Reflections on Reform of the Federal *Privacy Act*

David H. Flaherty*

June 2008

*Privacy and Information Policy consultant, Victoria, BC; Professor Emeritus, University of Western Ontario; 1st Information and Privacy Commissioner for British Columbia; author of Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States (1989).

"Today's commonplace information technologies — the Internet and new surveillance technologies such as digital video, linked networks, global positioning systems, black boxes in cars, genetic testing, biometric identifiers and radio frequency identification devices (RFIDs) — did not exist when the federal *Privacy Act* came into force in 1983. Characterizing the current Act as dated in coping with today's realities is an understatement — the Act is tantamount to a cart horse struggling to keep up with technologies approaching warp speed."[1]

"The federal *Privacy Act* is woefully deficient as a vehicle for protecting the privacy rights of Canadians. Time and again, Privacy Commissioners and privacy advocates have called for a thorough review and modernization of the legislation. The *Privacy Act* contains no effective mechanism to deal strategically with complaints, requiring that every complaint be examined – a potentially overwhelming, but unnecessary, burden. The Act was drafted well before the extensive penetration of computing power and surveillance technology into our lives. It was drafted long before the era of globalization and the extensive sharing of personal information across borders with corporations, with governments, and indirectly through corporations to foreign governments. It was drafted long before the era when the word terrorism began to fall from everyone's lips amid calls for ever greater amounts of personal information in the quest to enhance personal and national security."[2]

"The *Privacy Act* is at the hub of the informational relationship between state agencies and individuals. If the legislative framework that governs this relationship is weak, the entire edifice of accountability is undermined. Privacy is too important to be left to the vagaries of internal policy and management."[3]

---

[1] Privacy Commissioner of Canada, Annual Report to Parliament, 2004-2005, at http://www.privcom.gc.ca/information/ar/200405/200405_pa_e.asp

[2] "Response of the Privacy Commissioner of Canada about Possible Fusion of the Offices of the Privacy Commissioner of Canada and the Information Commissioner of Canada," Submission of the Office of the Privacy Commissioner of Canada to the Hon. Gérard La Forest, who was reviewing the issue, October 21, 2005, final page, at http://www.privcom.gc.ca/information/pub/sub_merger_051021_e.asp.

[3] Jennifer Stoddart, Privacy Commissioner of Canada, House Standing Committee on Access to Information, Privacy and Ethics, April 8, 2008.

Introduction

In what follows, I am taking advantage of the privileges of older age to write about matters that interest me on the basis of both memory and published material, especially from the years starting around 1974 when I began to take a close, critical interest in the development of data protection legislation in North America and Western Europe.[4] The purpose of these 'reflections' is not to produce an exhaustive, original piece of research, but rather to attempt to make a compelling and necessary case for immediate reform of an important, but now obsolete, piece of legislation. In so doing, I believe a return to the history of data protection is necessary, even if it is limited to a broad and general overview.

As someone trained as an historian, and with a career as an historian in my past, I am also well aware that there are relatively few original ideas in this world about almost anything, so I have enjoyed the task of revisiting and reconsidering ideas that I was exposed to at the feet of masters in the development of data protection legislation, and/or that I have borrowed from my friends, colleagues, and mentors in the global privacy community. I have also taken advantage of my circle of friendship in privacy matters to read and re-read the writings of many of my friends and also to interview some of them. Those who were willing and able to review earlier drafts are gratefully acknowledged below.[5]

Some readers will be familiar with the annual rankings of Privacy International, a human rights watchdog group based in London, which place Canada near the top of the privacy-league rankings.[6] Given the global perspective of Privacy International and its driving forces, I am inclined to take such praise with only a wisp of satisfaction, knowing full well that Canada only looks good compared to some truly benighted nations, such as the United Kingdom and the United States, where gross invasion of personal privacy is a daily sport of the business community, politicians, and lawmakers.[7] Privacy International is blessedly unaware of, and/or turns a blind eye to, some of the least progressive aspects of Canadian privacy law and practice, such as the antiquated federal *Privacy Act* and the lack of resourcing of privacy functions at federal government institutions.

---

[4] My attempted reliance on memory quickly floundered on the sands of the direct evidence of the frailty and fallibility of memories in general and my own in particular. My own published writings have been much more reliable in this regard.

[5] Thanks to friends and colleagues who provided detailed critiques of my drafts, including Ken Anderson, Colin J. Bennett, Robert Gellman, Ross Hodgins, Mimi Lepage, T. Murray Rankin, Q.C., and Gordon Smith.

[6] See http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559597. In the interests of candour, I have been an advisor to Privacy International since its inception, but I have not participated in the ranking process described here.

[7] The UK Information Commissioner's sponsored study of "Surveillance Societies" is accessible at http://ico.crl.uk.com/files/Surveillance%20society%20full%20report%20final.pdf
The latest critical review of the American scene is James B. Rule, Privacy in Peril (Oxford University Press, New York, 2007); see also Robert O'Harrow, Jr., "Centers Tap Into Personal Databases. State Groups Were Formed after 9/11," Washington Post, April 2, 2008, p. A1.

The collective goal of privacy advocates is robust data protection and security, with meaningful implementation over time, in all democratic societies. The operative words here are 'meaningful implementation over time.' While the *Privacy Act* was a progressive privacy statement in the early 1980s, it is now an outdated Act that no longer properly regulates how federal institutions collect, use, retain and disclose personal information. Data protection legislation (including the *Privacy Act*) is one, and only one means, to that end, as this essay will illustrate.

Reform of the *Privacy Act* should be made to appeal unanimously to the media, public servants, the political elite, the government of the day, and Members of Parliament, because privacy protection is a winning issue in an age of increased awareness and anxiety about identity theft and other forms of invasions of privacy. Widespread loss and misuse of personal information, fraud, privacy breaches, and the overall dissipation of personal privacy and the consequential loss of control over one's personal affairs has resonance with Canadians, notwithstanding innumerable counter forces like the necessity of personal and collective security. While polls show high anxiety about the preservation of privacy, lack of political leadership and commitment has hindered progress to date.[8] A primary goal of this essay is thinking about how to motivate such necessary change and to advance the cause of reform of the *Privacy Act* on the ground that such analysis and transformation is long overdue. The *Privacy Act* is a twenty-five year old house that has had little maintenance and refurbishment. It is now ripe for a major rehab job. Fiddling with the paint, or redecorating one room, will not do the job.[9]

Shaping a revised law and then implementing data protection are complex activities (although the former is much easier than the latter). However, updating the *Privacy Act* is an act of due diligence and good housekeeping for the federal government on an issue of public policy that is much more manageable than the more intractable problems facing Canada. There are no good reasons for further delays.

The case for immediate reform of the *Privacy Act* will be based on the following arguments:

(1) Privacy is a fundamental, societal value, and Canadians deserve and expect meaningful privacy/data protection laws;

(2) The Privacy Act is an antiquated piece of legislation, which does not meet the "national privacy standard" set out by Parliament in the *Personal Information Protection and Electronic Documents Act (PIPEDA);*

(2) An effective data protection law is contingent on adequate statutory powers for a meaningful and efficient oversight role for the Privacy Commissioner of Canada, which means the power to make orders; and

---

[8] See the Ekos poll conducted for the Privacy Commissioner of Canada in 2006 at http://www.privcom.gc.ca/information/survey/2006/ekos_2006_e.asp

[9] While I agree with the ten quick fixed offered up by the Privacy Commissioner of Canada, they are only a modest start at what is required. Testimony of Jennifer Stoddart, Committee on Access to Information, Privacy and Ethics, April 29, 2008.

(3) In order to have robust implementation of a data protection law, Parliament has to mandate a structure for privacy risk management in each federal institution, including Chief Privacy Officers, Privacy Impact Assessments, and privacy training.

The Constitutional Bases for Canadian Privacy Rights

It is important to emphasize at the outset the significance of privacy as a human value, as a human right, and, indeed, a constitutional right under the Canadian *Charter of Rights and Freedoms*.[10] Why is privacy important in Canada and to Canadians? Privacy is key in Canada because it forms an essential component of our collective social values and our legal landscape. Canadians lobbied hard for privacy protection in the 1970s and early 1980s. Privacy was first recognized as a human right in the *Canadian Human Rights Act* and was subsequently entrenched in the *Canadian Charter of Rights and Freedoms.* As a result, Canadians have come to expect and deserve adequate privacy protection as an essential component of our human dignity in Western societies.[11]

Appropriate resourcing of the implementation of data protection may also be problematic and therefore requires an ongoing commitment to the human rights goals of the legislation, which Parliament and legislatures frequently forget. Data protection is part of a legal framework intended to afford reasonable expectations of privacy rights articulated by the courts under the Canadian *Charter of Rights and Freedoms*; a "privacy" law is supposed to be about protecting human rights, which gives privacy an elevated stature in the pantheon of Canadian values protected by law. Speaking for the entire Supreme Court in a 1997 case, Justice La Forest stated that "[t]he protection of privacy is a fundamental value in modern, democratic states; …. An expression of an individual's unique personality or personhood, privacy is grounded on physical and moral autonomy — the freedom to engage in one's own thoughts, actions and decisions;…. Privacy is also recognized in Canada as worthy of constitutional protection, at least in so far as it is encompassed by the right to be free from unreasonable searches and seizures under s. 8 of the *Canadian Charter of Rights and Freedoms*;…."[12]

A recent startling development in the Canadian courts may foreshadow the ultimate constitutional weapons that Canadians will have to use to seek to protect their individual privacy, that is, asserting constitutional claims to privacy against government actions that are perceived to intrude on the privacy rights of individuals. The short version of the story is that the Ontario government, in its wisdom, wanted to enhance access to adoption records. The Ontario Information and Privacy Commissioner, Dr. Ann Cavoukian, despite advancing strong privacy arguments in a vigorous manner, was unable to persuade the Liberal government to make it possible for adult adoptees and adoptive parents to prohibit access to their personal information when they did not want to be

[10] See *Dagg v. Canada (Minister of Finance)* [1997] 2 S.C.R. 403.
[11] See Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser," New York University Law Review, 39 (1962), 962-1007; and the discussion of the goals of privacy legislation in Colin J. Bennett and Charles D. Raab, The Governance of Privacy. Policy Instruments in Global Perspective (MIT Press, Cambridge, MA, updated paperback edition, 2006), chapter 1.
[12] Quoted in *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] SCC, no 53, para. 25.

discovered. Several adoptees persuaded a talented crew of lawyers led by Clayton C. Ruby to challenge sections of the *Adoption Information Disclosure Act* in the Ontario Superior Court of Justice.

The result was a strong decision by Justice Edward Belobaba in support of the privacy rights of the litigants on the basis of section 7 of the *Charter*, resulting in the Ontario government revising the portions of the disputed law.[13] As the judge stated:

> [78] This case, in essence, is about the applicants' right to privacy. The basic issue is whether the applicants have a *Charter*-protected right to privacy in circumstances such as these where confidential, personal information is about to be released by the government, retroactively, and without their permission, to the persons whom they would least want to have it….
>
> [83] In this case, … the disclosure of the birth and adoption records under the new law , in circumstances where a reasonable expectation of privacy has been created, … constitutes an invasion of the dignity and self-worth of each of the individual applicants, and their right to privacy as an essential aspect of their right to liberty in a free and democratic society has been violated.

The Ontario Liberal government did not appeal this decision and plans to institute a disclosure veto as Dr. Cavoukian and others had initially recommended.

The reality is that the *Privacy Act* is closely tied to the values and rights acknowledged under the Canadian constitution, which explains its quasi-constitutional status, as acknowledged by the Supreme Court of Canada in *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] SCC, no 53, para. 24. The Court also stated that the "Privacy Act is a reminder of the extent to which the protection of privacy is necessary to the preservation of a free and democratic society." (para. 25) The Supreme Court has also recognized, on a number of occasions, the quasi-constitutional status of the protection of personal information because of the role of privacy protection in the maintenance of a free and democratic society: *H. J. Heinz and Co. Ltd v. Canada (Attorney General*), [2006] SCC 13, para. 28. Given the quasi-constitutional character of the protection of personal information, the right to privacy that the law confers on an individual in Canada is qualified as a quasi-constitutional right to privacy. This presupposes a strong *Privacy Act*.

The History of the Privacy Act[14]

The history of all law reform in English-speaking countries is a discouraging topic, especially that component of it which requires revising an existing piece of major

---

[13] *Cheskes v Ontario (Attorney General)*, 2007 CanLII, 38387 (On. S.C.), Sept. 19, 2007, http://www.canlii.org/en/on/onsc/doc/2007/2007canlii38387/2007canlii38387.html

[14] Readers have asked me why this account is so personalized. I obviously believe, based on my close observation of what was actually happening, that the people I have highlighted made a big difference because of their commitment to, and understanding of, the need for a data protection law. While they were not impervious to broad historical forces, such as the computerization of society, they promoted action to legislate because they decided it was the right thing to do. Canadians deserve such leadership today.

legislation. The enormous amount of creative energy and political will required to enact such a law quickly dissipates once the honeymoon phase is over, and the hard slogging of implementation begins, and continues on interminably, with limited energy and finite human and financial resources for such purposes. That, surely, is the history of data protection in Canada in the case of the federal *Privacy Act*, which entered into force on July 1, 1983.[15] Except for the U.S. *Privacy Act* of 1974, this Canadian law is the oldest piece of unrevised national privacy legislation in the English-speaking world. By the standards of 2008, it is a sorry piece of privacy legislation, especially in comparison to the counterpart law, the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), which now regulates the private sector in Canada (in the absence of substantially-similar provincial legislation).[16] To give but two examples, the private sector has to comply with a requirement to obtain information consent and to maintain security safeguards for personal information that have no direct counterparts in the *Privacy Act*.

It is worth celebrating the political sponsorship that brought the 1982 Privacy Act (Bill C-43) into existence. After the fall of the Joe Clark government in December, 1979, Conservative M.P. (and former Cabinet Minister) Perrin Beatty introduced as a private member's bill, Bill C-535, the *Privacy Act*, 1980, which was in fact the legislation that the Clark government had been working on to create a stand-alone federal privacy regime. The Clark government's greater interest was in introducing an access to government information (freedom of information) law. Public servants from the Department of Justice and the Privy Council Office simply revised Part IV of the *Canadian Human Rights Act* (enacted in 1977) at the same time on their own initiative. It had been the first piece of federal data protection legislation.[17]

A Cabinet Discussion Paper, June, 1980, prepared by the Department of Justice, outlined the key elements of what became the new *Privacy Act*. It amended Part IV to ensure consistency with freedom of information legislation and also to improve privacy protection.[18] Francis Fox, as Minister of Communications, shepherded the Access to Information and Privacy laws through Parliament. Committed Justice specialists like Barry Strayer (now a judge of the Federal Court of Canada), Stephen J. Skelly, Q.C., and Gillian Wallace, Q.C. (subsequently Deputy Attorney General for B.C.) were the brainpower on privacy legislation in the federal public service during this creative period that began in the early 1970s. Similar legislative initiatives in the Federal Republic of

---

[15] Its predecessor, Part IV of the *Canadian Human Rights Act* of 1977, was proclaimed in force on March 1, 1978.

[16] The OPC wrote in June, 2006 that "[t]he deficiencies in the *Privacy Act* are readily evident when compared to the comprehensive set of fair information principles embodied in *PIPEDA*." See Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 5; see also pp. 7-8. The *Personal Information Protection* Acts for the private sectors in B.C. and Alberta are even better than *PIPEDA* because of their coherent structure.

[17] For the history of its development, see David H. Flaherty, Privacy and Government Data Banks. An International Perspective (Mansell, London, UK, 1979), pp. 230-34. Key stages included the Privacy and Computers Task Force, which reported in December, 1972, and the Interdepartmental Committee on Privacy, chaired by the Departments of Justice and Communications.

[18] See Flaherty, Protecting Privacy in Surveillance Societies, pp. 243-46.

Germany, Sweden, and the United States inspired this Canadian leadership, as well s such underlying forces as included the ongoing computerization of society (which appears to be a quaint phrase in the world of the Internet and the World Wide Web).[19]

The key role of these politicians and public servants is a reminder that a committed cadre of subject-matter specialists is instrumental to both the introduction and further revision of any significant piece of privacy legislation. Coupling this commitment with political sponsorship from the government of the day is even more essential as happened again with the introduction of *PIPEDA* in the late 1990s, when the stimuli for action included protecting the trading interests of Canada in the face of the European Directive on Data Protection).[20] John Manley and Allan Rock were the key political sponsors of *PIPEDA*.

The Justice officials identified above were policy entrepreneurs in what privacy advocates would regard as the best sense of that term.[21] They were also part of a specialized international movement in advanced industrial societies that, for example, produced the highly-influential Organization for Economic Cooperation and Development's Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980).[22] Today's policy entrepreneurs are much more likely trying to impress their political masters by shaping policies that are highly-invasive of the privacy of individuals in the process of trying to promote national security and combat terrorism. In the aftermath of 9/11, achieving a balance of such competing interests is an almost impossible challenge for politicians, not least because there are real terrorists doing more than lurking in the weeds; privacy commissioners in Europe, Australasia, and Canada can do little more than "worry aloud" as such trump cards are waved in their faces. As I wrote elsewhere a decade ago, "the striking of balance within government is so much against the privacy interests of individuals that it is a wonder we have any privacy left once governments get through doing what is good for each and every one of us. What is good for government is always thought by those in government to be good for the public at large."[23] Governments may make all of the appropriate noises about sensitivity to privacy, but, as in the European Union, the real decisions, negotiations, and fine rule settings take place in legislative and political arenas, as illustrated by the decision to allow U.S. access to passenger air traffic data.[24]

---

[19] Flaherty, Protecting Privacy in Surveillance Societies, passim, and Simon Nora and Alain Minc, The Computerization of Society: A Report to the President of France (Cambridge, MA., MIT Press, 1980). The report originally appeared in France in 1978.

[20] The text of the Directive is available in Stephanie Perrin, Heather H. Black, David H. Flaherty, and T. Murray Rankin, eds., The Personal Information Protection and Electronic Documents Act: An Annotated Guide (Irwin Law, Toronto, 2001), Appendix 3, pp. 227-60.

[21] See the exploration of the roles of "privacy policy communities" in Bennett and Raab, The Governance of Privacy, pp. 217-21.

[22] http://www.oecd.org/document/18/0,3343,en_2649_201185_1815186_1_1_1_1,00.html .

[23] David H. Flaherty, "Controlling Surveillance: Can Privacy Protection Be Made Effective?" in Philip E. Agre and Marc Rotenberg, eds., Technology and Privacy: The New Lanscape (MIT Press, Cambridge, MA, 1997), p. 173.

[24] See information about the Passenger Protect Program of Transport Canada at http://www.tc.gc.ca/vigilance/sep/passenger_protect/menu.htm. The site usefully contains answers to 25 questions posed by the OPC, including the "Specified Persons List" (no fly list).

Creating the office of the Privacy Commissioner in 1982 as an independent Officer of Parliament with oversight authority was a major, innovative change. The powers were, and remain, those of an Ombudsman, that is, the incumbent can only give advice and issue recommendations but cannot make binding orders. Subsequent enactments of comparable laws in the larger provinces, starting with Quebec and then Ontario, B.C., and Alberta, have usually equipped the "Privacy Commissioner" with order-making power, at least in certain circumstances and for certain issues. Manitoba now appears to be following this model. As further discussed below, such empowerment should be legislated at the federal level as well, especially given the track record of these provincial commissioners in wielding such order-making power responsibly and intelligently and achieving positive results.[25] It is arguable that the optics of having regulatory authority is more important than the reality, since complaints about public sector violations of privacy in the provinces are usually dealt with by issuing reports containing non-binding recommendations.

As previously stated, the *Privacy Act* of 1982 was a piece of timely and progressive legislation.[26] But it is now a law that has been in force for twenty-five years of momentous changes in the automation of information and electronic data and the spread of the Internet and the World Wide Web. While it is not unusual for seminal pieces of legislation to remain unrevised even in the face of urgent necessity for improvement, the *Privacy Act* is especially weak in light of contemporary Canadian needs for robust data protection and security in the face of myriad challenges from hostile forces to the vanquished and diminishing valuation of individual privacy.[27]

There have been efforts at reform. From 1984 to 1987, the House of Commons Standing Committee on Justice and Solicitor General reviewed the functioning of the *Access to Information Act* and the *Privacy Act*. With T. Murray Rankin, Q.C., then on the Faculty of Law at the University of Victoria, the present writer was a specialist consultant to this committee that led to its 1987 report: Open and Shut: Enhancing the Right to Know and the Right to Privacy.[28] This exhaustive study "led the Committee to conclude that both Acts have shown major shortcoming and weaknesses. In some cases, the current legislative scheme is inadequate; in others, there are issues not addressed at all by the Acts." From a privacy perspective, the report recommended controls on the collection of the Social Insurance Number and on computer matching. It also wanted civil remedies in damages and criminal penalties for breaches of the *Privacy Act* and a new provision mandating security of personal information. It is almost quaint to be

[25] On the limits of such authority, see Flaherty, "Controlling Surveillance," in Agre and Rotenberg, eds., Technology and Privacy, pp. 174-76.

[26] While I am fond of suggesting to my political scientist friend, Colin Bennett, that he leave the history to me, his account of the multiple influences on the development of the *Privacy Act* is both sound history and very informative, especially of the international influences on this Canadian development. See Colin J. Bennett, "The formation of a Canadian privacy policy: the art and craft of lesson-drawing," Canadian Public Administration 33 (1990), 551-570.

[27] Of course, much about the age of ubiquitous computing serves our individual and collective interests as a matter of personal choice and collective acceptance.

[28] The present Minister of Justice, Rob Nicholson, was the Vice-Chair of this Committee.

reminded of some of the "emerging" privacy issues in the mid-1980s that concerned the Committee, including electronic surveillance in the workplace, urinalysis for drug testing, the use of the polygraph, and the oversight of the use of "microcomputers." Other recommendations for extension of privacy obligations to the federally-regulated private sector and to regulate transborder data flows were timely then and now.

The short history of the Mulroney government's response to Open and Shut was to do nothing in practice about revising the legislation, leaving many of the major inadequacies in the *Privacy Act* to remain to the present day. And, of course, many more weaknesses have emerged over time, as the pages below will discuss. In Open and Shut: the Steps Ahead, the government noted that the "Committee's report and other studies undertaken by the government have demonstrated that information law and government policy must respond to changing circumstances and rapidly developing new technologies. The government is committed to undertaking administrative improvements and legislative amendments to ensure that the Privacy Act is effective in meeting these new challenges for the protection of personal information." The lack of governmental follow-up had the effect of basing any potential reform primarily on administrative policy initiatives rather than on statutory changes. The Treasury Board Secretariat did develop new policies related to limiting uses of the Social Insurance Number, data matching, information management, communications, and security. However, many years later, it was still compensating for the lack of legislative reform with such initiatives as the Privacy Impact Assessment policy.[29]

One of the unappreciated legacies of the second Pierre Trudeau regime to Brian Mulroney was the *Access to Information Act*.[30] That may help to explain Mulroney's unwillingness to do anything for privacy. Even today, hostility to reform of the *Privacy Act* may be based on even greater hostility to the *Access to Information Act*. Bruce Phillips, Privacy Commissioner of Canada from 1991-2000, believes that the government of the day and public servants cannot think of one without the other.[31] The *Privacy Act* was seen as the corollary to the *Access to Information Act,* whereas the two are relatively

---

[29] I owe this point to Ross Hodgins of Health Canada.

[30] "By the time the federal government finally introduced the current Access law, it was well behind the curve for Western democracies… Even so, in the backrooms of Parliament Hill, whisperers claimed that passage of the Access Act had little to do with pulling Canadian democracy up by its bootstraps and even less to do with transparency. Instead, Ottawa insiders contended that the notoriously private Prime Minister Trudeau had finally put the Access Act into force only to undermine his Progressive Conservative successor. Trudeau's "gift" to Brian Mulroney threatened to rend government secrecy from its age-old moorings." David Berlin, "A Love Affair with Secrecy," at http://www.walrusmagazine.ca/articles/2004.11-politics-canada-access-to-information-act/2/

[31] See Justice La Forest's dissent in *Dagg v. Finance* where, with the approval of the majority, he stated (para. 45): "Recognizing the conflicting nature of governmental disclosure and individual privacy, Parliament attempted to mediate this discord by weaving the *Access to Information Act* and the *Privacy Act* into a seamless code. In my opinion, it has done so successfully and elegantly. While the two statutes do not efface the contradiction between the competing interests -- no legislation possibly could -- they do set out a coherent and principled mechanism for determining which value should be paramount in a given case." Justice La Forest subsequently described the *Access to Information Act* and the *Privacy Act* as "parallel statutes." Gérard V. La Forest, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues, Report of the Special Advisor to the Minister of Justice* (November 15, 2005), paragraph 47, available at http://www.justice.gc.ca/en/pl/toc.html.

separate spheres of activity and governance. The first regulates the collection, use, and disclosure of personal information; the second controls the public's access to general information. It would certainly appear that open, accountable government is a greater threat to government and senior public servants than privacy protection, especially given the evident weakness of the *Privacy Act* in terms of trying to restrict what the public sector can do with personal information in its custody and/or control. But there is a strong, evident need to separate these Siamese twins for purposes of law reform.[32]

This essay seeks to provide advice about modernizing the assessment of the *Privacy Act* found in the *Open and Shut* report by updating the report's analyses in light of the new challenges to privacy governance that have emerged through recent e-government and national security initiatives (among others).[33] An essential point is that while much has changed in terms of massive challenges to the privacy interests of individuals, there remains only a half-hearted commitment to implementation of the *Privacy Act*, because of the false fear that meaningful implementation would hamstring government activities involving the collection, use, disclosure, and retention of personal information for all kinds of purposes. The current *Privacy Act* provides Canadians with only the illusion of data protection. The reality is that the government of the day, and to a lesser extent Parliament, always has the upper hand in shaping or revising legislation impacting on the privacy rights of residents of Canada so as to meet its perception of the public interest. The only recourse is court challenges of the type described above.

The task of official and unofficial privacy advocacy is to articulate the privacy interests that are at stake in situation after situation so that the constitutionally and legislatively-protected privacy rights of individuals are diminished no more than is absolutely essential. This is an almost impossible burden for privacy advocacy in the twenty-first century for reasons explored in various parts of this essay, even if, as is the case with the present writer, one adopts a privacy pragmatist's approach rather than that of a privacy fundamentalist.[34] Fundamentalists might well adopt positions on *Privacy*

---

[32] Justice La Forest made this timely point as follows in 2005: "In the early 1980's, when the *Access to Information Act* and *Privacy Act* were first adopted, access to information and privacy were often thought to be opposite sides of the same "information management" coin. A quarter of a century later, it is apparent that this characterization is inapt. While the functions of the access to information regime have remained fundamentally unchanged, the range of issues and concerns related to privacy has expanded dramatically. In 2005, the Privacy Commissioner must assess and respond to the threats posed by an ever-increasing number of privacy-invasive technologies that did not exist (and could not even have been contemplated) in 1983. And this assessment must now be made not only in relation to privacy threats emanating from government (which was the sole concern of the Commissioner until 2001), but also from those arising out of private sector activity. The range of concerns facing the Privacy Commissioner's office, moreover, is beginning to extend beyond the realm of informational privacy, and now includes such intrusions into private and domestic life as unwanted telephone and email solicitations. So whatever truth there may be to the "same coin" adage (which some would contest), it is likely to become decreasingly relevant in the total landscape of future privacy protection needs." La Forest, *The Offices of the Information and Privacy Commissioners*, p. 41, available at http://www.justice.gc.ca/en/pl/toc.html

[33] In her appearance before the Standing Committee on Access to Information, Privacy and Ethics on April 8, 2008, the Privacy Commissioner of Canada was especially forceful and detailed on the need for "improved oversight of the government's public safety and national security programs."

[34] Despite the excellent work of the B.C. Civil Liberties Association, the B.C. Freedom of Information and Privacy Association, and the Canadian Internet Policy and Public Interest Clinic (CIPPIC) at the University

Act reform that would have the effect of shutting down parts of the Canadian government. A fundamentalist might so limit data sharing among government departments, even for authorized purposes and under controlled conditions, that Canadian residents would be asked repetitively for the same personal information. A constitutional balance is essential between the privacy rights of the citizens and the need for government to perform critical functions.

The history of privacy law reform in Canada further raises the critical issue of the central roles of politicians and public servants in setting agendas and priorities for the country, including on such matters as data protection. As noted above, Francis Fox played a key role in the early 1980s after Perrin Beatty had shown the way forward. Justice Minister Allan Rock and Industry Minister John Manley stepped up to the plate in the mid-1990s and accepted the need for data protection for the private sector on an expeditious basis.[35] These commitments were monumental, one can argue, in giving political direction to the senior mandarins in Ottawa, including Kevin Lynch, the present Clerk of the Privy Council, to invest in the issue, as they wisely did.[36] Since at least two of the last Privacy Commissioners of Canada, Bruce Phillips and Jennifer Stoddart, have produced coherent and inclusive plans for reform of the *Privacy Act*, it is now up to the government of the day, especially the Minister of Justice, to make this activity a very high priority.[37]

Current Argument for Reform of the Privacy Act

The Office of the Privacy Commissioner (OPC) has been advocating for a number of years the pressing need to review and update the *Privacy Act*. New challenges to privacy have emerged, notably with regard to potentially privacy-invasive communications and data processing technologies. The functioning of government has been profoundly transformed through e-government and integrative service delivery structures that span organizational boundaries and jurisdictions (e.g. Service Canada, etc.).[38] The economic and political environments—in Canada and abroad—have also changed dramatically since the days when the *Privacy Act* first came into force. Governments worldwide have adopted measures to protect national security, many of which undermine privacy rights. And with the increasingly global economy, more personal data are traveling across borders than ever before, with little or no Canadian

---

of Ottawa, privacy advocacy is underdeveloped in this country compared to the extraordinary work of such bodies in the U.S. as the Electronic Privacy Information Centre, the Centre for Democracy and Technology, etc. Links to all of them, and more, exist at http://www.oipcbc.org/links.htm.

[35] See Colin J. Bennett, "Adequate Data Protection by the Year 2000: The Prospects for Privacy in Canada," International Review of Law Computers & Technology, XI (1997), 82.

[36] See the "Introduction" to Perrin, Black, Flaherty, and Rankin, eds., The Personal Information Protection and Electronic Documents Act: An Annotated Guide, pp. xi-xiv.

[37] While it is reported that the Department of Justice (including its then Minister) was hostile to the enactment of *PIPEDA* on constitutional grounds because of its reliance on the trade and commerce power as the basis to regulate, there are no such bases for constitutional and legal debates in the context of the *Privacy Act*. The federal government has clear authority to act.

[38] See http://www.servicecanada.gc.ca/en/home.shtml .There is no evident mention of protection of personal information on this web site.

framework protecting that data. The OPC's annual reports to Parliament have documented all of these points, and more.[39]

With the adoption of the *Personal Information Protection and Electronic Documents Act*, the federal government currently holds the private sector to a higher standard than it imposes on its own operations involving the collection, use, disclosure, and retention of personal information. This is highly problematic, particularly in light of the fact that the Canadian government has gained extraordinary powers over the informational privacy of citizens through a series of legislative measures and changes in the machinery of government, particularly in the name of national security.[40] While such a re-balancing made sense in the immediate (and somewhat hysterical) aftermath of 9/11, all governments have little incentive to restrict their surveillance of the population in the light of multiple bureaucratic imperatives to collect and use more and more personal information to "solve" various problems. In the overall distribution of power in the federal public service, a small cadre of dedicated privacy specialists in the Department of Justice do not have much traction in the face of mighty Departments and crown corporations with massive databases and surveillance plans, each intended, the public is informed, to make Canada a better place. That is one more reason why the Privacy Commissioner of Canada needs order making power.

It is now commonplace in the 21st century for privacy advocates of all stripes, including privacy commissioners, to warn that we are living in **surveillance societies**. From a comparative perspective, the governments of Paul Martin and Stephen Harper have been relatively modest in their surveillance demands compared to the Labour government of Tony Blair in the United Kingdom with its introduction of national identity cards and massive data compilations ostensibly to help those in need, especially children, but resulting in a full-scale surveillance society. Richard Thomas, the Information Commissioner for the United Kingdom, has been especially articulate on this in the aftermath of the annual meeting of Privacy and Data Commissioners in London in November, 2006, which was devoted to an examination of this central theme.[41] Canadians require enhanced legislative protections to help foil a full-scale surveillance society in this country.

A related issue is the extent to which the federal government's *Privacy Act* is no longer comparable to those of provincial and territorial governments. The story is quite simple: for historical reasons of precedence in enactment, each one has improved mightily on the federal law. The latest enactment tends to have the most teeth and the most privacy protective requirements; the 2004 Ontario *Personal Health Information*

---

[39] See http://www.privcom.gc.ca/information/02_05_b_e.asp

[40] See Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act (June, 2006), p. 3, available at http://www.privcom.gc.ca/information/pub/pa_reform_060605_e.asp

[41] The Information Commissioner commissioned an excellent Report on the Surveillance Society by the Surveillance Studies Network; the text is available at http://ico.crl.uk.com/files/Surveillance%20society%20full%20report%20final.pdf

Protection Act (PHIPA) is a case in point.[42] The public and private sector Acts in Quebec, British Columbia, and Alberta have also raised the bar in terms of their scope and allowance for order making power.[43] Provincial government bodies in Ontario, Alberta, and British Columbia, for example, have to live in mortal fear of their Information and Privacy Commissioners, since they can order them to act in a certain way or to stop doing something. While the Privacy Commissioner of Canada can give advice, government institutions do not have to listen to her.

In addition, the *Personal Information Protection and Electronic Documents Act* has superseded the *Privacy Act* as the new federal standard in Canada for privacy promotion and protection. The OPC correctly stated in its June, 2006 comprehensive report on reform of the *Privacy Act* that "[t]he *Privacy Act* contains a much attenuated version of the fair information principles, with non-existent or overly-lenient controls on the information management practices of the federal government. The deficiencies in the *Privacy Act* are readily evident when compared to the comprehensive set of fair information principles embodied in *PIPEDA*."[44]

The Office of the Privacy Commissioner of Canada holds the view that the current situation is untenable, and that the *Privacy Act* should be renewed by Parliament, on an urgent basis, to better reflect emerging challenges to privacy and the desire of Canadians to have the federal government better protect personal information in its custody and control and across a much broader field of vision in terms of scope. Such views are irrefutable. There is also need for parity/comparability between the private and public sectors, since Canadians should have relatively uniform privacy rights, whether they are dealing with a bank, Air Miles, their family doctor, Canada Post, or Revenue Canada.

In June 2006, the OPC presented a comprehensive plan for reforming the *Privacy Act* to the House of Commons' Standing Committee on Access to Information, Privacy and Ethics. It contained a number of sound and insightful recommendations on how to improve the Act to provide stronger privacy safeguards.[45] A number of them are also reviewed and reflected in this essay. The OPC successfully encouraged the Standing Committee to conduct a review of the *Privacy Act* in the spring of 2008. The assistance of outside privacy expertise will be essential in this process, because the staff of this Committee, and the Library of Parliament, may not have the time and resources required for such a substantial overhaul. Such drafting work should be left to Justice staff anyway, after the Standing Committee has shown the way forward with specific recommendations.

---

[42] See Halyna Perun, Michael Orr, and Fannie Dimitriadis, Guide to the Ontario Personal Health Information Protection Act (Irwin Law, Toronto, 2005).

[43] It is commonly thought that the Privacy Commissioners and Ombudsmen without order-making power in the provinces and territories would dearly love to have it, since it is too easy for their governments to ignore them.

[44] Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 26.

[45] See Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act.

The Need for Privacy Management for Electronic Government Services

While recognizing its value, the OPC is understandably concerned about privacy issues emanating from the growth of e-government in Canada---both at the federal and provincial levels--- and, in particular, the growth in cross-jurisdictional transfers of personal information for a wide range of government programs. As the OPC has stated, "[n]ew technological initiatives such as government on-line implicate privacy, as the walls that are inherently part of the data structure fade away. If we are to create overarching databases or merge existing databases of personal information, privacy must be built into the design stages of the new technology and systems, as must security."[46] These are essential points because the growth of electronic government services and of cross-jurisdictional transfers of personal information are powerful and desirable imperatives for serving the public and the public good. There is nothing inherently wrong in either practice so long as they happen under controlled conditions and on the basis of valid express or implied consent from individuals. At present, the *Privacy Act* does not contain a meaningful consent standard.

Adopting privacy by design, and as many Privacy Enhancing Technologies (PETs) as possible, are essential best practices for achieving robust data protection in these electronic government services, including ensuring identity management, access controls, data masking, encryption, lock-boxes, and real-time auditing as key components of privacy management for Canadian governments.[47] Such ballyhooed technologies have to be put to protective use as well. Government institutions need to pressure vendors to offer them. The ongoing problem is to persuade the proponents of electronic government initiatives to take privacy and security seriously in the early and ongoing stages of product development and implementation by a proactive approach to privacy advocacy; that is the role of privacy watchdogs at every level, including and illustrating the need for Chief Privacy Officers, with human and financial resources at their disposal, within each government institution.[48]

The use and sharing of personal information across jurisdictions is of particular interest especially as it relates to service delivery. The relevant observation is quite simple. If the various levels of government in Canada have robust privacy laws in place,

---

[46] See Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 3 and pp. 11-13. The OPC also wrote in its Annual Report to Parliament, 2004-2005 that "government on-line may demand interoperable systems that pool personal information and make it available to more users for more purposes. The greater the amount of information, access, and number of users, the greater the vulnerability of the individuals to excessive government or bureaucratic surveillance…. E-government is upon us but the law is a long way behind. If government wants to become 'the most connected to its citizens', it must also be more protective of its citizens." This was Jennifer Stoddart's 2nd annual report to Parliament on the *Privacy Act*.

[47] See Bennett and Raab, The Governance of Privacy, pp. 177-202.

[48] I define "privacy watchdogs" to include Privacy Commissioners and their staff, Chief Privacy Officers appointed to articulate privacy interests inside any public or private sector organization, and traditional privacy advocates, who may be either individuals or members of public interest groups. See also the lists of "privacy interests of individuals in information about themselves" and of "data protection principles and practices for government personal information systems" in Flaherty, Protecting Privacy in Surveillance Societies, pp. 8, 380.

with independent oversight by a regulator, then such data sharing can be controlled by the application of the general and specific principles of each law (each of which is built around ten core privacy principles) and, more importantly, by entering into data sharing agreements among government entities that are essentially binding contracts.[49] Bureaucrats do not like having to negotiate such agreements, because they take time and they allow Privacy Commissioners, privacy advocates, and the media to get some sense of what is going on, or what is planned, and to help set the ground rules for data protection. But that is how governments should work to serve the public interest. The federal government simply believes that it can acquire whatever personal information it requires to do its job from other governments and related entities, especially those among the latter that it helps to fund. Data sharing agreements provide clear understanding, rules, accountability, and transparency for privacy protection.[50]

If all relevant privacy laws and related implementation are in fact robust, then one protected enclave can exchange personal information with another protected enclave, under controlled conditions, for legitimate and authorized governmental purposes. Members of the public can then take some satisfaction that Parliament, legislatures, and the privacy watchdogs have a good idea of what is taking place in terms of data exchanges for service delivery (and in the private sector) on the basis of data sharing agreements . Privacy protection is not the enemy, but the friend, of efficient service delivery across all levels of government. Making all of this consensual in nature is but among the many "solutions" that are readily available to sensitive and sensible governments, even in the context of an enhanced security climate. If Canadians want specific services, they will make the pragmatic decision to consent to the collection, use, disclosure, and retention of personal information for such purposes. This is only one of many ways in which privacy can be a manageable issue. Reform of the *Privacy Act* reflects the need for due diligence and sound information management for federal institutions. They should "say what they do, and then do what they say," which is easier said then done.

The Need for Privacy Management for Transborder Data Flows

The *Open and Shut* report of 1987 identified the need to provide an effective framework for transborder data flows. Incredible developments in this area associated with the Internet, the World Wide Web, and outsourcing drive the need for further urgent examination, particularly as they pertain to increased personal data exchanges between Canada and the United States for the purposes of national security, public safety programs, and any other public or private sector purposes. As the OPC has already stated about one aspect of these exchanges, "the Act should contain specific wording to define the responsibilities of those who transfer personal information outside the federal public

[49] One of the many problems with the *Privacy Act* is that it is difficult to track these privacy principles from the CSA Code and *PIPEDA* throughout its text. This leads to the suggestion for a more principled approach than currently exists in a revised *Privacy Act.*

[50] In a report in early May, 2008, the Auditor General of Canada criticized the Public Health Agency of Canada for its lack of data sharing agreements with the provinces for purposes of public health surveillance. See http://www.oag-bvg.gc.ca/internet/English/aud_ch_oag_200805_05_e_30701.html#hd5n

sector into other jurisdictions and to address the issue of adequacy of protection in those jurisdictions."[51] The OPC's 2005-2006 audit of the personal information management practices of the Canada Border Services Agency (CBSA) is exactly the kind of audit that the Privacy Commissioner of Canada should be doing in this regard.[52] Although the audit report contains a detailed description and analysis of how the CBSA should manage its data exchanges with the United States, neither the OPC nor the CBSA actually know how the Americans use such information.[53] This is unacceptable; the CBSA has an obligation to obtain relevant information from the United States in advance of such disclosures. In addition, the Privacy Commissioner herself stated on April 8, 2008: "Overall, the OPC concluded that the CBSA requires a comprehensive privacy-management framework to guide improvements to privacy related policies, systems, procedures and practices, including strengthening the monitoring of the day-to-day information handling practices."[54] This is not happening fast enough.

Data flows with other national jurisdictions must also be similarly managed for purposes of data protection in the public and private sectors. As the OPC has already stated, "most data protection statutes prohibit the disclosure of government-held information to a foreign state, except in very specific circumstances. This should be the standard for Canada and the *Privacy Act* should spell out the requirements to be included in any agreement, as well as accountability and reporting requirements concerning those agreements."[55] In addition, as the OPC has also eloquently stated, "[i]t is completely contrary to the intent of the *Privacy Act* that a government institution could disclose information to another institution or level of government without being obliged to thoroughly examine why the information is required, how it will be used, on what authority the request is made, and whether there are adequate safeguards to protect the information…. It would be appropriate to have specific wording in the *Privacy Act* that addresses the requirements to be included in any agreement under which personal information is to be transferred to a foreign jurisdiction."[56] This language should be included in a redraft of the Act.

---

[51] See Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, pp. 3-4 and 14-16. The Privacy Commissioner returned to the same issues of regulating transborder data flows in her appearance before the Standing Committee on Access to Information, Privacy and Ethics on April 8, 2008.

[52] See http://www.privcom.gc.ca/information/pub/ar-vr/cbsa_060620_e.asp. The writer was a member of the external Audit Advisory Committee for this audit.

[53] "… the Privacy Commissioner does not have jurisdiction outside Canada. Therefore, we did not audit the control and use of personal information once it had crossed the Canada-U.S. border into the United States." http://www.privcom.gc.ca/information/pub/ar-vr/cbsa_060620_e.asp#006, 2.28. See also Treasury Board Secretariat, "Privacy Matters: The Federal Strategy to Address Concerns about the USA Patriot Act and Transborder Data Flows," at http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/pm-prp/pm-prp_e.asp

[54] Jennifer Stoddart before the House Standing Committee on Access to Information, Privacy and Ethics, April 8, 2008.

[55] See Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 4.

[56] See Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, pp. 14-15.

One can also readily agree with the OPC conclusion that "Canadians are entitled to know the extent to which their personal information is transferred across borders into the hands of a foreign government."[57] This is nowhere more important than in Canada's relationship with the United States with respect to cross-border information sharing. The current situation may well strike a layperson as completely out of Canadian control; that should not be, and need not be, the case. But, again, some expert guidance is available and transferable, as in the document from the Treasury Board Secretariat on "Taking Privacy into Account before Making Contracting Decisions."[58] This wise advice is specifically directed to the approximately 250 federal departments, foundations, agencies of government, and crown corporations that are subject to the *Privacy Act*.[59] But unless each of them has someone actually minding their privacy shop and acting as a privacy conscience and as a source of privacy expertise for the organization, they will not even know that such guidance exists.

The Need for Privacy Management for Outsourcing and Public Private Partnerships

The OPC's proposals for reforming the *Privacy Act* contained several recommendations and proposals for addressing the protection of personal information from unauthorized uses and disclosures (or the risks thereof) that could result from outsourcing and public-private partnerships. The OPC briefly mentioned provincial models for managing such outsourcing (namely B.C.), which seek to ensure that the personal information of citizens is effectively protected when service arrangements involve outsourcing to private sector entities.[60]

The B.C. Ministry of Health's outsourcing of the delivery of the administrative and technical components of the province's Medical Services Plan and the Pharmacare Plan to MAXIMUS Inc., a U.S. company, has been one of the most controversial of such outsourcing initiatives in Canada, producing a brouhaha about the reach of the *USA Patriot Act* in particular and a complex set of amendments to the B.C. *Freedom of Information and Protection of Privacy Act*.[61] While it is helpful to have rules, these were so excessive in the circumstances that 2006 amendments were required to allow B.C. public servants to use their Blackberries and laptops when traveling in the United

[57] See Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 15.

[58] See http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/gd-do_e.asp. In 2004–2005, Treasury Board Secretariat engaged all of the Deputy Ministers for all departments and agencies to do a complete analysis of their outsourcing activities, inter alia, to ascertain the level of organizational risk vis-à-vis the flow of data to the US and the application of the *USA Patriot Act*. That review led to this document, which is said to be well known within the federal public service.

[59] Testimony of Jennifer Stoddart before the House Standing Committee on Access to Information, Privacy and Ethics, April 8, 2008. The substantial increase in coverage (from 170) was a consequence of the *Federal Accountability Act* (December, 2006).

[60] See http://www.mser.gov.bc.ca/privacyaccess/main/Contracting.htm

[61] See the Patriot Act resources available on the web site of the B.C. Information and Privacy Commissioner at http://www.oipcbc.org/sector_public/archives/archives.htm

States.[62] The business functions transferred to MAXIMUS BC HEALTH Inc. include assisting and processing enrolment and account changes for beneficiary services, processing all automated and manual medical claims and payments for medical practitioners and providers, supporting automated and manual telephone support services for medical providers and the general public, and supporting the various and complex technology services that enable the business services.

The irony is that this regulatory activity, the oversight of the B.C. Information and Privacy Commissioner, and the complex and detailed Master Service Agreement between the Ministry and the contractor mean that MAXIMUS BC HEALTH is subject to much more stringent data protection and security requirements in practice than the B.C. Ministry of Health itself, for example, or any of the health authorities in the province. The goal should be similarly robust data protection and security in place for government departments and outsourcers/private partners with independent oversight, such as now exists for MAXIMUS BC HEALTH and for Sun Microsystems of Canada for its electronic health record work in B.C. MAXIMUS has a Chief Privacy Officer, on-line privacy training, almost instant reporting of privacy breaches to the Ministry, automated auditing of staff access to personal information in systems, and careful monitoring of experience by senior management and the Board of Directors.

As the BC Ministry of Health recently stated, "[e]nsuring the privacy and security of personal information is a fundamental element of the contractual relationship with MAXIMUS BC."[63] To this end, the Ministry seeks ongoing assurances, through a rigorous, independent, and external auditing process, that "the significantly enhanced privacy and security arrangements required under existing and new legislation as well as rigorous contract parameters are met consistently and reliably by MAXIMUS BC." The outsourcing has also demonstrably resulted in the delivery of far superior service to the appropriate constituencies, especially the general public, than existed prior to outsourcing. Minister of Health George Abbott stated in July, 2006, that "'British Columbians continue to receive a record-high level of service from the Province's Medical Services Plan and PharmaCare programs through Health Insurance BC. Our government committed to providing British Columbians with MSP and PharmaCare services through Health Insurance BC that were fast, responsive and accurate. …We are seeing consistently high quality results from this program – a major change from the 1990s, when phone services were closed one day a week just to deal with the paperwork backlogs."[64]

The *Privacy Protection Schedule* that the B.C. government imposed on MAXIMUS as a schedule to its contract is an excellent model that is being frequently

---

[62] See (section 33.1).

[63] Request for Proposals, SysTrust, 5970 Control Reliance and Other Ad Hoc audits, B.C. Ministry of Health, No. ON-001481, Feb. 18, 2008.

[64] News release, B.C. Ministry of Health, July 19, 2006. MAXIMUS BC HEALTH operates Health Insurance BC.

emulated across the sectors in B. C. and now in the rest of the country.[65] Sun Microsystems of Canada Ltd., which has won a contract from the B.C. Ministry of Health to build the backbone for the electronic health record in the province, had to agree to similarly strict rules on data protection.[66] A revised *Privacy Act* should mandate such requirements.

British Columbia, as a consequence of the *USA PATRIOT Act* debate, has the leading edge practices and procedures in Canada to protect personal information when governments choose to engage in outsourcing and public-private partnerships. In particular, these provide lessons for enhanced privacy management in the federal public sector, especially since so many such personal information handling activities, or portions thereof, are already outsourced to myriad service providers in ways largely unknown, one suspects, to the Office of the Privacy Commissioner.[67] As the OPC has wisely recommended, the "*Privacy Act* should, at a minimum, also make it clear that, when government work is outsourced, the government institution remains accountable for personal information and that the information is considered to be under the control of the institution."[68] This recommendation is a very good illustration of how easy it is to prescribe for what is required to make outsourcing a positive benefit for all parties; the process does not require the development of ruses worthy of medieval theologians. One of the key privacy defences for MAXIMUS BC Health, for example, is that while it has "custody" of sensitive personal information, "control" remains very much with the BC Ministry of Health. This should always be the case in such outsourcing relationship and public-private partnerships. Government institutions always have to retain control of personal information collected, used, disclosed, or retained for their purposes; they also have to take steps that service providers and outsources are acting in compliance with the *Privacy Act*.

The Need for Chief Privacy Officers, Privacy Impact Assessments, and Independent Oversight as Privacy Management Tools in an Enhanced Privacy Act

Outside of the minimal accountability and reporting requirements set out for government institutions under the *Privacy Act*, the Treasury Board of Canada has established much of the accountability regime for personal information management in the federal government by issuing policy and administrative procedures.[69] But this Secretariat has not done much else, over time, to ensure the implementation of the

---

[65] See the schedule at http://www.mser.gov.bc.ca/privacyaccess/?

[66] The present writer has been a privacy advisor to both MAXIMUS BC HEALTH and Sun Microsystems during their contract negotiations.

[67] I make this observation, without prejudice, based on my own experience as a consultant and as an advisor to the Privacy Commissioner of Canada. I am also well aware of the virtue of not blowing the whistle on some of my clients, whom I am elsewhere encouraging to do well.

[68] See Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 4.

[69] Its web site lists about 20 policies and procedures at:
http://www.tbs-sct.gc.ca/pubs_pol/gospubs/tbm_128/siglist_e.asp

Privacy Act across the federal government.[70] As I wrote in 1989, "[t]here is no continuing activist mentality on the implementation of data protection at the Treasury Board, especially outside the specialists in the Administrative Policy Branch. Neither the president of the Treasury Board nor the secretary had, or indeed have, any particular interest in conflicts with their political and public service colleagues about the protection of privacy…. The Treasury Board is not doing much more than it must under the Privacy Act, and it depends on the privacy commissioner to make the law effective."[71]

Although the Open and Shut report gave higher priority to compliance activity at the Board, the results were short lived. In 1994 the Board did issue a helpful policy on "Privacy and Data Protection," which appears to have been largely ignored in practice.[72] Another positive exception was a burst of energy to guide and encourage the preparation of Privacy Impact Assessments at the turn of the century.[73] The web site of the Treasury Board states that the "President of the Treasury Board is the Minister responsible for government-wide administration of the legislation," but that has not resulted in meaningful activities for privacy protection beyond the most basic.[74] The more relevant statement is that "Ministers and Heads of Agencies are responsible for ensuring that their organizations comply with Access to Information and Privacy legislation." Again, this is nothing more than a pious platitude. In practice, it means that no one is minding the privacy shop for the government of Canada at government institutions.

It is time for the Chief Information Officer of Canada (in the absence of a Chief Privacy Officer) to step up to the plate on behalf of the Treasury Board even under the current structure. The CIO and the Treasury Board should not be allowed to take shelter behind the notion that it is up to the OPC, and individual departments, to be alone responsible for making the *Privacy Act* meaningful in practice, even in its current "privacy light" version.[75] In particular, the CIO can ensure an ongoing marriage between

---

[70] See Flaherty, Protecting Privacy in Surveillance Societies, pp. 267-69. I note in passing that the Information and Privacy Commissioner for B.C. does not even include the Treasury Board of Canada among the almost forty sites that it links to its own web site: www.oipcbc.org.

[71] Ibid., pp. 268-69.

[72] http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/CHAP1_1-2_e.asp#policy. The OPC itself noted in 2006 that "[a]lthough there has been a Treasury Board Secretariat policy on data matching since 1989, many program managers asked about it in 2004 had never heard of it." Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 5.

[73] http://www.tbs-sct.gc.ca/pgol-pged/piatp-pfefvp/index_e.asp. The Information, Privacy and Security Policy Division of the Chief Information Officer of Canada continues to do some privacy training on basic topics.

[74] http://www.tbs-sct.gc.ca/atip-aiprp/index_e.asp

[75] The following statement by the OPC in June, 2006 is highly pertinent here: "We suggest that Treasury Board Secretariat (TBS), as the locus for privacy policy implementation in the federal government, assume a leadership role in the development of a privacy management framework. But it cannot effectively do so in the absence of a legal framework and resources. For TBS to effectively carry out this role, it needs the gravitas, both push and pull, of a modernized *Privacy Act*, which is the responsibility of the Department of Justice. While the TBS is to be congratulated on the excellent work it has recently done with respect to providing better guidance on outsourcing of government activities involving personal information, as explained more fully below, the *Privacy Act*, through its numerous shortcomings and deficiencies, falls short of providing authority or parameters for the development of this framework. As much as the work of

privacy and security specialists in mutual support of these intimately-related goals. A CPO would be of great benefit in this process. Privacy-intensive government institutions, such as Public Safety Canada, Transport Canada, and Service Canada, do not have Chief Privacy Officers in place.

The Treasury Board Secretariat does maintain a list of "privacy and access coordinators" for government institutions.[76] It would appear that more than 200 persons hold such a title in entities that range from being huge (Health Canada) to small (a local port authority). The task of a privacy and access coordinator is primarily to process requests for access to information under either the *Privacy Act* or the *Access to Information Act*.[77] That is at least what the positions have become over time, with a few exceptions such as Health Canada, which has a more coherent approach to privacy management. (See appendix 1 below) A senior coordinator wrote that "at this point in the history of our legislation, the title of ATIP Coordinator often conjures up only the image of those who retrieve documents and process access to information and privacy requests. Most Coordinators are primarily in the request processing business. It is a circumstance that occurs by default because of capacity. If there are limited resources and there is a choice of responding to requests or developing policies and guidelines, the former always wins out."[78] The coordinator role is almost always at a fairly junior level in the bureaucratic hierarchy; incumbents rarely have the clout to make a significant difference in their agency. In fact, even a Chief Privacy Officer would have problems making his or her own voice heard in such hierarchical power structures.

A critically-important improvement would be to amend the *Privacy Act* to require the appointment of Chief Privacy Officers (CPO) for the government of Canada and in each government institution, or at least in those that are privacy intensive (collecting, using, disclosing, and retaining a great deal of personal information on members of the public and employees). What is being recommended here is much more policy oriented than the current work of an Access to Information and Privacy Coordinator. A CPO should certainly raise the profile of privacy within any government institution and provide a focal point for the solution of ongoing privacy issues in a pragmatic manner.[79] Of course, they will require a very senior reporting relationship, appropriate human and financial resources to do the job, a Privacy Team/advisory group, general and specific privacy policies and related procedures and processes, the conduct of Privacy Impact Assessments for significant data bases, on-line privacy training for all staff, robust

---

TBS is to be complimented, it is essentially based on policy and, consequently, left to the vagaries of administrative procedures and the will of the Executive. Canadians deserve better, and so do elected officials that represent them." Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, pp. 10-11.

[76] See http://www.tbs-sct.gc.ca/atip-aiprp/apps/coords/index_e.asp

[77] While processing access and privacy requests is an important and complex activity, it requires a different type and level of skills than is required to be the privacy watchdog/centre of privacy expertise for a large and diffuse federal department or agency.

[78] Ross Hodgins, Director, Access to Information and Privacy division, Health Canada, to David H. Flaherty, March 18, 2008.

[79] I have never known a Chief Privacy Officer and his or her team to run out of work, since issues of privacy and security are everywhere in data-intensive organizations in both the public and private sectors. In effective practice, their roles and responsibilities grow exponentially.

security practices, meaningful confidentiality agreements, Frequently Asked Questions, auditing, and a full range of security controls from identity management to role-based access.[80] In a number of these instances, the CPO can breathe life into policy work that the Treasury Board has already done, which now requires meaningful implementation.

Emerging experience in North America in the public and private sectors suggests that the CPO model can be the focal point in an organization for achieving systematic solutions to privacy issues.[81] The Conference Board of Canada, for example, has a Council of Chief Privacy Officers.[82] The U.S. Department of Commerce, the Department of Homeland Security, and the Internal Revenue Service have appointed CPOs. Major tech firms like IBM, Microsoft, Sun Microsystems, Oracle, and Hewlett-Packard have had CPOs for years. The Canadian Millenium Scholarship Foundation, a federal entity, has a CPO as well.[83] The Ontario government has a Chief Information and Privacy Officer.[84] The preferred approach would be to separate such positions because of the enormous responsibilities of both (comparable to the successful argument that Canada should continue to have a Privacy Commissioner and an Information Commissioner).[85]

Although Health Canada decided not to officially appoint an Assistant Deputy Minister as the CPO for the agency, because of the lack of a precedent in federal institutions, it is worthwhile outlining what it has done (and what it wanted to do) to better manage privacy in recent years, because Health Canada has become a federal model in this regard. The Assistant Deputy Minister, Corporate Services Branch (CSB), was to be the Chief Privacy Officer (CPO) for the Department and, even though he does not have the title of CPO, he is accountable to the Deputy Minister for championing privacy initiatives internally and externally. This concept of a privacy champion in every government institution is very important for advancing a culture of sensitivity to privacy. In addition, the Health Portfolio Privacy Committee provides a senior level review of privacy issues and is a key mechanism for ensuring a horizontal and collaborative approach to integrate privacy policies and practices across the business lines of health portfolio institutions. The Committee reports to the Departmental Executive Committee through the ADM. The network of privacy contacts provides advice and support to the Health Portfolio Privacy Committee with regard to operational implications related to

---

[80] See Guidelines for Managing Privacy, Data Protection and Security for Ontario Hospitals (A Report prepared by the Ontario Hospital eHealth Council's Privacy and Security Working Group – July 2003). www.oha.com. See also Bennett and Raab, The Governance of Privacy, pp. 260-62; and the U.K. Information Commissioner's Privacy Impact Assessment Handbook (2007), at http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html

[81] See "The Rise of the Chief Privacy Officer," Business Week, Dec. 14, 2000, at http://www.businessweek.com/careers/content/dec2000/ca20001214_253.htm;

[82] http://www.conferenceboard.ca/CPO/ Member organizations include the Canadian banks, Bell Canada and Telus, Canada Post, and IBM Canada.

[83] http://www.millenniumscholarships.ca/en/privacy/index.asp

[84] See http://www.accessandprivacy.gov.on.ca/english/index.html

[85] The conclusion of Justice La Forest, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues, Report of the Special Advisor to the Minister of Justice*, available at http://www.justice.gc.ca/en/pl/toc.html

privacy.[86]

Health Canada thus has developed a solid capacity for privacy policy work. (See appendix 1) Its Access to Information and Privacy Division (staff of 44) has both a Policy Unit (14 officers) and an Operational Unit (30 analysts). Organizationally, it allows for mobility between the units, particularly at the more junior levels. Both policy and operational personnel operate on a portfolio basis in that they are responsible for assisting and providing advice to specific program and service areas within the Department. One of the main advantages of having a policy unit is that Health Canada can maintain an active privacy training and awareness program in a very large and decentralized Department. The Privacy Commissioner of Canada recently advocated that all federal managers and executives should have privacy information management training, just as they are now required to have financial and human resource management training.[87]

The concept of Chief Privacy Officers, with staff and financial resources, in place across all governmental and private sector concerns in this country is an idea whose time has truly come. The Government of Canada should emulate Ontario and appoint a Chief Privacy Officer to serve as the government's focal point for privacy advice across the entire government; each privacy-intensive federal entity should have similar officials in place for the same purposes. Such officials would be vital counterparts to the existing Chief Information Officers and Chief Security Officers, who are also crucial contributors to the data protection imperative.

Reform of the *Privacy Act* itself, however desirable, is not a magic bullet or a panacea that will cure all privacy ills in the federal domain. It can only be one component of enhanced privacy management for federal institutions, crown corporations, and other federal entities, such as the Canadian Blood Services, that are largely funded by the federal government and that now escape statutory regulation.[88] On-line privacy training on a repeat basis for anyone who works with personal information is absolutely essential for enhancing compliance.[89] The government itself must make its departments do their privacy jobs with commitment and resolution on an ongoing basis.

---

[86] I am grateful to Ross Hodgins of Health Canada for providing me with the information in these paragraphs about the scope of privacy management at Health Canada.

[87] Testimony of Jennifer Stoddart before the House Standing Committee on Access to Information, Privacy and Ethics, April 8, 2008.

[88] See the informative discussion of a "privacy management framework" in the OPC's Annual Report to Parliament, 2004-2005 at http://www.privcom.gc.ca/information/ar/200405/200405_pa_e.asp#018

[89] The OPC made this highly-relevant comment on training in June, 2006: There is a need to "foster a process of continuous learning in privacy management across the federal government through the incorporation of personal information management skills development in public sector professions that handle highly sensitive information: human resources, the legal community, financial management --grants and contributions and other types of funds transfer, payment management, etc. In other words, the *Privacy Act* should provide a set of normative principles that would guide the design of a core curriculum for ATIP managers and staff, PIA specialists, etc. The *Privacy Act*, as it stands, is completely devoid of such a framework." Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 10.

The OPC has argued that the accountability requirements, namely for privacy impact assessments and controls on data matching, should be mandated in the *Privacy Act* to ensure that federal departments and agencies adhere to them rigorously.[90] That makes excellent sense. An argument can be made that full-scale PIAs should only be statutorily mandated for the most intrusive and sensitive personal information systems.[91]

In addition, the standards that have emerged for contemporary accountability regimes for personal information management in Canada and in other English-speaking countries mean that federal departments and agencies should be assuming and ensuring greater openness, accountability, and transparency for privacy management, and the *Privacy Act should* mandate such an approach. It is in the best interests of federal departments and agencies, especially those that are privacy intensive, i.e. holding large amount of personal information, to adopt sound management techniques for privacy risk management. The components of robust privacy and security management are now well known.[92] A revised *Privacy Act* should mandate as many of them as possible in a privacy management framework.

The Need for Order-Making Power for the Privacy Commissioner of Canada

The Privacy Commissioner of Canada needs more power in order to get the attention of the government and government institutions on an ongoing basis. As the OPC itself stated in 2006, "[t]he Privacy Commissioner is an ombudsman, with no order-making powers. The ability to truly fulfill the ombuds-role has frequently been frustrated by limitations in the Privacy Act. The question of order-making power will need to be carefully examined in the context of the Privacy Act reform. The Act should specifically

---

[90] The OPC's Annual Report to Parliament for 2004-2005 noted that "[a]lthough government use of data matching (or "computer-matching") arguably poses the greatest threat to individuals' privacy, the *Privacy Act* is silent on the practice. Privacy Commissioners (bolstered by Parliamentary Committees) have all recognized the dangers inherent in excessive and unrelated data collection. All have recommended amending the *Privacy Act* to ensure that government institutions link personal records in discrete systems only when demonstrably necessary, and under the continued vigilant oversight of the Privacy Commissioner of Canada. The recommendations have not been followed through." In June, 2006, the OPC added that "…there is still a place to set out in legislation a framework identifying the principles governing data- matching and the responsibilities of the parties involved. The legislation should include basic elements, such as definitions, a requirement for advance notification to OPC, and powers of the Commissioner to stop the proposed data matching from taking place if it is not up to standards." Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 31.

[91] For access to comparative research on PIAs and their useful application, see the web site of the UK Information Commissioner at http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/privacy_impact_assessment_international_study.011007.pdf. See also the U.K. Information Commissioner's Privacy Impact Assessment Handbook (2007), at http://www.ico.gov.uk/upload/documents/pia_handbook_html/html/1-intro.html.

[92] See the excellent material on "Building a Privacy Management Framework for the Federal Government," in Office of the Privacy Commissioner of Canada, Report to Parliament on the *Privacy Act*, 2004-2005, at http://www.privcom.gc.ca/information/ar/200405/200405_pa_e.asp#018. It notes that Human Resources and Skills Development Canada (HRSDC) presented their privacy management framework to the ADM Privacy Committee in June 2004.

empower the Privacy Commissioner to engage in mediation and conciliation, as is already the case under PIPEDA."[93] Most of this list makes perfect sense. The Commissioner should also have a statutory mandate to educate and inform Canadians about their privacy rights.

In the author's opinion and experience, the case for order-making power for the Privacy Commissioner of Canada, first in the public sector and later in PIPEDA, is a powerful and persuasive one. The Information and Privacy Commissioners in Ontario, B.C., and Alberta are as successful as they are because they are true regulators, even though they rarely exercise actual order-making power on the privacy side of their mandate.[94] It is the prospect of their doing so that makes all parts of government pay attention to them. The supposedly-superior merits of the ombudsman approach are the stuff of myth and legend and an unwillingness to learn from Canadian experience outside of Ottawa and the federal realm. It is time to break free of this paradigm. Politicians and public servants will pay more attention to the advice of the Privacy Commissioner of Canada if she has the ability to use order-making power in appropriate circumstances.[95] Of course, such decisions can be appealed to the courts, as is already the case in provinces with order-making power. Decisions in such appeals will further enhance the jurisprudence of privacy as illustrated by decisions of the Supreme Court of Canada quoted above.

The OPC's June, 2006 report on reform of the Privacy Act discussed the pros and cons of this issue of order-making power in a manner that at least gets away from certain stereotyping that surfaced in such discussions in the past.[96] The OPC called for further study of the issue and posed some relatively academic questions for consideration. It is time for greater boldness and indeed action. The OPC well stated the main current argument against the ombuds-person model, the argument of actual history. It stated: "The recommendations of an ombuds-person must be respected, given due consideration, and acted upon except in exceptional circumstances, else there is no ability to achieve balance, assist citizens and resolve issues. Governmental disregard of objections and concerns raised by the OPC puts the fundamental informational privacy rights of all Canadians profoundly at risk."[97] That is in fact what has happened over time; the Privacy Commissioner of Canada has become something of a toothless watchdog. At present, it is much too easy for federal departments and agencies to dismiss the Privacy Commissioner as only being able to give advice (which one does not have to take). They

[93] See Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 4. The OPC's Annual Report to Parliament for 2004-2005 noted that "[w]hile the ombudsman model has been an effective one in avoiding an adversarial climate to encourage compliance, appeals to fairness and good sense are only as effective as the compliance they engender."

[94] The Quebec Commission d'accès à l'information more often than not uses its power of order-making in both access and privacy matters (private and public sectors).

[95] See my early discussion of this issue in Flaherty, Protecting Privacy in Surveillance Societies, pp. 394-96.

[96] Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, pp. 19-22.

[97] Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 21.

are not always careful listeners. The only real way for the OPC to get appropriate attention for its views from the government and Parliament is for the OPC to have order-making power. Even then, Parliament can always do what it wants in the exercise of parliamentary supremacy, and the courts can overrule a Privacy Commissioner.

Mid-way through my term as the first Information and Privacy Commissioner for British Columbia in the 1990s, I made this comment about my exercise of order-making power, which I think is still valid: "…I use it mainly to win agreement on my recommendations that are normally arrived at by joint deliberations with authorities that keep my colleagues and myself sensitive to the demands of daily bureaucratic life and the reality of service delivery to the public…. My power on any issue is also effectively limited in our democratic society by the fact that the legislature can in fact do almost anything it wants to invade personal privacy by law or regulation, despite my best advice to the contrary. Only an aroused public can seek to mitigate this Achilles heal of data protection."[98]

There are unfounded fears that giving selective order-making power to the Privacy Commissioner of Canada will require an enhanced bureaucracy and substantially-increased expenditures from the public purse.[99] The evidence from the provinces does not support these fears. Order-making on privacy issues remains the exception rather than the norm, lay persons and lawyers are writing orders on Freedom of Information (FOI) and privacy issues, and staff sizes and budgets for combined FOI and privacy management are less than at the OPC.

Learning to Work With the Privacy Commissioner of Canada

When will federal politicians and public servants learn to inform and consult the Privacy Commissioner of Canada, for example, in advance of their latest scheme that may be highly privacy intrusive and that will likely lead to sensational media treatment, including the fact that the Commissioner had never heard of the system?[100] When will Privacy International, the premiere international privacy lobby group, be able to stop informing national Commissioners of developments that they should have known more than something about in advance, such as the Society for Worldwide Interbank Financial Telecommunication (SWIFT) debate in 2006?[101] SWIFT was disclosing significant amounts of personal information on international bank transfers to the U.S. government

---

[98] 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 (University of Toronto Press, Toronto, 1999), pp. 26-26.

[99] See the discussion during the testimony of David H. Flaherty before the House Committee on Access to Information, Privacy and Ethics, May 8, 2008.

[100] See Jennifer Stoddart's reaction to alleged Canadian participation in the FBI's "Server in the Sky" initiative in Bill Curry, "Law Enforcement/Biometrics: Canada working with FBI on 'server in the sky,'" The Globe and Mail, Saturday, Jan. 19, 2008, p. A6: "…she first learned of the plan this week from a media report from London. No Canadian officials had informed her of the project."

[101] After the New York Times broke the SWIFT story, Privacy International lodged privacy complaints with data protection agencies in thirty-two countries. See the OPC's report of its findings in the SWIFT matter (April 2, 2007) at http://www.privcom.gc.ca/cf-dc/2007/swift_rep_070402_e.asp

in response to legal subpoenas without being open and transparent about the practice. Will it always take a major privacy disaster, such as the loss of CDs with massive amounts of personal information on 25 million persons in the United Kingdom in November 2007, to result in enhanced resourcing and empowerment of these official privacy watchdogs?[102]

One does not have to be very cynical to recognize that the federal government and federal institutions want to do what they want to do, when they want to do it, to meet the perceived political exigencies of the moment and to stay in power. Bennett and Raab observe that "[m]any parts of government wish to ensure that privacy considerations do not unduly constrain their intensive use and sharing of databases…."[103] Watchdogs like Privacy Commissioners can be a major irritant for even well-intentioned Ministers and senior public servants, who may be all too ready, for example, to trample individual rights in the rush to protect national security. Of course, even to write such a sentence may suggest that privacy advocates always want to trump other values. Such is far from the case in Canadian experience going back to the mid-1970s. It is hard to recall a Privacy Commissioner in Canada taking a foolish position or one that did not seek to articulate the privacy interests at stake in a particular situation requiring commentary. Even George Radwanski, whose career as Privacy Commissioner of Canada ended with his resignation on June 23, 2003 for his spending and borrowing habits, took strong and well-informed positions on many of the privacy issues he gave advice on.[104] It is sad but true that governments perceive a weak Privacy Commissioner as a positive good, thus offering only the illusion of data protection.[105] That situation has to change in the interests of the public, not least because of the constitutional protection accorded to the right to privacy in the *Charter*.

The Resourcing of the Privacy Compliance Function at the Office of the Privacy Commissioner and in Government Institutions

Canada could enact the best public-sector privacy law in the world, and it still would not mean much in practice if Parliament does not ensure that resourcing (human and financial) is put in place both for the OPC and for each government institution. Not a single 'Privacy Commissioner' in Canada is properly resourced to perform the full scope of his or her statutory duties. By any kind of civilized and/or comparative standard, the human and financial resources available to them are inadequate.[106] However hard the

---

[102] See the Press Release from the UK Information Commissioner's Office on Dec. 17, 2007, "Information Commissioner welcomes the government's commitment to strengthen the powers of the ICO," at http://www.ico.gov.uk/upload/documents/pressreleases/2007/gov_announcement_171207_final.pdf

[103] Bennett and Raab, The Governance of Privacy, p. 222.

[104] See the discussion of his "activist style" in Colin J. Bennett, "The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas," Canadian Public Administration, 46 (2003), 232-33, 234, 236.

[105] See Flaherty, Protecting Privacy in Surveillance Societies, pp. 158, 389, 391-94

[106] Justice La Forest noted in the fall of 2005, with respect to both the Privacy Commissioner and the Information Commissioner, that "the combined budgets of the two offices for the 2004-2005 fiscal year were $15 million, representing less than 50 cents per Canadian. By way of comparison, the government's total expenditures for 2003-2004 were approximately $141 billion." La Forest, *The Offices of the*

current staff of the OPC work, it is humanly impossible for them to do everything that is required, despite recent staffing increases. The plethora of issues requiring attention is literally overwhelming, in addition to all of the routine tasks requiring attention.[107] The primary work of achieving privacy compliance has to rest with each government institution; the OPC should be monitoring and auditing what they actually do.

Under-resourcing of all Privacy Commissioners across Canada has meant that, with rare exceptions, none of their staff members have really developed ongoing expertise on one kind of major data protection problem or another, such as biometrics, encryption, electronic health records, or almost any security issue.[108] Staff of these offices also have to be more disciplined so as not to chase every rabbit that surfaces in a daily media report of one sort of another that appears to affect the privacy interests of Canadians. If appropriate staff expertise exists, then those persons can manage the issue of the day and leave the rest of the staff to go about their main tasks. Self-discipline to focus on the essential priority components of meaningful and effective data protection has to be the main preoccupation at the OPC and across the country.[109] Giving policy advice, conducting investigations, audits, and site visits, and educating the public are more important than the processing of routing complaints.

More specialized policy resources in the OPC, including additional outsourcing to other competent privacy professionals, including at law firms, will also encourage government departments and crown corporations to consult with it more regularly and frequently to build in the data protection and security controls that are requisite in the design of all information systems containing personal information.[110] Even though there are several hundred thousand persons who are required to comply with the *Privacy Act*, including 217,000 public servants, the OPC cannot hope to be funded for exponential growth in budget or staff. It has 140 staff at present, who will have to work smart, and with considerable focus, to fulfill public expectations.

"Building in privacy by design" is the name of the data protection game, and privacy specialists at the OPC have to work with the relevant bureaucrats to achieve it.[111] Even if the latter have thought carefully about appropriate solutions, it is essential to give

---

Information and Privacy Commissioners: The Merger and Related Issues, Report of the Special Advisor to the Minister of Justice, p. 26.

[107] In addition, I am not aware of any privacy-intensive federal department or crown corporation (with the possible exception of Health Canada) that is properly resourced to implement the current *Privacy Act*, never mind an improved one.

[108] Of course, all of them can rise to the occasion as required on any of these issues. I also think that the track record of the Office of the Ontario Information and Privacy Commissioner is perhaps unrivalled on this set of issues, not least because of the long-time role of Dr. Ann Cavoukian, the current Commissioner.

[109] See Flaherty, Protecting Privacy in Surveillance Societies, "conclusion," and Bennett and Raab, Governance of Privacy, ch. 8.

[110] External research funded by the OPC through its Contributions Program is making a major contribution to understanding of new and emerging privacy and security issues. See http://www.privcom.gc.ca/resource/cp/index_e.asp

[111] See Dr. Ann Cavoukian, Ontario Information and Privacy Commissioner, "Privacy by Design." A Crucial Design Principle, Inaugural Lecture, Identity, Privacy and Security Initiative, University of Toronto, Sept. 17, 2007, at http://www.ipc.on.ca/images/Resources/up-2007_09_17_UofT.pdf

the OPC a high-level overview of what is being contemplated so that no one will be blindsided in the media or in Parliament further along the route of a specific development.[112] Unfortunately, government institutions fear that the Privacy Commissioner will try to "stop" an initiative if they are informed too early in the process. If everyone has to be onside in a government institution before making a timid approach to the privacy watchdog, that is a recipe for a privacy disaster in the making.[113] While the government should get its house in order on a particular issue or approach, consulting with the OPC should be an integral part of the process from almost the beginning so as to reduce the risk of nasty surprises for the government institution. For example, a government institution presenting the OPC with even a competent conceptual Privacy Impact Assessment should be well ahead in achieving privacy risk management.

The Oversight Role of the Standing Committee on Access to Information, Privacy and Ethics

The mere existence of the House of Commons' Standing Committee on Access to Information, Privacy and Ethics should be very important for promoting oversight activities, including the appointment or re-appointment of any Privacy Commissioner of Canada. Members of this Committee, supported by ongoing staff resources, need to develop some privacy expertise of their own to not only promote legal reform, as in the case of revitalizing the *Privacy Act*, but also to ensure that outstanding individuals are appointed to fill these critically-important posts in Canadian society. Of course, members also have a critical mandate to ensure that the Office of the Privacy Commissioner of Canada is doing its job effectively, pragmatically, and creatively.

Privacy advocates should perceive the new Standing Committee as a positive development. There is finally a committee that has the opportunity to pay ongoing attention to privacy matters and to become educated about them. It will soon learn which expert witnesses are both credible and helpful. Jennifer Stoddart has followed up on her

---

[112] "In terms of qualities that go with leadership, I would emphasize the ability to win an argument and to get the intended audience to listen. Many of you will remember the debacle over the HRDC longitudinal labour force file around 2000 when Bruce Philips was the Privacy Commissioner. One of the key results of the discussions that took place then was that senior executives of HRDC realized that while they've been hearing from the Privacy Commissioner of Canada, they hadn't been listening to what he was saying. A good privacy commissioner has to get government departments, as well as the private sector, to listen to his arguments or her arguments and to take them seriously." (Testimony by David H. Flaherty on the appointment of Jennifer Stoddart as Privacy Commissioner of Canada, House of Commons, Standing Committee on Government Operations and Estimates, No. 68, Nov. 4, 2003). Having order-making power for the Privacy Commissioner of Canada will focus this attention span.

[113] "The concept of a privacy watchdog is one that I've promoted over the last 20 years. I've written that the watchdog must have both a bark and a bite. Successful implementation of a data protection regime requires active, energetic leadership and dedicated trained staff. I emphasize that one of the key roles of a privacy commissioner is to articulate the privacy interests that are at stake in any situation as a kind of an alarm system for the society. I've written that the primary role of a data-protection agency is the actual articulation and advancement of the privacy interests that must be defended in a particular setting. The role of the Privacy Commissioner in situation after situation is to surface the privacy issues that need to be debated and discussed." (Testimony by David H. Flaherty on the appointment of Jennifer Stoddart as Privacy Commissioner of Canada, House of Commons, Standing Committee on Government Operations and Estimates, No. 68, Nov. 4, 2003.)

substantial experience in briefing Quebec parliamentarians and government officials on such matters with ongoing appearances before the Standing Committee; this can only be to the good in terms of developing some real privacy expertise.[114]

Each of the "Privacy Commissioners" of Canada dating back to 1978 and the appointment of Inger Hansen has brought his or her own style to the articulation of the job requirements.[115] Based on close observation of such officials in Canada, Western Europe, and Australasia, dating back to the 1970s, the argument of this writer is that they have to adopt a forceful, aggressive, dynamic, committed, yet pragmatic approach to fulfillment of their job requirements.[116] These are not jobs for shrinking violets or the insecure. After listing the seven roles of the Privacy Commissioner, Bennett wisely opined that "[t]his flexible and multiple set of powers and quite expansive mandate would give any observer the impression that the privacy commissioner is a person of considerable power within the federal system. Yet, the exercise of the powers of the office is essentially dependent on the style, character, skill and personality of the commissioner himself or herself and on how that person perceives and is perceived by the wider organizational environment."[117]

The Standing Committee also needs at least several ongoing staff and consultants that can develop a strong background on privacy matters, much more than one can expect from clerks of such committees and their supporting researchers because of their general duties in these circumstances.[118] One remembers fondly the example of the U.S. House Subcommittee on Government Information in the 1970s and 1980s where, for many years, Robert Gellman was a one-man band of privacy expertise for members of the committee. There has never been a Canadian federal equivalent in Parliament over time, and there needs to be. Achieving meaningful and effective data protection requires the development of clear thinking and accompanying expertise on myriad topics. The House Standing Committee needs to play a strong role in pushing for *Privacy Act* reform as a matter of the highest priority and in the best interests of constituents.

Enhancing the Audit Authority and Audit Capacity of the Privacy Commissioner of Canada and of Government Institutions

I was fortunate in the 1980s to learn about the beneficial effects of auditing for privacy compliance in Germany, and since then I have become a bit of a broken record on the topic.[119] As Information and Privacy Commissioner in B.C., I pioneered the idea of site visits as an elemental form of both auditing and consciousness-raising. Experience

---

[114] Stoddart is a former president of the Commission d'accès à l'information du Québec

[115] For comments on the styles of Inger Hansen and John Grace, see Flaherty, Protecting Privacy in Surveillance Societies, pp. 263-64, 272-75.

[116] See Flaherty, Protecting Privacy in Surveillance Societies, pp. 385-91.

[117] Bennett, "The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas," Canadian Public Administration, 46 (2003), 220.

[118] Issues should as whether the Standing Committee or the Research Branch of the Library of Parliament actually hire the researchers, as well as the required budget, need to be resolved. Such committees can have only limited effectiveness without strong staff support.

[119] See Flaherty, Protecting Privacy in Surveillance Societies, pp. 400-401.

as a consultant since 1999 has reinforced my views of the central importance of audits and site visits to promote and achieve compliance. How else can one really find out what is happening in practice? In an ideal world, government institutions will plan or commission ongoing internal and/or external privacy audits and then present the results to the OPC. There is delicious irony in the resources that the B.C. Ministry of Health is devoting to privacy audits of MAXIMUS BC HEALTH, when such audits are not common in the Ministry itself or in B.C.'s health authorities across the province, especially with the envisioned roll-out of electronic health records. The current Privacy Commissioner of Canada is investing significant resources in the auditing process and conducting some very important audits of key personal information systems.[120] She also requires authorization to release the results upon completion of the final audit report.

Reform of the *Privacy Act* should now require that federal departments and agencies use their internal and external auditors to add privacy and security auditing to their routine activities. Even filling out a privacy check list would be a significant eye opener for government institutions that have little idea about the actual state of their data protection compliance with a broad range of statutory requirements, except for the number of requests each year for access to personal information and/or the number of privacy complaints received. Such a checklist can also incorporate best practices to help keep government institutions out of privacy trouble.

The Need for the OPC to Move beyond Complaint Handling

In his report on the proposed merger of the offices of the Information Commissioner and the Privacy Commissioner, Justice Laforest stated that in "keeping with the ombudsman function, the primary duty of both the Information and Privacy Commissioners is to independently and impartially investigate and make recommendations with respect to complaints from persons alleging that a government institution has breached their rights under the *Access to Information Act* or *Privacy Act*."[121]

This simple and accurate description in fact highlights a critical deficiency in the current *Privacy Act*. In the 21st century, as noted above, responding to complaints is only a very small part of what a privacy watchdog needs to do to seek to control bad surveillance, at least compared to the need to give systemic and specific advice, to conduct general and specific investigations, and to carry out audits and site visits.[122] As Bennett and Charles D. Raab have said of the multiple role of the Privacy Commissioner, she is expected at some point to perform seven interrelated roles: ombudsman for citizen complaints, an auditor of organizational practices, a consultant on new and existing information systems, an educator of the public, policy advisor, a negotiator, and an

[120] See the reports of major audits at http://www.privcom.gc.ca/information/02_05_a_e.asp
[121] La Forest, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues, Report of the Special Advisor to the Minister of Justice*, p. 15.
[122] See the discussion in Flaherty, "Controlling Surveillance," in Agre and Rotenberg, eds., Technology and Privacy, pp. 184-87.

enforcer.[123] Bennett and Raab conclude that the more general and proactive powers are the more important ones. Each of these roles requires resourcing, commitment, ongoing leadership, and actual results in the face of multiple demands and competing priorities. Justice La Forest specifically recognized, later in his report, that "[t]he Privacy Commissioner, in contrast [to the Information Commissioner], is more frequently involved in high-level debates about the long-term, systemic, and often transnational effects on privacy of proposed and existing legislation and policy, such as the government's reaction to the threats of organized crime and terrorism and the privacy implications of novel surveillance and information gathering technologies."[124] This is currently, and has to remain, a key focus for the OPC.

Under-resourcing of the Office of the Privacy Commissioner of Canada has meant almost unbelievable, and certainly unacceptable, delays in conducting investigations and responding to privacy complaints from the general public. These delays for complaints are routinely more than a year in practice.[125] The solution is to authorize the OPC to focus only on meaningful complaints and to pay less or no attention to what it deems to be less important, or repetitive complaints; the *Privacy Act* should reflect this right to prioritize, since responding to complaints is only one facet of making data protection meaningful.

In a January 15, 2008 submission to Industry Canada on revision of *PIPEDA*, the Privacy Commissioner asked for discretion in responding to complaints, because of "the lengthy and increasing delays we face in handling complaints while at the same time [we should] be in a position to take a more pro-active approach in addressing more systemic and pervasive issues through research, public education, Commissioner initiated complaints and audits…. Privacy issues have traditionally arisen in the context of discrete transactions between an individual and an organization and have come to light as a result of individual-driven complaints. Today, major privacy issues arise from more systemic threats resulting from rapidly-advancing information technologies, particularly those enabled by the internet. **Such new and emerging threats affect society as a whole, at such a pervasive level, in such complex and obscure fashion, and on such a daily basis, that in most cases, the average person would not even know about them, let alone complain about them.** One has only to think of the vast array of surveillance technologies and nanotechnologies which are becoming commercially available, RFIDs, social networking, behavioural on-line marketing etc. Increasingly, data protection authorities around the world are recognizing that this is where our efforts must be directed if we have any chance of curbing these privacy threats as they emerge."[126]

---

[123] Bennett, "The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas," Canadian Public Administration, 46 (2003), 220, 237. Bennett and Raab have elaborated on these roles for data protectors in the oversight and enforcement of data protection law in The Governance of Privacy, pp. 133-143.

[124] La Forest, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues, Report of the Special Advisor to the Minister of Justice*, p. 34.

[125] See the last annual report of the OPC at http://www.privcom.gc.ca/information/ar/200607/200607_pa_e.asp#019

[126] http://www.privcom.gc.ca/parl/2008/let_080115_e.asp (emphasis added)

The same forceful arguments should be applied to shaping an approach to complaint management under the *Privacy Act*. In fact, the latest formulation of the required change from the Privacy Commissioner of Canada wisely reads as follows: "Providing discretion for the OPC to more efficiently and expeditiously deal with complaints which have less systemic and societal significance, enabling the OPC to invest more resources in complaints that will have a significant impact on improving the state of personal information management across the federal government."[127]

The Importance of Requirements for Privacy Breach Notification

Canada has moved quickly into the world of requirements for privacy breach notification to both Privacy Commissioners and to affected individuals. To date, it has largely been an issue under privacy legislation for the private sector. But when the New Brunswick Department of Health and Wellness lost several tapes of patient information in transit between that province and British Columbia in October, 2007, the N.B. Minister of Health determined that over six hundred persons needed to be notified of the loss and of the risk to their identity through identity theft.[128] MAXIMUS BC HEALTH, the custodian of the Medical Services Plan database, simultaneously flagged the accounts of affected British Columbians to monitor for unusual activity. This embarrassing episode (data tapes were not encrypted while in transit with a local courier firm) required significant amounts of senior executive time to manage in the legislature and in the media. Cabinet members were not pleased with several days of bad publicity. The B.C. Information and Privacy Commissioner immediately announced his own investigation of what had happened (adding to the embarrassment of the government and the Ministry of Health).[129]

The CIBC fax fiasco is another case in point from the private sector, where brand and reputational damage was significant. The connection among these episodes and *Privacy Act* reform is that federal institutions will not be able to escape similar obligations and costs in the event of such breaches. Few will have breach notification guidelines in place and will have no experience in what to tell frightened clients in the face of another privacy crisis. Fortunately, both the OPC and Treasury Board Secretariat have now provided guidance on these matters.[130] It will be essential to include statutory requirements for the handling of privacy breaches, including mandatory reporting to the OPC, in a revised *Privacy Act*, as the Privacy Commissioner has recently

---

[127] Testimony of Jennifer Stoddart before the House Committee on Access to Information, Privacy and Ethics, April 8, 2008.

[128] See the report (May, 2008) of the BC Information and Privacy Commissioner, at www.oipcbc.org

[129] See http://www.oipcbc.org/news/rlsgen/F07-33250_Media_Release(11_Dec_07).pdf: "I am deeply concerned that unencrypted personal data has apparently been shipped in a manner that on its face doesn't meet the Ministry's legal duty to take reasonable steps to protect personal information," the Commissioner stated."

[130] See the valuable guidance for the private sector from the OPC in its "Privacy Breach Checklist," (August 1, 2007), at http://www.privcom.gc.ca/information/guide/2007/gl_070801_checklist_e.asp. The Treasury Board guidance is at http://www.tbs-sct.gc.ca/atip-aiprp/in-ai/in-ai2007/breach-atteint_e.asp (March, 2007).

recommended.[131] Mandatory reporting of significant breaches and the resulting costs, embarrassment, bad publicity, and negative media will likely do a great deal to promote enthusiasm for effective privacy management to minimize such breaches, especially among those who do not take privacy risk management seriously. There is also a need to fashion sanctions for negligent breaches.[132]

So What Can and Should Be Done to Improve the Privacy Act? Some Final Reflections.

The following timely words belong to a summary comment from the Privacy Commissioner of Canada in June, 2006: "The urgency of reforming the *Privacy Act* increases with each passing year. What is needed is legislation that is responsive to the complexities of contemporary governance, provides an effective framework to minimize risks to informational privacy in the face of new technologies, enables public accountability, and allows Parliament to fully assume its role of guardian of our fundamental values, including the right of informational privacy."[133] That is a full and necessary agenda for the government of Canada and the Minister of Justice in particular.

A series of propositions require articulation to bring this series of reflections on reform of the *Privacy Act* to a conclusion:

- The current *Privacy Act* is highly-inadequate for needs of thethe 21st century. Simply in terms of the ten privacy commandments in the national privacy standard, it is weak on eight of them, including lack of accountability;[134] deficiencies in openness; failures in identifying purposes; absence of meaningful consent standards; not a success in limiting collection; failure to limit use, disclosure, and retention; absence of data quality tests to ensure accuracy; and a complete absence of security safeguards.[135]
- There is a clear lack of political will to revise the *Privacy Act*; it is not a captivating topic for the government, politicians, or bureaucrats. IT SHOULD BE; the public should demand no less.
- Few politicians in power care about privacy, except if a privacy crisis needs to be urgently managed in the usual manner, i.e. fending off the Opposition, the media, and concerned portions of the public. At best, privacy is a generic concern that

[131] As recommended in testimony of Jennifer Stoddart before the House Standing Committee on Access to Information, Privacy and Ethics, April 8, 2008.
[132] See Paul M. Schwartz and Edward J. Janger, "Notification of Data Security Breaches," Michigan Law Review, 105 (2007), 913-985, at http://www.paulschwartz.net/pdf/datasec_schwartz-janger.pdf
[133] Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 6.
[134] See, for example, Office of the Privacy Commissioner of Canada, Governmental Accountability for Personal Information. Reforming the Privacy Act, p. 19: "The *Privacy Act* should also ensure greater transparency, accountability and oversight over the activities of national security agencies, including more stringent reporting requirements to Parliament."
[135] These principles were articulated in the Canadian Standards Association's Model Privacy Code and enshrined in law in Schedule 1 of *PIPEDA*. They comprise the "national privacy standard" for Canada, which should be as applicable to the public as to the private sectors.

does not rise to the level of the need for action. Politicians need education so that they understand what privacy protection is all about. Constituents deserve at least that much from their elected representatives.

- Freedom of Information only appeals to Opposition politicians, not to politicians in power. It has no appeal, and is only a bother, if not a threat, to the government and public servants and their control of access to general information. This is a deplorable state of affairs, given the fact that open, transparent, and accountable government is fundamental to democracy in Canada. FOI and privacy are separate domains when it comes to needed law reforms.
- National security and law enforcement interests can sideline even the most reasoned and pragmatic approaches to revitalizing the *Privacy Act*, because they are so powerful and so aligned with the U.S. government with a sorry record of national data protection for the public sector that is even worse than Canada's. But there is no reasons that national security and law enforcement concerns cannot coexist in an atmosphere of mutual respect for the rules of the road.
- The government needs to be persuaded that privacy protection is a "conservative" issue, a "liberal" value, and a potential win/win that transcends political ideology and affiliation.
- Public servants were given no new resources to implement the *Privacy Act* and the *Access to Information Act* with predictable unhappiness over time. These pieces of legislation have left a bad taste behind. **An imperative for a revitalized *Privacy Act* is appropriate resourcing of its implementation at government institutions.**
- Sparring factions in the Department of Justice (the *Charter* people versus human rights versus access and privacy specialists) will never agree among themselves, because of their competing turfs and their respective technical expertise; their political and bureaucratic masters will have to tell them what to do and how to do it. That is a task for the Minister of Justice and his Deputy Minister.
- If concrete proposals for revision are at hand, it might be possible to hook reform of the *Privacy Act* to a government reorganization or housekeeping bill that amends several statutes at the same time. The key is preparation for such an eventuality.
- What would the Privacy Commissioner of Canada ask for if she had a meeting with the Minister and/or Deputy-Minister of Justice? Or the Clerk of the Privy Council, who was Deputy-Minister of Industry Canada when PIPEDA made headway? The OPC is prepared for such an eventuality and should be pushing for such meetings, not least because it has nothing to lose in the face of more than a generation of inertia on the part of key stakeholders. The public interest is at stake.
- Emphasizing the need for security safeguards as a core component of privacy protection, and one of the ten privacy principles, might be an easy sell for the government, politicians, and senior public servants, especially since the *Privacy Act* contains no security standards at all. That position is indefensible.
- While the U.S. has not seen fit to engage in a major overhaul of its 1974 *Privacy Act*, the U.S. federal government has developed extensive sectoral legislation to regulate specific problems, especially in the private sector. Parliament should try

to ensure that major pieces of new or revised legislation include progressive data protection measures that are commensurate with what an improved and enhanced *Privacy Act* should look like. A precedent is the confidentiality rules in the federal *Statistics Act*.[136]

- Informed U.S. observers, like Bob Gellman, say that they do not really know how to fix their *Privacy Act*; the situation in Canada is quite different.[137] Bruce Phillips produced a plan late in his term for what to do to fix the Act and presented it to the Deputy Minister of Justice.[138] As noted in several places above, Jennifer Stoddart has suggested the additional broad topics that now need to be addressed and has additionally proposed "quick fixes" for reform.[139]
- Most importantly, Canada and its provinces have excellent recent models of enhanced and improved legislation, starting with *PIPEDA* for the federal private sector, B.C. and Alberta's *Personal Information Protection Act* (*PIPA)* as much more coherent approaches to private sector regulation than *PIPEDA* (with its clumsy structure), and Ontario *PHIPA*, which I regard as taking a very intelligent and intelligible approach to data protection for the very complex area of the protection of health information (public and private sectors). See below.
- *PIPEDA* has the great advantage of being built around, in a sense, the Canadian Standards Association's *Model Code for the Protection of Personal Information* with its emphasis on the ten privacy commandments (which are almost invisible in the current *Privacy Act*).[140] One might also simply propose extending the best elements of *PIPEDA* to the public sector. The *Privacy Act* must at least feature such a principled approach.
- If one accepts a commonly-asserted dictum that fashioning data protection is not rocket science, it would take a relatively short time to develop instructions for legislative draft persons in the Department of Justice. The recommendation would be to build on what is in the current *Privacy Act* and then add on the best parts of *PIPEDA*, the *PIPA*s, and especially *PHIPA*. There is no need to re-invent the wheel.
- It is highly relevant to point out in this context that an act like Ontario *PHIPA*, addressing the most complex issues of health data protection, does not unduly harness or restrict the Ontario health care industry, led by the Ministry of Health

---

[136] Statistics Canada, over the past 20 years, has worked very hard at putting in place a policy framework that supports confidentiality, privacy, and security, and informed individuals believe that this has served the agency well. The direction and support of Ivan Fellegi, the long-time Chief Statistician, was instrumental in all of this. A year or so ago, in an interview Fellegi said that one of his most important achievements was the creation of a Division as the focal point in the organization for legal/policy matters relating to confidentiality, privacy, and security.

[137] See Gellman's critique of the U.S. *Privacy Act* in Robert Gellman, "Does Privacy Law Work?" in Philip E. Agre and Marc Rotenberg, eds., Technology and Privacy: The New Lanscape (MIT Press, Cambridge, MA, 1997), pp. 195-202, 212-15: "It would be too glib to call the Privacy Act a failure." (p. 201)

[138] For odd reasons, his successor, Radwanski, apparently wanted nothing to do with reform of the *Privacy Act.* Readers should also be reminded the legislative drafting for law reform is not the task of an Officer of Parliament.

[139] Testimony and submission of Jennifer Stoddart before the House of Commons Standing Committee on Access to Information, Privacy, and Ethics, April 29, 2008.

[140] See the informed comments on the CSA Code in Perrin, Black, Flaherty, and Rankin, eds., The Personal Information Protection and Electronic Documents Act: An Annotated Guide, pp. xiv-xv, 3-6, 10-11, 13-46.

and involving a large number of health regions, individual hospitals, labs, pharmacies, and doctors' offices. While it is a suitably complex piece of legislation, *PHIPA* has the effect of creating a large sandbox in which these health information custodians can collect, use, disclose, and retain personal information in compliance with a set of detailed rules, which are subject to the independent oversight of the Ontario Information and Privacy Commissioner.[141] In particular, health information custodians are permitted to share personal health information for legitimate purposes within this protected enclave. In terms of mandatory privacy risk management, such health information custodians are required to publicize their statements of information practices and to have Privacy Officers (contact persons) and privacy training in place for their agents. Requirements of either express or implied consent from individuals inform the entire process.[142] All of these Ontario ideas, which are reflected in other provincial privacy laws, are worthy of serious consideration for a revitalized *Privacy Act.* Again, the essential need is for the federal government to learn from the experience of others and to regain its position as the leader in Canadian data protection.

[141] For those who doubt whether such offices have teeth, consult its highly-critical privacy review of Ontario Smart Systems for Health Agency, dated March 16, 2007, and its equally strong order against the Ottawa Hospital (Order HO-002, July 2006) for serious data breaches under *PHIPA* at www.oipc.on.ca. The Ontario Commissioner has greater order making power under *PHIPA* than under the older *Freedom of Information and Protection of Privacy Act (FIPPA),*

[142] See, generally, Halyna Perun, Michael Orr, & Fannie Dimitriadis, Guide to the Ontario Personal Health Information Protection Act (Irwin Law, Toronto, 2005). www.irwinlaw.com.

Appendix 1: An Overview of the Privacy Responsibilities of Health Canada's Policy Unit

- Supports Health Canada in adopting a corporate-wide approach to manage privacy and mitigate privacy risks;
- Provides privacy policy advice to Branches and Regions as designated on the Portfolio list on a wide array of initiatives involving personal information, such as secondary uses and de-identification and re-identification of personal information;
- Develops policies and guidelines in collaboration with program officials to assist them in implementing programs and services in a manner consistent with privacy principles;
- Manages the Departmental Privacy Impact Assessment Program;
- Delivers the privacy training program to Departmental audiences and participates in the ongoing development, revision and updating of the program;
- Assists the Operational Unit by developing procedures to streamline the processing of privacy requests;
- Supports the health sector's response to privacy challenges by working with federal/provincial/ territorial stakeholders and national associations to develop pan-Canadian solutions, particularly in resolving issues associated with the deployment of Electronic Health Record Systems;
- Cooperates with other federal departments and agencies to advance national and cross-sector privacy issues, for example works with Industry Canada to ensure that the concerns of health providers are addressed in any revisions to the *Personal Information Protection and Electronic Documents Act.*