2. APPROACHES TO CONSENT IN CANADIAN DATA PROTECTION LAW

PHILIPPA LAWSON AND MARY O'DONOGHUE*

I. INTRODUCTION

Recognizing the dangers to privacy posed by new technologies, Canada has enacted legislation designed to protect individuals from inappropriate and unwanted uses of their personal information. Public sector privacy laws were enacted in the 1980s, followed by private sector laws in the 1990s. Since 2004, all government and commercial activity in Canada is subject to data protection legislation.

Although all the statutes rely to some degree on consent for valid collection, use, and sharing of personal information, the role of consent varies significantly by sector: public sector laws rely on consent as a *justification* for data collection,

* We would like to thank Louisa Garib, James Wishart, Janet Lo, Tara Berish, Catherine Thompson, and Martin Saidla for their excellent research support, without which this paper could not have been written. Thanks also to David Matheson, Charles Raab, Marsha Hanen, George Tomlinson, Jena McGill, Jocelyn Cleary, Michael Froomkin, and Teresa Scassa for their helpful comments on a draft version of this paper.

use, or disclosure, while private sector laws treat consent as a *requirement* for valid collection, use, or disclosure. Private sector statutes provide more scope for individuals to negotiate privacy protection, although the effectiveness of this control is questionable. The role of consent is further differentiated in the employment and health contexts, neither of which is examined here.

In this chapter, we describe approaches to consent in public and private sector Canadian data protection law. We note the markedly different role played by consent in each sector's laws, and the rationale for that difference. Although we accept that context (citizens vs. consumers) is a consideration in developing data protection rules, we suggest that a more nuanced understanding of government-citizen relationships might result in a greater role for consent in that context. Nevertheless, we caution against too much reliance on consent, given that its exercise is often more notional than real.

II. TWO COMPETING APPROACHES: HUMAN RIGHTS VS. FAIR INFORMATION PRACTICES

Privacy is treated as a human right in many international covenants, including the Universal Declaration of Human Rights (1948), the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950), and the International Covenant on Civil and Political Rights (1966).[1] Under the human rights approach, privacy is a moral imperative and covers more than data protection.

Canada signed the UN Declaration, but like other common-law jurisdictions, it neither provided strong constitutional privacy protections, nor sited privacy protection statutes in the human rights arena. In contrast, the Quebec Charter of Human Rights and Freedoms (1975) enshrines a right to privacy for residents of Quebec, and amendments to the Civil Code (1991) provide extensive privacy rights.

An alternative and pragmatic approach to privacy focuses on data protection. Privacy law in Canada tends toward this approach, reflecting "Fair Information Practices" promulgated by Alan Westin and adopted by the Organisation for Economic Co-operation and Development (OECD) in its 1980 Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Under this

1. Universal Declaration of Human Rights (1948), art. 12; International Covenant on Civil and Political Rights (1966), art. 17 states, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence . . . Everyone has the right to the protection of the law against such interference or attacks"; European Convention, art. 8, states, "Everyone has the right to respect for his private and family life, his home and his correspondence."

approach, consent is a central requirement but may be qualified by a broad and undefined notion of "appropriateness." However, important elements of the human rights approach have been incorporated into Canadian private sector data protection statutes, establishing certain non-waivable rights while also deferring to business "needs." This straddling of approaches is awkward and has led to a sometimes-confused jurisprudence.

Both the OECD Guidelines and the Canadian privacy enactments discussed here confine their ambit to data protection ("recorded information" about identifiable individuals) rather than privacy protection at large. Excluded from data protection law, and thus from the scope of this paper, are privacy issues such as spatial privacy, bodily privacy, search and seizure, and surveillance.

III. CONSENT IN PUBLIC SECTOR PRIVACY LEGISLATION

A. Development of Public Sector Privacy Legislation in Canada

Beginning in the 1980s, Canadian jurisdictions enacted statutory rules for handling personal information, regulating initially only the public sector, and following the voluntary OECD guidelines. The guidelines set a minimum standard of Fair Information Practices, attempting to balance competing interests between privacy protection and business-related transborder data flow; the protection of privacy is always qualified by the need "to avoid undue interference with flows of personal data between Member countries."[2]

The federal Privacy Act[3] was passed as a companion piece with the federal Access to Information Act[4] in 1982. These statutes provide for two separate oversight bodies: the Information Commissioner of Canada and the Privacy Commissioner of Canada. Ontario and the other provinces followed, generally incorporating both privacy protection and access to information in a single statute with a single overseeing Commissioner. Later provincial statutes mirror in significant ways the Ontario access and privacy scheme, with very similar structure and exemptions.[5] The Acts apply to a wide range of federal, provincial, and municipal bodies.

2. Colin J. Bennett, *Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada*, August 1997. (Unpubl). http://web.uvic.ca/~polisci/bennett/research/index.htm.

3. Privacy Act, R.S.C. 1985 c. P-21.

4. Access to Information Act, R.S.C. 1985 c. A-1.

5. The Freedom of Information and Protection of Privacy Act (FIPPA) R.S.O. 1990 c. F.31; and the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) R.S.O. 1990 c. M.56.

B. Legislative Purposes

Privacy statutes in Canada generally include an explicit purpose clause.[6] The Supreme Court of Canada has stated that the purposes of access to government information and protection of privacy are linked to important democratic values, including accountability and citizen participation in government, and the citizen's fundamental right to privacy.[7] Indeed, the Court has characterized the Privacy Act as a quasi-constitutional enactment:

> The *Privacy Act* is also fundamental in the Canadian legal system . . . Its aims are, first, to protect personal information held by government institutions, and second, to provide individuals with a right of access to personal information about themselves . . . The *Official Languages Act* and the *Privacy Act* are closely linked to the values and rights set out in the Constitution, and this explains the quasi-constitutional status that this Court has recognized them as having. However, that status does not operate to alter the traditional approach to the interpretation of legislation . . . The quasi-constitutional status of the *Official Languages Act* and the *Privacy Act* is one indicator to be considered in interpreting them, but it is not conclusive in itself. The only effect of this Court's use of the expression "quasi-constitutional" to describe these two Acts is to recognize their special purpose.[8]

Exceptions from the Privacy Act rights should therefore be interpreted narrowly and should not be used to undermine the broad purpose of the legislation. Strict construction requires that the objective not be frustrated except in the clearest of cases, and the onus lies on those asserting the exception.[9]

The Ontario Freedom of Information and Protection of Privacy Act (FIPPA)[10] is largely based on the recommendations in the 1980 Williams Commission Report.[11] The Report expressed the importance of privacy in human rights language, observing that privacy "is linked to fundamental concerns for the

---

6. Privacy Act s 2 (n. 3): "The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information."

7. *Dagg v Canada (Minister of Finance)* [1997] 2 S.C.R. 403.

8. *Lavigne v Canada (Office of the Commissioner of Official Languages)* 214 D.L.R. (4th) 1, para 24; see also *Heinz, infra* para 28: "The importance of this legislation is such that the *Privacy Act* has been characterized by this Court as 'quasi-constitutional' because of the role privacy plays in the preservation of a free and democratic society."

9. *Lavigne, paras 30–31 (n. 8); Canada (Information Commissioner) v Canada (Immigration and Refugee Board)* [1997] F.C.J. No 1812, paras 34–35 (Federal Court Trial Division); *Reyes v Secretary of State* (1984), 9 Admin. L.R. 296, 299, para 3 (Federal Court Trial Division).

10. Freedom of Information and Protection of Privacy Act (n. 5).

11. *Public Government for Private People,* Report of the Commission on Freedom of Information and Individual Privacy/1980.

preservation of human dignity and personal freedom," identifying "the essential concern of the individual," which is to maintain the right to limit the disclosure and subsequent use of information concerning himself.[12] The Report adopted Alan Westin's definition of informational privacy: "the claim of individuals . . . to determine for themselves when, how and to what extent information about them is to be communicated to others."[13] The Commission recommended provisions to promote individual control over personal information held by government but acknowledged that "the collection of personal information by government is not likely to occur in circumstances in which the individual has an effective choice in refusing to supply the information in question."[14] The Commission recommended balancing individual privacy interests against the legitimate needs of government:

> Important as the informational privacy value is, it is but one of a number of potentially conflicting values competing for attention. The government must gather personal information if it is to successfully and efficiently administer the social and economic programs adopted in response to its perceptions of the public interest; if we are to have a government-operated medical insurance scheme, for example, it is inevitable that some personal information gathering activity will occur. Similarly, concern about the use of surveillance technology by law enforcement authorities must be measured against the need for effective law enforcement. The potential dangers in the use of numerical identifiers such as the Social Insurance Number must be weighed against the desirability of accurate identification of records concerning individuals and the possible benefits of personal data for medical research purposes.[15]

Consent is not the primary mechanism suggested for delivering control. Rather, the Commission recommended that individual control be achieved through the following:

- Notice to the individual of collection of personal information
- Direct collection from the individual
- Access to one's personal information and right of appeal to independent review body
- Right to correction or attachment of statement of disagreement
- Onward disclosure of corrections to those to whom the personal information has already been disclosed
- Right to notice of FOI request, to object or to appeal

---

12. *Ibid.*, 500, 502.
13. *Ibid.* n. 11.
14. *Ibid.* n. 11.
15. Commission on Freedom of Information, *Public Government*, 505 (n. 11).

- Opportunity to refuse consent to:
  - disclosure of personal information pursuant to FOI request
  - inconsistent uses and disclosures
  - early destruction of personal information

Other enacted recommendations include limitations on government collection; restrictions on use and disclosure; standards of accuracy and currency; and secure keeping and disposal of personal information.

Statutory permission to derogate from some rules ensures government flexibility.[16] To better protect personal information, however, governments may be required to undertake Privacy Impact Assessments (PIAs), described by the Privacy Commissioner of Canada as a risk mitigation tool.[17] The federal government issued a directive requiring all federal agencies to conduct a PIA of proposed and revamped projects and programs that may impact privacy. The Privacy Commissioner may review and comment on the PIA and make recommendations, but the decision regarding adoption of the recommendation lies with the government department.[18]

A debate about the proper level of individual control over government processing of personal information arose in 2003. The Saskatchewan Government developed a Framework for handling personal information that made more room for consent.[19] The Information and Privacy Commissioner issued a report criticizing the Framework for going beyond the requirements of the Freedom of Information and Protection of Privacy Act. He noted that under the Act "consent is not usually required for collection, use, or disclosure provided the government institution is only collecting, using, or disclosing for purposes directly related to its core purpose... we are aware of no Canadian jurisdiction that has elected to codify a consent-driven approach for its public sector privacy regime."[20] In his highly critical report, Commissioner Dickson stated that while the Privacy Assessment and Framework were predicated on the CSA Model Code, the latter is "voluntary, consent driven, and not designed for government."[21] "Public sector realities" militate against a consent-based system. In delivering programs, government requires vast amounts of personal information, and the efficient delivery of services would be impaired by a consent requirement and increase

16. See for example, Ontario FIPPA, ss. 39 to 43.

17. Privacy Impact Assessment Fact Sheet, Privacy Commissioner of Canada http://www.privcom.gc.ca/fs-fi/02_05_d_33_e.asp.

18. Treasury Board guidelines for applying the Privacy Impact Assessment Policy.

19. *An Overarching Personal Information Privacy Framework for Executive Government*, 2003.

20. *Report on the Overarching Personal Information Privacy Framework for Executive Government*, June 15, 2004 (Saskatchewan) Response of Information and Privacy Commissioner, CA2 SA IPC A04 R25.

21. *Ibid.*

costs. Other mechanisms ensured that government activity was limited to that necessary for government programs. "As a consequence, public sector privacy rules are not consent based."[22]

C. The Role of Consent in Public Sector Legislation

Public sector consent arises in two distinct contexts: consent to disclosure of personal information in response to access to information (FOI) requests from third-party members of the public; and as a justification for government collection, use, disclosure and retention—just one of many possible justifications. (In certain circumstances the head has a duty to disclose personal information without consent where necessary in relation to a grave health, safety, or environmental hazard.)[23]

Individual consent plays a relatively minor role in public sector data protection law. While it can be relied upon for data uses and disclosures, it is rarely if ever *required*. Consent is only *one* of the statutory factors permitting government to derogate from the basic rules, and it will not usually be sought if government may act under another listed factor. Generally, government will seek or rely on individual consent when it cannot fit a transaction within one of the other derogations, or where it wishes to emphasize the "consensual" nature of a transaction.[24]

Although the Supreme Court has ruled that the federal *Privacy Act* has "quasi-constitutional" status,[25] the Ontario FIPPA lacks explicit language confirming that the privacy rights it creates cannot be bargained away.[26] Some provisions contain prescriptive language, including those for collection, use, and disclosure—"no person shall collect"—indicating that the rules must be followed despite consent.[27] The Ontario Court of Appeal has found that consent is not a substitute if the statutory conditions for collection are not present.[28]

---

22. *Ibid* n. 20.

23. See Ontario FIPPA s 11.

24. For example, where police are requested to provide an employment background check, they usually require the individual being checked to sign a consent form, even where background check is statutorily mandated.

25. *Lavigne* (n. 8).

26. See Preamble to Ontario Human Rights Code: "Whereas recognition of the inherent dignity and the equal and **inalienable** rights of all members of the human family is the foundation of freedom, justice and peace in the world and is in accord with the *Universal Declaration of Human Rights* as proclaimed by the United Nations." See also section 9 of Code: "No person shall infringe or do, directly or indirectly, anything that infringes a right under this Part."

27. E.g., Ontario FIPPA s. 38(2) collection; s 40 retention and accuracy; s 41 "shall not use"; s 42 "shall not disclose" (n. 5).

28. "It is conceded on the appeal that the application judge erred in law by finding that s. 28(2) does not apply where the information is collected on consent. Consent is not one

Conditions for valid collection include that collection be expressly authorized by statute, collected for law enforcement, or *necessary* to the proper administration of a lawfully authorized activity.[29] Additional personal information with limited relevance may not be collected, regardless of consent.[30] Given the remedial nature of the Act, derogation with consent from the protections is likely unlawful, and the government should not be permitted to rely on consent.

In practice, citizens often volunteer additional unnecessary information to government in communications that include necessary information. So perhaps the rule should focus on use, and volunteering the information should be insufficient to permit the use or retention of the additional information.

D. Rights to Withhold or Withdraw Consent

Public sector enactments are largely silent on the right to withhold or withdraw consent. Withholding depends on factors such as statutory or legal requirements compelling compliance, the common law, the ability of the individual to negotiate, and the importance of the government program that may be withheld if consent is not granted. The Ontario Commissioner has said about bargaining with government:

> Any discussion of "choice" must include an analysis of an individual's relative "bargaining power," or range of options available in various situations. When interacting with public sector (government) organizations, an individual is typically faced with a situation in which he or she has asymmetrical bargaining power (i.e., limited, if any, choice).[31]

---

of the three conditions set out in s. 28(2) that allow the collection of personal information by or on behalf of a municipality . . . I also agree with the appellants that contrary to the observation of the application judge, there is evidence in the record that some people who sell second-hand goods require the proceeds to meet their daily needs and therefore, when faced with the choice of providing the information or not selling the goods, cannot confidently be said to be giving their consent freely." See *Cash Converters v City of Oshawa* 2007 ONCA 502, para 34 (Ontario Court of Appeal).

29. Ontario FIPPA s 38(2) (n. 5).

30. Ontario adjudicator held economic duress a factor in requiring welfare recipients to disclose welfare status to potential employers; enforced disclosure **not** necessary to administration of welfare program. See Investigation I94–085P, *Ministry of Housing*, [1995] O.I.P.C. No. 315, 2–3 (Ontario Office of the Information and Privacy Commissioner); Privacy Complaint MC-030044-1, *Toronto Community Housing Corporation*, [2004] O.I.P.C. No. 196, 3–5 (Ontario Office of the Information and Privacy Commissioner).

31. Ann Cavoukian and John Eichmanis, *Privacy as a Fundamental Human Right vs. an Economic Right: An Attempt at Conciliation*, (IPC, Toronto, 1999 p. 1). http://www.ipc.on.ca/images/Resources/up-1pr_right.pdf.

As indicated in the following, a refusal to consent to disclosure is not determinative:

> In general, under the privacy protection provisions of the Act, the mere fact that someone has requested confidentiality with respect to certain information does not, in itself, provide an absolute prohibition on the disclosure of that information. This principle is reflected in the wording of the Act (which does not require consent for all disclosures of personal information) and is supported by compelling public policy considerations. To conclude otherwise would unduly restrict the ability of government institutions, faced with a request of confidentiality from an individual, to disclose personal information where a legal requirement or some other consideration makes it prudent, and correct, to do so.[32]

Requiring individuals to supply unnecessary personal information constitutes an unlawful collection.[33] In practice, where an individual wishes to resist collection, there is usually no prior necessity ruling on point, the discretion as to scope lies with the administrator so the individual may have to "comply now and grieve later."

E. Notice

Notice of collection is one of the most important public sector rights. Along with a default requirement for direct collection of information, it provides transparency regarding content and scope of collection, enabling access and correction rights and aids in knowledgeable consent. The Ontario FIPPA requires that notice must include the legal authority to collect the information, the purposes for which it will be used, and name and contact information for an official who can answer questions.[34]

Government standard consent forms offered as evidence of both knowledge (notice) and consent to collection, use, and disclosure may describe in the broadest and most general terms the information to be collected, the collection sources, the uses, and disclosures. Concerns about standard forms include knowledgeable consent, scope of consent, ability to vary or modify the consent form, and freedom to withhold consent. Where government relies on consent to disclose under FIPPA, consent is explicitly required to be knowledgeable—the individual must identify the "information in particular" and consent to its disclosure. A standard consent form may therefore be too general to enable the person to "identify the information in particular."[35]

---

32. Ontario Investigation Report MC-050017-1.

33. Alberta Information and Privacy Commissioner Investigation Report P2005-IR-007, [2005] A.I.P.C.D. No. 45, 3–4 at paras. 10, 17.

34. *Ontario* FIPPA, s 39(2) (n. 5).

35. See Ontario Investigation Reports I96–119P; I96–071P; Investigation Reports MC-050045-1 and MC-050047-1. The form of consent to employment-related police

F. Conclusions—Public Sector Consent

Given that governments may collect, use, and disclose information without individual consent, it is not contemplated that the individual can negotiate to block or modify transactions. Instead, public sector legislation provides a set of rules (with multiple derogations) that are more in the nature of obligations of government and public servants than a set of individually enforceable "privacy rights."[36] To the extent that individual control is a central aspect of data protection, this results in relatively weak privacy protection.

Governments could give much greater recognition to the sensitivity of the personal information they hold, and to the constitutional dimension of personal privacy rights,[37] by developing a more nuanced approach to individual consent and control respecting personal information.

IV. CONSENT IN PRIVATE SECTOR PRIVACY LEGISLATION

Quebec introduced the first Canadian private sector data protection laws in 1994, with the Act Respecting the Protection of Personal Information in the Private Sector, (Québec Act).[38] The federal Personal Information Protection and Electronic Documents Act (PIPEDA)[39] was enacted in 2001, followed by the Alberta Personal Information Protection Act (Alta PIPA),[40] and British Columbia Personal Information Protection Act (BC PIPA)[41] in 2004. These laws focus on the collection, use, and disclosure of personal information by organizations. The federal law applies only to commercial activities, whereas the three provincial

---

criminal background checks resulted in police disclosing to potential employers information about mental health police records. It was held that the form language was "too broad" and "d[id] not adequately describe the type of information that lead to the disclosure."

36. Ontario's legislation does not provide for individual enforcement of rights (except the right of access to own personal information) or for individual remedies for privacy breaches. See Ontario FIPPA Part III (n. 5) and *Lawrence J. M. David v Robert Binstock, Registrar, Information and Privacy Commissioner/Ontario,* Tor. Doc. 494/04 (Toronto Divisional Court); *Rita Reynolds v Robert Binstock, Registrar, Information and Privacy Commissioner/Ontario,* Tor. Doc. 485/04 (Toronto Divisional Court). The federal *Privacy Act* provides individual access to the Federal Court.

37. See Ontario Superior Court decision regarding the constitutionality of statutory disclosure of adoption information, Charter s. 7 Principle of Fundamental Justice articulated "Where an individual has a reasonable expectation of privacy in personal and confidential information, that information may not be disclosed to third parties without his or her consent." See *Cheskes, Patton* et al. *v Attorney General of Ontario* docket 06-CV-319936PD2, September 19, 2007 (Belobaba J.).

38. R.S.Q. ch.P-39.1.

39. S.C. 2000 c.5.

40. S.A. 2003 c.P-6.5.

41. S.B.C. 2003 c.63.

laws extend to noncommercial activities. All four laws cover employment relationships,[42] and all four exclude certain kinds of activities such as journalism, art and literature,[43] and historical or genealogical material[44] from their scope.[45]

A. Legislative Purposes

There is an interesting divergence among the statutes with respect to statutory purposes. The Québec Act is explicitly designed to particularize the informational privacy rights set out in articles 35–40 of the Civil Code, which establish that "every person has a right to the respect of his reputation and privacy." In contrast, PIPEDA and its two provincial offspring contain purpose clauses referring not only to individual privacy rights but also to "the need of organizations to collect, use, or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."[46] This reference to business needs has led to the application of an uneasy "balancing test" when assessing reasonableness/ appropriateness under the Act.[47] Rather than focusing on the individual's right to privacy and considering legitimate business needs as one of many potential limits on this right, the assessment of legality treats "legitimate" business needs as a primary consideration. The Federal Court of Appeal has held that "the need for balancing is clear from the purpose clause which is section 3 in *PIPEDA*,"[48] stating that:

> even though Part 1 and Schedule 1 of the Act purport to protect the right of privacy, they also purport to facilitate the collection, use, and disclosure of personal information by the private sector. In interpreting this legislation, the Court must strike a balance between two competing interests.[49]

This explicit recognition of the context in which the rights arise—indeed, of the very threats that led to the legislation of those rights—is unusual.

---

42. Although differently: PIPEDA (n. 37) and the Québec Act (n. 36) apply the same rules to employment and consumer relationships; Alberta and BC apply separate rules in the employment context.

43. PIPEDA s 4(2)(c) (n. 37); Alta PIPA s 3(b) (n. 38); BC PIPA s 3(2)(b) (n. 39); Québec Act (n. 36).

44. Québec Act s 1 (n. 36).

45. Such exemptions are broader than, and in addition to, specific exceptions to the general consent rule.

46. PIPEDA s 3 (n. 38); Alta PIPA s 3 (n. 38); B.C. PIPA s 2 (n. 39).

47. *Wansink v Telus Communications Inc.*, 2007 FCA 221 (CanLII), para 10 (Federal Court of Appeal); *Englander v Telus Communications Inc.*, 2004 FCA 387 (CanLII), para 46 (Federal Court of Appeal); *Eastmond v Canadian Pacific Railway* 2004 FC 852 (CanLII), para 129 (Federal Court Trial Division). See also PIPEDA Case Summaries # 14, 39, 279.

48. *Eastmond*, para 129 (n. 45).

49. *Englander*, para 46 (n. 45).

Public sector statutes, in contrast, do not give explicit recognition to governments' legitimate need to use personal information—it is simply implied.

B. The Role of Consent in Private Sector Data Protection Laws

The requirement for consent to the collection, use, and disclosure of personal information is a cornerstone of all three common-law regimes.[50] Such consent must be informed and voluntary: all statutes include notice requirements[51] and a "refusal to deal" provision, prohibiting organizations from requiring, as a condition of the transaction, consent to unnecessary collection, use, or disclosure of personal information.[52] Under all regimes, use or disclosure of the information for different purposes requires additional consent.[53] In some cases, companies have failed the consent test by using overly vague or otherwise inadequate notice regarding their intended uses.[54]

Consent plays a less central but still critical role in Quebec, where it is required for uses and disclosures not relevant to the original stated purpose of collection, but not for the initial collection, which is instead subject to notice obligations, rights of refusal, and a "necessity" requirement.[55] Under the Alberta and B.C. laws, consent plays a limited role in the employment context, where "reasonableness" is more often the test applied.[56]

The consent requirement is accompanied in all four regimes by other obligations derived from the OECD Principles and "Fair Information Practices," including security safeguards, data accuracy, accountability, openness, and individual access to information. Moreover, consent is heavily qualified: each statute includes a long list of law enforcement, emergency, research, and other

50. Quebec law's requirement for consent to collection of personal data is implicit in obligation to inform and individual's right to refuse. See Québec Act ss 8 and 9 (n. 36).

51. PIPEDA Sch.1, Principle 4.3 (n. 37); Québec Act s 8 (n. 36); Alta PIPA s 13 (n. 38); BC PIPA s 10 (n. 39).

52. PIPEDA's refusal to deal provision is slightly different from Alta PIPA and BC PIPA, referring to "the explicitly specified and legitimate purposes" rather than "what is necessary to provide the product or service," but has been interpreted as meaning the latter. Quebec's provision covers employment contracts as well as consumer contracts, and allows exceptions where "authorized by law" or where the request is unlawful.

53. PIPEDA Sch.1, Principle 4.3.1 (n. 37); Québec Act ss 13, 18 (n. 36); Alta PIPA s 8(4) (n. 38); BC PIPA s 8(4) (n. 39).

54. *Englander* (n. 45). See also PIPEDA Case Summaries # 24, 97, 152, 180, 203, 244, 250, 296, 349, and Report on the Investigation into Collection, Use and Disclosure of Customer Information Re: EPCOR [2004] A.I.P.C.D. No. 15; Investigation Report P2004-IR-001 Alberta Information and Privacy Commissioner, (July 26, 2004).

55. Québec Act ss 5–13 (n. 36).

56. Alta PIPA ss 15, 18, 21 (n. 38); BC PIPA ss 13, 16, 19 (n. 39).

exceptions for which nonconsensual collection, use, or disclosure is considered socially desirable.[57]

Less recognized are statutory rights and obligations that apply *regardless* of consent. All statutes include nonconsent-based limits on collection. PIPEDA and the Quebec statute require that collection of personal information be limited to that "necessary" for the specified purposes.[58] (In all regimes, consent must be for specified purposes.) The Quebec law further provides that "in case of doubt, personal information is deemed to be non-necessary."[59] The Alta PIPA requires that collection be "reasonable" for the specified purposes,[60] while the BC PIPA requires simply that the collection must fulfill the specified purposes.[61] Although this suggests a lower standard of protection in the western provinces, such does not appear to be the case in practice. Alberta's "reasonableness" requirement has been interpreted as "necessary,"[62] while the issue appears not yet addressed in B.C. Numerous PIPEDA and Quebec cases have found noncompliance because of unnecessary collection of personal information for authentication, employee checks or other purposes.[63]

All regimes also require that the specified purposes and/or practices meet a test based on reasonableness/appropriateness or fundamental rights.[64] These rights operate regardless of consent, and thus complement the consent-based analysis. Subsection 5(3) of PIPEDA limits the purposes for which organizations can legitimately collect, use, or disclose personal information to those purposes "that a reasonable person would consider are appropriate in the circumstances." This clause has been relied upon in numerous PIPEDA findings, both as an inquiry separate from consent[65] or conflated with the consent analysis, as a basis on which to find that consent was or was not present.[66]

---

57. PIPEDA s 7 (n. 37); Alta PIPA ss 14, 17, 20 (n. 38); BC PIPA ss 12, 15, 18 (n. 39). Some of these exceptions have been the focus of fierce debate among stakeholders, while others are widely accepted.

58. PIPEDA Sch.1, Principle 4.4 (n. 38); Québec Act, s 5 (n. 36).

59. Québec Act, s 9 (n. 36).

60. Alta PIPA s 11(2) (n. 38).

61. BC PIPA s 11(a) (n. 39).

62. In Alberta Report P2005-IR-007, the Alberta Commissioner wrote, "If the collection of D/L number is not necessary for a business purpose, it cannot, as required by section 11(2), be reasonable for meeting the purposes for which the information is collected."

63. See PIPEDA Case Summaries # 22, 97, 257, 288; *X. c. Ameublements Tanguay*, [1995] C.A.I. 377 (Inquiry Report); *Pleins Droits de Lanaudière inc. et Oeurvres du Toit de Bethléem inc.* [1996] C.A.I. 399.

64. PIPEDA s 5(3) (n. 37); Alta PIPA ss 11(2), 16(2), 19(2) (n. 38); BC PIPA s 14 (n. 39); Quebec CCQ, Art.3, 37; Québec *Charter of Human Rights and Freedoms,* R.S.Q. c.C-12, s.5.

65. E.g., PIPEDA Case Summaries # 48, 94, 152, 193, 256, 280.

66. E.g., PIPEDA Case Summaries # 24, 40, 99, 104, 127, 152, 232, 245, 281, 287, 288.

Although apparently limited to "purposes," the provision has been interpreted as extending to practices.[67] For example, overly invasive debt collection practices have been found to violate PIPEDA, although the purpose of debt collection is clearly legitimate.[68] This broad interpretation of Subsection 5(3) recognizes the limits of consent as an effective data-protection principle. Without it, PIPEDA would fail to protect against excessive disclosure and other inappropriate practices, even where consent is not required. In recognition of this gap, both Alberta and B.C. supplement their consent-based regimes with rules requiring that the *practices* of collection, use, and disclosure, as well as the *purposes* behind them, be reasonable.[69]

While the Quebec statute does not include a "reasonableness" standard, per se, its express purpose is to establish rules "for the exercise of the rights conferred by articles 35 to 40 of the Civil Code."[70] Article 37 of the Code mandates "serious and legitimate reason[s]" for the creation of a file on another person, and states that one must not, "when establishing or using the file, otherwise invade the privacy or damage the reputation of the person concerned."[71] Moreover, the Québec Charter of Human Rights and Freedoms establishes privacy as a human right, stating, "Every person has a right to respect for his private life."[72] These provisions have been referenced in cases involving alleged breaches of the Québec Act,[73] as grounds for applying a reasonableness/proportionality test similar to that developed by the Supreme Court of Canada in *R. v. Oakes*.[74]

It has been argued that as a result of over-emphasis on consent, "a robust reasonable purposes test has not been developed" under PIPEDA.[75] If this is true, we submit that it is less a result of "over-emphasis on consent" per se, and more a result of conflation by some decision-makers of consent and reasonable purposes. In any case, our review suggests that a surprisingly robust "reasonable purposes" test has in fact emerged from the PIPEDA case law to date.[76] The test has been applied in a manner akin to the test for justification of otherwise

67. *Eastmond* (n. 45). See also PIPEDA Case Summaries #61, 99, 130, 232, 245, 282, 317.

68. PIPEDA Case Summaries #61, 130, 282, 317.

69. Alta PIPA, ss 2, 6, 11(2), 16(2), 19(2) (n. 38); B.C. PIPA, ss 4(a), 11, 14, 17 (n. 39).

70. Québec Act, s.1 (n. 36).

71. Civil Code of Québec, R.S.Q. c.C-1991.

72. Québec Charter of Human Rights s 5 (n. 62).

73. *St-Amant c. Meubles Morigeau ltée*, [2006] R.J.Q. 1434 (Québec Superior Court); *Pitre v Industrielle Alliance, compagnie d'assuances générales* (6 November 1995) Québec 200-32-000046-952, J.E. 96-19 (C.Q. civ. Pet. Cré.) (Azimut); *Pouliot c. Biochem Pharma Inc.* [1996] R.J.Q. 1845; *Duchesne v La Great-West, Compagnie D'Assurance-Vie* (14 December 1994) Alma 160-05-000129-867 (C.S.) (Azimut).

74. [1986] 1 S.C.R. 103, 1986 CanLII 46 (S.C.C.).

75. Lisa Austen, "Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA," *University of Toronto Law Journal* 56 (2006): 181.

76. *Wansink* (n. 45); *Eastmond* (n. 45); PIPEDA Case Summaries #279, 290, 351.

Charter-infringing activity established by the Supreme Court of Canada in *R. v. Oakes*.[77] It has been set out in a clear and logical manner, with four criteria:

i) Demonstrable necessity to meet a specific need
ii) Likely effectiveness in meeting that need
iii) Proportionality between loss of privacy and benefit gained
iv) Absence of a less privacy-invasive means of achieving the same goal

It has been most clearly and convincingly articulated in the context of employee monitoring and surveillance,[78] but also in the context of employer use of biometric[79] and GPS[80] systems.

A similar balancing test has been applied under the Quebec law.[81] Quebec jurisprudence also separates the requirements of consent and necessity: both criteria must be met for valid collection, use, or disclosure.[82]

C. Limits on Contracting Out of Privacy Rights

In addition to these important complements to consent-based data protection, some statutes include explicit provisions invalidating attempts by organizations to contract out of their statutory obligations. The Alta PIPA provides that any waiver or release from the protections of the Act is against public policy and therefore void.[83] Although the B.C. Act expressly prohibits only those contractual waivers relating to withdrawal of consent,[84] the B.C. Privacy Commissioner has expressed "serious reservations about any suggestion that one can validly derogate from [any of] PIPEDA's minimum standards or protections by contract."[85]

Similarly, although the Québec Act has no explicit provision invalidating contractual waivers, Article 8 of the Civil Code of Québec states that "no person may renounce the exercise of his civil rights, except to the extent consistent with public order," and Quebec courts and Privacy Commissioners have found that the "necessity" criterion cannot be overridden by individual consent.[86]

---

77. *Oakes* (n. 72).

78. *Eastmond* (n. 45); PIPEDA Case Summaries #279, 290.

79. *Wansink* (n. 45); PIPEDA Case Summary #281.

80. PIPEDA Case Summary #351.

81. *Pouliot* (n. 69); *Laval (Ville) v X.* (21 February 2003) Montreal 500-02-094423-014 (Cour du Québec, Chambre civile).

82. *Laval* (n. 77).

83. Alta PIPA s 4(7) (n. 38).

84. BC PIPA s 9(3) (n. 39).

85. Order P05–01 (May 25, 2005); *K.E. Gostlin Enterprises Limited* [2005] B.C.I.P.C.D. No. 18 (QL).

86. *Laval* (n. 77); *Tremblay v Caisse populaire Desjardins de St-Thomas*, [2000], CAI 154 (Inquiry Report); *Julien v Domaine Laudance*, [2003] CAI 77; *A. v C.*, [2003] CAI 534; *Agyemang v Ipex Inc.*, [2001] CAI 201.

In contrast, PIPEDA not only lacks a "non-waivability" provision, but expressly permits the waiver of one's right to withdraw consent. Principle 4.3.8 states:

> An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

Although an outlier with respect to other data protection regimes, the existence of this specific permissive provision suggests that other rights under PIPEDA cannot be so waived.[87] Moreover, as the B.C. Privacy Commissioner has found,[88] the public policy nature of privacy rights argues strongly for the invalidation of contractual waivers from those rights, especially in the context of contracts of adhesion. A finding that rights set out in data protection laws cannot be surrendered by individuals other than in exceptional circumstances would be consistent with Canadian common law on statutory illegality.[89]

D. Forms of Consent—Criteria for Validity

The Quebec law requires that consent be "manifest" in order to be valid. Thus, unless it can be logically inferred from the actions of the individual, consent must be positively communicated through an "opt-in" process.[90] However, s.17 of the Act sets out a significant exception to this rule: in the case of "nominative lists" (names and contact information), enterprises may communicate the information to third parties for commercial or philanthropic prospection, as long as they give individuals on the list a "valid opportunity to refuse" such use of their personal information.[91]

In contrast, the three common-law statutes allow for opt-out consent generally, provided that certain conditions are met. The Alberta and B.C. statutes permit opt-out consent only where the individual is notified, given a reasonable opportunity to decline, and does not decline after a reasonable period of time; and where the collection, use, or disclosure in question is reasonable given the sensitivity of the information.[92] PIPEDA gives only general guidance, stating that "an organization should generally seek express consent when the information is likely to be considered sensitive."[93] However, the federal Commissioner has articulated criteria for valid opt-out notice, including limited and well-defined purposes; clear notice, brought to the individual's attention at the time of collection;

---

87. This issue does not appear to have been addressed in PIPEDA case law.

88. *Order P05-01* (May 25, 2005).

89. Waddams, *The Law of Contracts*, 5th ed. (Aurora: Canada Law Book, 2005) 396, para 560; *Still v M.N.R.* (C.A.), (1997), [1998] 1 F.C. 549 (Federal Court of Appeal).

90. *Bedard v Robert, J.E.* 2003–589 (S.C.).

91. *Deschenes c. Groupe Jean Coutu* et al. PV 98 08 42.

92. Alta PIPA s 8(3) (n. 38); B.C. PIPA s 8(3) (n. 39).

93. Principle 4.3.6 (n. 37).

and a convenient procedure for opting out of secondary purposes.[94] Disturbingly, a 2006 CIPPIC study of online retailers found that, while the vast majority of companies rely upon opt-out consent for secondary uses and disclosures, most fail to meet one or more of these criteria for valid opt-out consent.[95]

A key criterion for valid opt-out consent is notice. Yet, none of the four statutes specifically requires that notice be *brought to the attention of* the individual. PIPEDA merely requires "a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used."[96] The Alberta and B.C. PIPAs merely require that notice be "in a form that the individual can reasonably be expected to understand" and that "gives the individual a reasonable opportunity to decline."[97] Although courts and commissioners have interpreted these provisions as requiring that notice of purposes and opt-out options be brought to the attention of individuals at the time of collection,[98] studies indicate that many businesses are not doing so.[99] Without a clear requirement for *effective* notice (and enforcement of it), opt-out consent becomes meaningless. Even then, theoretical and empirical studies in psychology and economics suggest that opt-out consent protocols will always result in a large number of cases in which consent is wrongly assumed.[100]

E. Rights to Withhold, Negotiate, and Withdraw Consent

All three common-law statutes give individuals the right to withhold consent to unnecessary purposes,[101] while Quebec's Act requires that consent be "free,"[102] and that organizations relying on opt-out consent "grant the persons concerned a valid opportunity to refuse."[103]

---

94. PIPEDA Case Summary #207.

95. Canadian Internet Policy and Public Interest Clinic (CIPPIC), *Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up?* (April 2006).

96. Schedule 1, Principle 4.3.2 (n. 37).

97. Alta PIPA s 8(3)(a) (n. 38); B.C. PIPA s 8(3)(a) and (b) (n. 39). The B.C. PIPA also requires that the organization "disclose to the individual verbally or in writing . . ."

98. See *Englander* (n. 45); PIPEDA Case Summaries #24, 244, 263, 273; *Marbre c. Clearnet SCP* C.A.I., Doc # 99 01 29.

99. CIPPIC, *Compliance* (n. 91); EKOS Research Associates Ltd., *Business Usage of Consumer Information for Direct Marketing: What the Public Thinks* (Public Interest Advocacy Centre, 2001).

100. Ian Kerr et al., "Soft Surveillance, Hard Consent," *Personally Yours* 6 (2006): 1–14; Eric Johnson, Steven Bellman and Gerald Lohse, "Defaults, Framing and Privacy: Why Opting in ≠ Opting Out," *Marketing Letters* 13, no. 1 (2002): 5–15.

101. PIPEDA, Schedule 1, Principle 4.3.3 (n. 37); Alta PIPA s 7(2) (n. 38); BC PIPA s 7(2) (n. 39); see also Québec Act s 9 (n. 36).

102. Québec Act s 14 (n. 36).

103. Québec Act s 232(2) and s 23 (n. 36).

In addition, Alberta's Act includes an unusual provision allowing individuals to *negotiate* the terms of their consent. Subsection 7(3) states:

> An individual may give a consent subject to any reasonable terms, conditions or qualifications established, set, approved by or otherwise acceptable to the individual.

This appears to validate individual consumer revisions to standard form agreements regarding data collection, use, or disclosure, as long as they are reasonable.[104]

PIPEDA includes a right to withdraw consent at any time upon reasonable notice, but subject to "legal or contractual restrictions."[105] Alberta and B.C. include more robust and detailed withdrawal rights that can be overridden if withdrawal would frustrate the performance of a legal obligation.[106] In contrast to PIPEDA, B.C.'s provision expressly forbids organizations from prohibiting the withdrawal of consent, and as noted, the Alta PIPA includes a general prohibition on contractual waivers. The Québec Act includes no general right to withdraw consent,[107] but does give individuals the right to remove their names from "nominative lists,"[108] and is subject to the Quebec Civil Code, which includes a non-waivability clause.[109]

Rights to withdraw are an essential component of consent rights if, as we posit, the purpose of such rights is to give individuals control over their personal information. However, they may be more illusory than real, given human tendencies to accept the status quo.[110]

F. Conclusions—Consent in Private Sector Data Protection Law

Although different in important respects, all four private sector data protection laws in Canada treat consent as one part of a two-part test to determine validity of data collection, use, or disclosure. A baseline reasonableness test applies, regardless of whether consent is required or was obtained. This ensures, at least in theory, that individuals remain protected from inappropriate uses and disclosures of their personal information even when consent is not required or was given without full awareness. Moreover, consent cannot, in general, be used to

---

104. We could find no case law interpreting this provision.

105. Principle 4.3.8 (n. 37).

106. Alta PIPA s 9 (n. 38); BC PIPA s 9 (n. 39).

107. This was confirmed in the case of *X. v Equifax*, in which the Commission found that there is no general right to withdraw consent or to have one's information deleted from a file: CAI File No.03 21 10 (27 May 2005).

108. Québec Act ss 17(2), 25, 26 (n. 36).

109. Quebec CCQ Article 8.

110. Kerr et al., "Soft Surveillance, Hard Consent" (n. 96).

vitiate statutory privacy rights.[111] It is designed to enhance, not to diminish, established rights.

The role of consent in this context is, clearly, to provide individuals with greater *control* over their personal information, above and beyond those protections against privacy invasions that they enjoy as a result of reasonableness-based limits on corporate data activities. That consent is designed to provide control is demonstrated by, for example, Alberta's provision allowing individuals to set conditions on their consent,[112] Quebec's time limit on consent,[113] Alberta, B.C., and PIPEDA's rights to withdraw consent,[114] and all three provinces' limits on collection from third parties.[115]

But there is reason to question the effectiveness of the control that these consent provisions actually provide to individuals—less because of the numerous exceptions to consent in each statute, and more because of the explicit recognition of business "needs" and sanctioning of opt-out consent under each regime.[116] Theoretical and empirical studies have questioned both the validity and the effectiveness of opt-out consent.[117] Indeed, one could argue that the validity of opt-out methods eliminates the very control that consent is meant to provide. Consent is meaningless without awareness of that to which one is being assumed to consent. For this reason, we believe that informational privacy may ultimately be protected less by consent requirements and more by rights-based reasonableness tests incorporated in each statute.

V. CONCLUSIONS

Consent is a critical component of data protection, providing individuals with some control over their informational privacy. However, it offers insufficient protection on its own, given the realities of human, government, and marketplace behavior. This is so in both the public and the private sectors, where consent requirements need to be supplemented with reasonableness standards for effective data protection.

111. The clear exception to this rule is PIPEDA's clause allowing individuals to contract out of their right to withdraw consent.

112. Alta PIPA s 7(3) (n. 38).

113. Québec Act s 14 (n. 36).

114. Alta PIPA s 9 (n. 38); B.C. PIPA s 9 (n. 39), PIPEDA Schedule 1 Principle 4.3.8 (n. 39).

115. Québec Act s 6 (n. 38); Alta PIPA ss 7(1)(b), 13(2), (3) (n. 38); B.C. PIPA s 12(2) (n. 39).

116. Albeit more limited under the Quebec law, which permits opt-out consent protocols only with respect to name, address, and telephone number ("nominative lists"): see Québec Act s 22 (n. 36).

117. CIPPIC *Compliance* (n. 91); EKOS (n. 92); Kerr et al., "Soft Surveillance, Hard Consent" (n. 96).

The most striking difference between the public and private sector regimes is the relative importance and role of consent. Although central to private sector regimes, consent plays a minor role in public sector privacy protection

Despite their flaws, the four private sector data protection statutes establish a sensible regime in which consent plays an important but not determinative role. Their greatest flaw is, arguably, the explicit recognition of business needs and consequent sanctioning of opt-out consent, without effective notice requirements. Consent requirements should be accompanied by stronger notice requirements as well as more effective enforcement regimes in these statutes.

In contrast, public sector data protection laws rely less on consent and more on privacy protective rules and processes required of government. Yet, the technological capacity of government to track and surveil citizens is beyond anything contemplated at the time of enactment of these laws. Privacy laws have simply not kept pace with advances in technology.[118] In this context, public sector deprivation of individual control may go too far in protecting government interests and it is disrespectful of individual autonomy and dignity. It is also disrespectful of the sensitive nature of the personal information collected and the constitutional aspects of privacy protection. Although individual consent is clearly inappropriate in some circumstances (such as tax administration), it is not always inappropriate in the public sector context. A case-based analysis would, in our view, indicate areas in which more choice on the part of the individual is warranted.

In a liberal democracy, values of participatory democracy and citizen autonomy should lead to greater control by citizens over their personal information. However, such control must be real, not illusory. Experience with private sector data protection laws suggests that consent is not completely effective. Any reforms designed to give citizens more control over their government-held information should take heed of that experience.

118. Uwe Hessler, *Harsh Words from German Commissioner on Data Protection: Who's in the Driver's Seat Concerning Data Privacy?* Deutsche Welle 24.04.2007, http://www.dw-world.de/dw/article/0,2144,2456060,00.html.

Privacy Commissioner of Canada, *Annual Report to Parliament,* 2004–2005, http://www.privcom.gc.ca/information/ar/200405/200405_pa_e.asp.