal information.

Building on the review of PIPEDA's structure, I will analyze PIPEDA's treatment of employment information at three different stages: the requirement for consent; efficiency (the needs of organizations) and the reasonable purposes assessment. Rather than be complicit in the presumption that personal information will be available, my analysis will focus on the initial point of collection.

### Consent

PIPEDA Principle 4.3 requires the knowledge and consent of the individual for the collection, use or disclosure of her personal information except where inappropriate.

Section 7(1) sets out the only exceptions to this requirement of consent:

7. (1) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if

(a) the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(b) 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 province;

- (c) the collection is solely for journalistic, artistic or literary purposes;
- (d) the information is publicly available and is specified by the regulations; or
- (e) the collection is made for the purpose of making a disclosure
- (i) under subparagraph (3)(c.1)(i) or (d)(ii), or
- (ii) that is required by law.

These provisions, in combination with PIPEDA's language of "right of privacy with regard to their personal information" effectively suggest a reading of privacy as control.

Paul Schwartz identifies three aspects of "privacy as control":

...first, the notion that the term "privacy" means control (or rights of control) over the use of personal data or information, second the notion that the expression "right to privacy" means the right or claim to control the use of personal data or information; and third, the notion that the central aim of privacy regulation should be promoting individual's control (or rights of control) over personal data or information.<sup>58</sup>

This focus on control, as Anita Allen points out, leads to a conflation of consent and actual privacy, where we believe that privacy is appropriately protected "even if individuals choose to waive and alienate most of their privacy, so long as their acts of waiver or alienation are fully consensual and informed."<sup>59</sup> There is no indication, however, of why or how individual choice is automatically privacy-protective. Where an individual is making a decision, on what basis do we presume that protection of privacy (her own or a larger social value of privacy) will be the (or even a) consideration in decision making? In part, a conceptualization of privacy as a collective social value may help to redress this since it

---

<sup>58</sup> As summarized in Anita Allen, "Privacy as Data Control: Conceptual, Practical, and Moral Limits of the Paradigm" (2000) 32 Conn. L. Rev. 861 at 863 [Allen, "Privacy as Data Control"].

<sup>59</sup> Anita L. Allen, "The Wanted Gaze: Accountability for Interpersonal Conduct at Work" (2001) 89 Geo. L.J. 2013 at 2014 [Allen, "Wanted Gaze"].

recognizes the necessity of all persons having some minimal level of privacy rather than predicating its analysis on individual abilities to negotiate privacy.

Reviewing the series of findings where an employer has requested that existing employees provide consent for additional collection of personal information<sup>60</sup> it becomes evident that little or no substantive assessment of consent is being performed by the Privacy Commissioner. Although the PIPEDA requirement that consent be informed is respected, there is little or no inquiry into the meaningfulness of consent. In fact, with the exception of Finding #10, one of the earliest PIPEDA findings, Privacy Commissioners under PIPEDA have consistently indicated that the potential duress of a situation where negative consequences attach to a refusal of consent does not affect the voluntariness of the consent. Thus, any indication of consent is presumed to be sufficient, and the issue of whether a choice is truly consensual is not inquired into.

In some cases, neither the consent analysis nor the consent is evident. In OPC e.speak, for instance, the Assistant Privacy Commissioner suggests that the organization has met the consent requirements of PIPEDA in the face of complaints from individuals who are explicitly refusing consent.

PIPEDA recognizes a variety of potential forms of consent. Principle 4.3.6 of Schedule 1 reads:

---

<sup>60</sup> See Case Summary #10 [http://www.privcom.gc.ca/cf-dc/2001/cf-dc\\_010817\\_e.asp](http://www.privcom.gc.ca/cf-dc/2001/cf-dc_010817_e.asp), Case Summary #65 [http://www.privcom.gc.ca/cf-dc/2002/cf-dc\\_020814\\_e.asp](http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020814_e.asp), Case Summary #127 [http://www.privcom.gc.ca/cf-dc/2003/cf-dc\\_030304\\_3\\_e.asp](http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030304_3_e.asp), Case Summary # 232 [http://www.privcom.gc.ca/cf-dc/2003/cf-dc\\_031001\\_03\\_e.asp](http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031001_03_e.asp), and Case Summary #281 [http://www.privcom.gc.ca/cf-dc/2004/cf-dc\\_040903\\_e.asp](http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp).

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative.<sup>61</sup>

The Privacy Commissioner's Fact Sheet "Determining The Appropriate Form of Consent Under the Personal Information Protection and Electronic Documents Act"<sup>62</sup> discusses express consent, negative (opt-out) consent and implied consent as well as situations where no consent is required.

As Paul Schwartz notes, the conflation of privacy and consent becomes even more problematic when notions such as implied consent are factored in. As he writes, privacy as consent:

...neglects the actual conditions of choice regarding the processing of personal information and permits notice to become an alibi for take-it-or-leave-it data processing. Notice is emerging as the cornerstone for a legal fiction of implied consent on the Internet. A given course of conduct is said to signal acquiescence, and therefore, implied consent.<sup>63</sup>

Perrin et al make the point that the CSA Code consent requirement is significantly stronger than traditional data protection statutes, which require only knowledge or consent "where appropriate."<sup>64</sup> While this may be true, a stronger consent requirement (without more) is not sufficient to lift PIPEDA from the status of data protection towards recognition of the value of privacy rights.

---

<sup>61</sup> PIPEDA *supra* note 1, Principle 4.3.6.

<sup>62</sup> Online : [http://www.privcom.gc.ca/fs-fi/02\\_05\\_d\\_24\\_e.asp](http://www.privcom.gc.ca/fs-fi/02_05_d_24_e.asp).

<sup>63</sup> Paul M. Schwartz, "Internet Privacy and the State" (2000) Conn. L.Rev. 815 at 825 [Schwartz].

<sup>64</sup> Perrin *supra* note 35 at 22.

In fact, making consent the focus effectively hijacks scrutiny from the personal information management processes of an organization and places it instead on the individual decision.

As Regan notes:

A definition of privacy as the right of the individual to control access to himself or herself, in effect, rests upon an exaltation of the powers of the individual. It also explains the failure to examine the interests of the organizations collecting and using personal information; instead, the individual is given the means to mediate his or her relationship with the organization. By placing the burden on the individual, there is less need to evaluate whether organizational interests are indeed social interests or whether individual privacy interests could be conceived as social interests.<sup>65</sup>

Is it possible to separate this privacy as consent conflation by invoking the notion of privacy as social value? Not entirely. Earlier I discussed Anita Allen's criticism of data protection – that it constructs privacy as somehow optional in that it may be waived or alienated. Allen argues that this results in a presumption that, as long as decisions are being made, privacy is being protected.<sup>66</sup> This notion, troubling enough at a theoretical level, becomes especially problematic when applied in an employment situation.

Findings to date from the Privacy Commissioner espouse a formal equality model which presumes that an individual has a freely exercised right to refuse consent to the collection of personal information. In fact, as Jeremy de Beers notes:

...employees are rarely in a position of equal bargaining power, and are therefore unable to protect themselves. Employers are more likely to have additional job applicants than prospective employees are likely to have additional job opportunities. Often employees have little power to negotiate the terms of the employment relationship. Thus, employers have virtually unfettered access to private information regarding their employees.

---

<sup>65</sup> Regan "Legislating Privacy", *supra* note 15 at 219.

<sup>66</sup> Allen, "Wanted Gaze", *supra* note 59 at 2014.

Furthermore, employees often lack the resources to commence and pursue claims against employers if and when violations do occur.<sup>67</sup>

A substantive understanding of equality would seem necessary here in order to take account of the obvious power differential in the situation as well as the implicit economic advantage being offered/provided in exchange for consent. Such a notion of consent would be effectively grounded in the recognition of privacy as a social value.

As discussed, the Privacy Commissioner has referred to the British Columbia and Alberta private sector privacy approach to employment information with some approval. The B.C. and Alberta laws that the Commissioner takes note of effectively remove the question of consent from the data management of personal employee information.

British Columbia's *Personal Information Protection Act*<sup>68</sup> s. 13, for instance, states that:

*13(1) Subject to subsection (2), an organization may collect employee personal information without the consent of the individual.*

*(2) An organization may not collect employee personal information without the consent of the individual unless:*

*(a) section 12 allows the collection of the employee personal information without consent, or*

*(b) the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual.*

*(3) An organization must notify an individual that it will be collecting employee personal information about the individual and the purposes for the collection before the organization collects the employee personal information without the consent of the individual.*

---

<sup>67</sup> Jeremy de Beers, "Employee Privacy: The Need for Comprehensive Protection" (2003) 66 Sask. L. Rev. 390 at 391 [de Beers].

<sup>68</sup> S.B.C. 2003, c. 63 [BC PIPA].

Similar provisions appear in s. 16 with regard to the use without consent of employee personal information and in s. 19 regarding the disclosure without consent of employee personal information.

Similarly, s. 15 of the Alberta *Personal Information Protection Act*<sup>69</sup> reads:

*15(1) Notwithstanding anything in this Act other than subsection (2), an organization may collect personal employee information about an individual without the consent of the individual if*

- (a) the individual is an employee of the organization, or*
- (b) the collection of the information is for the purpose of recruiting a potential employee.*

*(2) An organization shall not collect personal information about an individual under subsection (1) without the consent of the individual unless*

- (a) the collection is reasonable<sup>70</sup> for the purposes for which the information is being collected,*
- (b) the information consists only of information that is related to the employment of volunteer work relationship of the individual, and*
- (c) in the case of an individual who is an employee of the organization, the organization has, before collecting the information, provided the individual with reasonable notification that the information is going to be collected and of the purposes for which the information is going to be collected.*

Similar provisions appear in s. 18 with regard to the use without consent of employee personal information and in s. 21 regarding the disclosure without consent of employee personal information.

It would seem, then, that under these models employee personal information<sup>71</sup> could be collected without consent where (a) the purposes are reasonable; (b) the information

<sup>69</sup> S.A. 2003, c. P-6.5 [Alberta PIPA].

<sup>70</sup> Section 2 of Alberta PIPA, *supra* note ? states in part that “the standard to be applied under this Act is determining whether the thing or matter is reasonable or unreasonable, or has been carried out or otherwise dealt with reasonably or in a reasonable manner is what a reasonable persona would consider appropriate in the circumstances.” This language ultimately mirrors that of s. 5(3) of PIPEDA.

collected is limited to that necessary to accomplish the purposes; and (c) the employee receives notification that her information is to be collected and the purposes to which the information will be put.

Certainly such a solution eases concerns about the decontextualization of consent which seems a result of the data protection focus, however it does so by removing individual agency from the equation altogether! While it is evident why such a solution would meet with approval from organizations – economic and administrative efficiency is enhanced by the removal of the requirement to obtain consent – this is far, far removed from substantive privacy protection.

Re-viewing the Privacy Commissioner's findings, it is interesting to note that although on the surface PIPEDA treats employee information differently than do Alberta and British Columbia, this is more a formality than an actuality. Where systemic collections of personal information about employees were instituted, the Privacy Commissioner either deemed consent to have been given or simply failed to address the issue entirely in her finding. In situations where individual employees were asked to consent or to somehow voluntarily provide the required information, the Privacy Commissioner's treatment of consent is negligible. Rather than explore what consent means and whether it can be meaningfully given or received in situations of duress, pressure, coercion or consequences, the Privacy

---

<sup>71</sup> Neither BC PIPA nor Alberta PIPA purports to exempt all information about an employee from the requirement of consent. Rather, each speaks of "personal employee information". This would set up a double threshold, where employers must first demonstrate that the information reasonably falls under the rubric of personal employee information and then demonstrate that the purposes for which the information is collected, used or disclosed are reasonable.

Commissioner presumes its legitimacy and in so doing, renders the requirement for consent effectively moot.

Alberta and British Columbia eradicate consent from the employment relationship, focusing instead on reasonableness. Although PIPEDA formally requires that consent be given except in limited exceptions, in practice it too seems to eradicate the question of (meaningful) consent from the employment relationship. Schwartz observes that notice and consent alone were insufficient to protect privacy<sup>72</sup> -- here we see a situation so degraded that notice alone is expected to be sufficient!

Should the Commissioner's suggestion be followed, then, PIPEDA would seek to recognize the right of privacy of individuals with regard to their personal information and balance that right against the need of the particular organization to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. While technically this would constitute a "separate scheme" for employment information, ultimately it would result in a situation where "reasonableness" is the final arbiter of PIPEDA privacy. That is, just as employee information would be able to be collected, used or disclosed without consent if the reasonableness standard is met, to too does PIPEDA s. 5(3) impose an overall appropriate purposes test.

#### The Needs of Organizations: Privileging Efficiency

---

<sup>72</sup> Schwartz, *supra* note 63 at 827.

PIPEDA's purpose clause requires that privacy be balanced against "the needs of organizations to collect, use and disclose personal information."

Obviously, the question of a system-wide initiative is a difficult one for legislation which centres around notions of choice and consent. This is particularly evident with the growing trend of employers turning towards video surveillance in the workplace.

A review of Privacy Commissioner findings reveals tension when a systemic employer initiative conflicts with the individual focus of PIPEDA. It is interesting to note that notwithstanding PIPEDA's requirement for consent prior to the collection of personal information, not only is there no consent requested by the employers prior to instituting system-wide surveillance measures, but the Privacy Commissioner does not comment on this absence or make any statements about the importance of consent.<sup>73</sup> In OPC e.speak, the Assistant Privacy Commissioner found that the company had met the consent requirement despite the fact that 3 complainants had explicitly refused to consent to collection of the information.<sup>74</sup> While the company had not (and could not) collect the information without consent, the question of how employees who refused to consent could function coexistent with the systemic initiative which required the information is left unaddressed.

In fact, in e.speak, Justice Gibson expressed concern about PIPEDA's intersection with systemic effectiveness, writing:

---

<sup>73</sup> See case summary # 114 online: Office of the Privacy Commissioner [http://www.privcom.gc.ca/cf\\_dc/2003/cf\\_dc\\_030123\\_e.asp](http://www.privcom.gc.ca/cf_dc/2003/cf_dc_030123_e.asp) and case summary # 264 at [http://www.privcom.gc.ca/cd-dc\\_040219-01-e.asp](http://www.privcom.gc.ca/cd-dc_040219-01-e.asp).

<sup>74</sup> OPC e.speak, *supra* note 56.

I am loathe to conclude that, on facts such as those before the Court where consent is sought from a large number of individuals by the employer of those individuals and the vast majority provide consent, while a very small minority, as here, refuse consent, Parliament intended that that small minority should be able to paralyze action by the employer that it considers to be in its business interests and that view is not opposed by the vast majority of affected employees.<sup>75</sup>

I would suggest that the problem with implementation of systemic initiatives is one that is endemic to a data protection scheme. The benefits to the employer of the system implementation are so economically desirable that recognition of individual right(s) over personal information is difficult to conceive of meaningfully. Certainly the individual value of privacy appears diminished next to the economic and administrative efficiency promised by such systems.

It is interesting to note, in this regard, that a key recognition of the Standing Committee was that “privacy interests are at worst ignored and at best not given sufficient weight in determining the balance between privacy and security or privacy and economic interests.”<sup>76</sup> Again, this is a situation where recourse to a conceptualization of privacy as social value is necessary in order to constitute PIPEDA’s conceptualization of privacy as a substantive right.

#### Balancing: Appropriate Purposes

---

<sup>75</sup> E.speak, *supra* note 55 at para 51.

<sup>76</sup> Canada, *Privacy: Where Do We Draw the Line? Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities*, (Ottawa: PWGSC Publishing, 1997) at 13 [Standing Committee].

As demonstrated in the above sections, it seems that PIPEDA's treatment of the personal information of employees either completely ignores the issue of consent or alternatively renders consent nugatory by a failure to insist that it be meaningful. Both in situations where consent was required and where it wasn't, the Privacy Commissioner's analysis has focused on the s. 5(3) reasonable purposes analysis.

Section 5(3) is an overarching requirement, providing that all collections, uses or disclosures must be for purposes that a reasonable person would consider appropriate in the circumstances. This is the case notwithstanding the provision of consent. That is, even where an organization receives consent from an individual, it is still open to the individual to challenge the appropriateness of the purposes for which the information was collected. Should the purposes fail to meet the s. 5(3) threshold, the organization would have contravened PIPEDA regardless of the fact that the information was collected with consent.<sup>77</sup>

The Privacy Commissioner has suggested a possible amendment to PIPEDA which would treat employee information in a way commensurate with the approaches taken by the provinces of British Columbia and Alberta in their private sector legislation. Ultimately, this too will result in a s. 5(3) analysis.

Alternatively, it might be decided to remove employment information from the ambit of PIPEDA and create a separate scheme. I would suggest that this would still be subject to

---

<sup>77</sup> It is interesting to note that the reverse is not true. PIPEDA requires consent for the collection of personal information, unless one of the exemptions set out in s. 7(1) applies. Even where the purposes are reasonable, this should not result in override of the consent requirements of PIPEDA.

the same critiques. While PIPEDA itself would no longer struggle to arrive at a reasonable result in cases regarding employee personal information, the larger difficulty would be extant in both the new employment code and in PIPEDA as it remained – assessing the reasonableness of purposes will still be required under each legislative scheme.

A review of OPC e.speak and the e.speak decision itself provide interesting insight into how this analysis has developed.

Section 3 speaks of the “need of organizations” and in many of the OPC case summaries there is evidence of a legitimate need as information is required by new regulatory requirements or policies. However, in this situation there is no such need to ground demand, , nor does the Privacy Commissioner engage in any analysis attempting to distinguish the organizations need from its want. Instead, the case summary reflects arguments about enhanced security of information, lowered security costs, and the efficiency and cost-effectiveness of streamlining work processes.

In her analysis, the Privacy Commissioner concludes that the biometric voice print does not reveal much information about the individual, that the uses to which the voice print could be put by the company were limited and thus that the biometric voice print used solely for one-to-one authentication purposes was fairly benign as far as privacy invasions go. In contrast she awarded strong recognition to the purported risk to the company should it fail to secure the privacy of customer information.<sup>78</sup> Accordingly, the Assistant Privacy Commissioner

---

<sup>78</sup> Interestingly, although this might have been positioned as a conflict between consumer privacy and employee privacy, instead it is the economic impact of failing to provide consumer privacy that is keyed on.

concluded that since the voice print was not unduly privacy invasive, an appropriate balance between the employees' right to privacy and the employer's "needs" had been struck.

Justice Gibson engaged in similar analysis at the Federal Court, writing:

Taking into account the foregoing, and against the above brief analysis of: the degree of sensitivity associated with voice prints as personal information; the security measures implemented by Telus; the bona fide business interests of Telus as established on the evidence before the Court and to which the collection of voice prints is directed; the effectiveness of the use of voice prints to meet those objectives; the reasonableness of the collection of voice prints against alternative methods of achieving the same levels of security at comparable costs and with comparable operational benefits; and the proportionality of the loss of privacy as against the costs and operational benefits in the light of the security that Telus provides; I conclude that the collection of the voice print information here at issue would be seen by a reasonable person to be appropriate in the circumstances, as they existed at all times relevant to this matter, and against the security measures adopted by Telus.<sup>79</sup>

Although PIPEDA speaks of a privacy right, privacy itself seems absent from these analyses.

There is no discussion of the importance of privacy or of the right to privacy of the individuals involved with regard to their personal information – it is presumed and thus any real recognition of privacy is thereby omitted from the analysis. Thus, the strong benefits to the organization are weighed against a recognized "low-level" invasion voice print and outweigh it handily.

Such shifts may be the rule rather than the exception. Priscilla Regan has identified a shifting analytic focus whereby:

...the debate moved from the idea of privacy to an examination of the ideas that were supported by other interests and focused on how other ideas and

---

<sup>79</sup> E.speak, *supra* note 55 at para 48.

interests would be compromised by privacy protection. In effect, this changed the policy debate from one of ideas to one of interests. In each case, opponents did not challenge privacy as a value, but instead focused on the importance of the competing interest, and the value associated with that interest, and on the need to balance privacy against that interest.<sup>80</sup>

This analysis is a fascinating one. Because of the seemingly universal applicability of the balancing analysis, the process of assessing appropriateness and the factors by which it is arrived at are a valid and important area of inquiry for any who wish to understand PIPEDA. Simultaneously, the factors by which such balance is achieved are becoming more settled within the Office of the Privacy Commissioner and yet we continue not to see any concrete articulation of privacy or privacy rights.

The process by which an administrative decision maker (or ombuds-person, in the case of the Privacy Commissioner) determines a rights claim is not accident, but rather is linked to the conceptual underpinnings of the right itself. Thus, when the s. 5(3) analysis is done without reference to privacy, this isn't a simple failure to articulate but rather indicates a PIPEDA framework which has strayed almost inconceivably far from the notion of privacy as a social value.

We must begin to reinsert privacy into the balancing process. "The language we use to frame a question determines the types of solutions we devise. The language of data protection revolves around commercial rather than social considerations."<sup>81</sup> The test as it is currently applied appears to prioritize efficiency and business success rather than the privacy interests and concerns of individuals and society. An explicit articulation of privacy as a

---

<sup>80</sup> Priscilla M. Regan, "Privacy Legislation in the United States: a debate about ideas and interests" (1996) 62 Int'l. Rev. Admin. Sci 465 at 470 [Regan, "Privacy in the US"].

<sup>81</sup> Steeves, "Response to Walter's", *supra* note 19 at 448.

social interest must take place within the balancing process in order to correct for this kind of shift in analysis. Only then will PIPEDA's privacy right be substantive and meaningful.

### E: Conclusion

Charles Raab has argued that:

Privacy protection may be in danger of becoming absorbed into the conceptual framework of consumerism, where it is just one among other criteria such as value for money, wholesomeness, convenience and the like. In this light, the practical necessity of transmuted privacy rights into the operational inventory of fair information principles can be seen as assisting the absorption unless participants bear in mind what the principles represent.<sup>82</sup>

I have shown how, notwithstanding its purpose to recognize a right of privacy, The data protection conceptualization of privacy as control as implemented in PIPEDA has not served to protect privacy well. It has led to a focus on individual choice which conflates choice with privacy. It has stacked seemingly individual benefit against systemic rewards and found the individual claim wanting. Finally, it has erased privacy from the balancing process.

When the Standing Committee considered privacy regulation in Canada, they concluded that:

...if we approach privacy issues from a human rights perspective, the principles and solutions we arrive at will be rights-affirming, people-based, humanitarian ones. On the other hand, if we adopt a market-based or economic approach, the solutions will reflect a different philosophy, one that

---

<sup>82</sup> Charles D. Raab, "From Balancing to Steering: New Directions for Data Protection" in Colin J. Bennett and Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999) at 76.

puts profit margins and efficiency before people, and may not first and foremost serve the common good.<sup>83</sup>

PIPEDA's purpose clause speaks of privacy "of the individual", and the Privacy Commissioners interpretations thus far have remained focused on privacy as an individual right. Regan argues that when privacy is identified solely with boundaries used to protect or segregate an individual from society as a whole, privacy comes to be viewed as "an impediment to the functioning of society."<sup>84</sup> In a similar vein, Gregory Walters claims that:

Rights presuppose competition and conflict as guarantees that self-seeking individuals will not be trampled in their conflictual relations with others. As such, rights submerge the values of community, obscure moral responsibility, and alienate persons. Community, on the other hand, connotes common interest and cooperation, mutual sympathy, and fellow feeling that ranges from one's family through one's ethnic and other groups to the nation state.<sup>85</sup>

Regan notes that the insistence on privacy as an individual right leads inevitably to an individual/society dichotomy, and that focus on that dichotomy obscures the question of what a society is actually made up of.<sup>86</sup>

There need be no dichotomy between an individual right of privacy and a recognition of the social value of privacy. As Walters suggests:

[t]he community of rights involves not only duties of non-interference with respect to privacy as entailed by negative rights, but also positive duties and rights to productive agency, employment, economic and political democracy. The community of rights is a society whose government actively seeks to help fulfill the needs of its members, especially those who are most

---

<sup>83</sup> Standing Committee, *supra* note 76 at 33.

<sup>84</sup> Regan, "Privacy in the US" *supra* note 80 at 472.

<sup>85</sup> Gregory J. Walters, "Digitizing Technology, Transforming Ourselves: Can We Ethically Balance Human Rights and Security?" (1999) 10 N.J.C.L. 373 at 397[Walters].

<sup>86</sup> Regan, "Legislating Privacy", *supra* note 15 at 218.

vulnerable, for the freedom and well-being that are the necessary goods of human agency, when persons cannot attain this fulfillment by their own efforts.<sup>87</sup>

Val Steeves suggests that “[i]f we are going to be able to address the real issues of privacy protection in a networked world, we need to expand our enquiry beyond the technicalities of data protection and begin to explore the bigger picture, the social value of privacy.”<sup>88</sup> I have attempted to do that just, showing how reference to a conceptualization of privacy as a social value can reinvigorate existing provisions of PIPEDA, making the Act meaningful. It is clear that the language of PIPEDA may be read either way – we do ourselves a disservice if we accept a compromised data protection reading of PIPEDA when this more robust privacy-valuing approach is equally possible.

---

<sup>87</sup> Walters, *supra* note 85 at 397.

<sup>88</sup> Steeves, “Road Map”, *supra* note 5 at 2.

BIBLIOGRAPHYLegislation

*Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982.c. 11.

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

*Personal Information Protection Act*, S.A. 2003, c. P-6.5

*Personal Information Protection Act*, S.B.C. 2003, c. 63

Part IV of the *Canadian Human Rights Act*, S.C. 1976-77, c. 33.

Jurisprudence

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

*Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773.

*R v. Dymment*, [1988] 2 S.C.R. 417.

*Turner et al. v. Telus Communications Inc.* 2005 FC 1601.

Government Documents

Canada, *Privacy: Where Do We Draw the Line? Report of the House of Commons Standing Committee on Human Rights and the Status of Persons with Disabilities*, (Ottawa: PWGSC Publishing, 1997)

*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Council of Europe Convention 108)* online: <http://www.coe.int/treaty/EN/cadreprincipal.htm>.

*Directive on the Protection of Personal Data With Regard to the Processing of Personal Data and the Free Movement of Such Data (EU 95/46)*. Online: European Union  
[http://europa.eu.int/comm/internal\\_market/privacy/law\\_en.htm](http://europa.eu.int/comm/internal_market/privacy/law_en.htm).

*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* released 23 September 1980. online: OECD  
[http://www.oecd.org/document/18/0,2340,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html).

*International Covenant on Civil and Political Rights*. 19 December 1966, 999 U.N.T.S. 171, Can. T.S. 1976 No. 47, 6 I.L.M. 368 (entered into force 23 March 1976). Online:  
[http://www.unhchr.ch/html/menu3/b/a\\_ccpr.htm](http://www.unhchr.ch/html/menu3/b/a_ccpr.htm).

*Universal Declaration of Human Rights*, GA Res. 217 (III), UN GAOR, 3d Sess., Supp. No. 13, UN Doc. A/810 (1948). Online: <http://www.un.org/Overview/rights.html>.

Privacy Commissioner Findings

Case Summary #281. online: Office of the Privacy Commissioner  
[http://www.privcom.gc.ca/cf-dc/2004/cf-dc\\_040903\\_e.asp](http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp)

Case Summary #10. online: Office of the Privacy Commissioner  
[http://www.privcom.gc.ca/cf-dc/2001/cf-dc\\_010817\\_e.asp](http://www.privcom.gc.ca/cf-dc/2001/cf-dc_010817_e.asp).

Case Summary #65. online: Office of the Privacy Commissioner  
[http://www.privcom.gc.ca/cf-dc/2002/cf-dc\\_020814\\_e.asp](http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020814_e.asp).

Case summary # 114. online: Office of the Privacy Commissioner  
[http://www.privcom.gc.ca/cf\\_dc/2003/cf\\_dc\\_030123\\_e.asp](http://www.privcom.gc.ca/cf_dc/2003/cf_dc_030123_e.asp).

Case Summary #127. online: Office of the Privacy Commissioner  
[http://www.privcom.gc.ca/cf-dc/2003/cf-dc\\_030304\\_3\\_e.asp](http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030304_3_e.asp).

Case Summary # 232. online: Office of the Privacy Commissioner  
[http://www.privcom.gc.ca/cf-dc/2003/cf-dc\\_031001\\_03\\_e.asp](http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031001_03_e.asp).

Case Summary # 264. online: Office of the Privacy Commissioner  
[http://www.privcom.gc.ca/cd-dc\\_040219-01-e.asp](http://www.privcom.gc.ca/cd-dc_040219-01-e.asp).

Case Summary #281. online: Office of the Privacy Commissioner  
[http://www.privcom.gc.ca/cf-dc/2004/cf-dc\\_040903\\_e.asp](http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040903_e.asp).

#### Secondary Material: Books

Bennett, Colin J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992).

Perrin, Stephanie et al., *The Personal Information Protection and Electronic Documents Act: An Annotated Guide* (Toronto: Irwin, 2001).

Regan, Priscilla M., *Legislating Privacy: Technology, Social Value, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995).

#### Secondary Materials: Articles

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

Allen, Anita L., "The Wanted Gaze: Accountability for Interpersonal Conduct at Work" (2001) 89 Geo. L.J. 2013.

Berzins, Christopher, "Protecting Personal Information in Canada's Private Sector : The Price of Consensus Building" (2002) 27 Queen's L.J. 609.

de Beers, Jeremy, "Employee Privacy: The Need for Comprehensive Protection" (2003) 66 Sask. L. Rev. 390.

Flaherty, David H., "Visions of Privacy: Past, Present, and Future" in Colin J. Bennett and Rebecca Grant, eds. *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999) 19.

MacKay, A. W., "The Waves of Information Technology, the Ebbing of Privacy, and the Threat to Human Rights" (1999) 10:3 N.J.C.L. 411.

Raab, Charles D. and Colin J. Bennett, "Taking the Measure of Privacy: Can Data Protection Be Evaluated?" (1996) 62 Int'l. Rev. Admin. Sci.535.

Raab, Charles D., "From Balancing to Steering: New Directions for Data Protection" in Colin J. Bennett and Rebecca Grant, eds., *Visions of Privacy: Policy Choices for the Digital Age* (Toronto: University of Toronto Press, 1999) 68.

Regan, Priscilla M., "Privacy Legislation in the United States: a debate about ideas and interests" (1996) 62 Int'l. Rev. Admin. Sci. 465.

Scassa, Teresa, "Text and Context: Making Sense of Canada's New Personal Information Protection Legislation" (2001) 32 Ottawa L. Rev. 1.

Schwartz, Paul M., "Internet Privacy and the State" (2000) Conn. L.Rev. 815.

Shestack, Jerome J., "The Jurisprudence of Human Rights" in Theodor Meron, ed., *International Law of Human Rights*, vol. 1(Oxford: Clarendon Press, 1984) at 74.

Steeves, Val, "A Better Road Map for the Information Highway: Critical Human Rights Issues in the Access and Privacy Field" (Paper presented at the Access & Privacy: the New Way of Doing Business conference held by Management Secretariat of the Government of Ontario, 12 September 1997 at 3. online: University of Ottawa Human Rights Research and Education Centre <<http://www.uottawa.ca/hrrec/publicat/mbs.html>>

Steeves, Val, "A Response to Professor Walter's Article "Digitizing Technology, Transforming Ourselves"" (1999) 10 N.J.C.L. 445

Walters, Gregory J., "Digitizing Technology, Transforming Ourselves: Can We Ethically Balance Human Rights and Security?" (1999) 10 N.J.C.L. 373.

#### Secondary Materials: Online

Clarke, Roger, "Beyond the OECD Guidelines: Privacy Protection for the 21<sup>st</sup> Century" online: <http://www.anu.edu.au/people/Roger.Clarke/DV/PP21C.html#ScopeDP>