Colin J. Bennett

The privacy commissioner of Canada: Multiple roles, diverse expectations and structural dilemmas

Abstract: The contemporary roles of the privacy commissioner of Canada are multiple: he can be an ombudsman, auditor, consultant, educator, policy adviser, regulator and judge. Yet, Canadian privacy legislation provides quite poor guidance as to how he should perform and balance these roles and tends to put emphasis on complaints-resolution, a function that is less useful in promoting general compliance with the privacy principles. The analysis of the experience of privacy protection agencies, however, suggests that the most important powers are those that are general rather than specific, and proactive rather than reactive. The implementation of privacy protection law is as much an educational effort as a regulatory one, as much can be achieved in anticipation of policy and system development if privacy protection is built in at the outset. The successful implementation of privacy protection policy involves a considerable degree of learning and mutual adjustment and readjustment. It is not characterized by a top-down process of command, control and sanction. The privacy commissioner is one among many actors involved in privacy protection policy in Canada, and his success is dependent on the recognition that he has many policy instruments at his disposal, besides the law, to encourage higher standards for the treatment of personal information by Canadian organizations.

Sommaire : Le Commissaire à la protection de la vie privée du Canada joue à l'heure actuelle des rôles multiples : il peut être ombudsman, vérificateur, consultant, éducateur, conseiller en politique, responsable de la réglementation et juge. Et pourtant, les lois canadiennes relatives à la protection de la vie privée n'offrent que de médiocres directives quant à la manière dont il devrait s'acquitter de ces différents rôles et les équilibrer. Elles ont tendance à mettre l'accent sur la résolution des plaintes, fonction qui est moins utile pour promouvoir l'observation des principes du respect de la vie.

The author is professor, Department of Political Science, University of Victoria. He is grateful to David Flaherty and Dona Vallières of the Office of the Privacy Commissioner for their helpful comments on an earlier draft of this paper and to Martin French for research assistance. He would also like to acknowledge the Journal's anonymous reviewers. Earlier drafts of this article were delivered at the conference "Independence and Responsibility: The Officers of Parliament," 2-3 November 2001, University of Saskatchewan, and at the conference "Two Sides of the Same Coin: Relations between Parliamentary Agencies and the Public Service," Canadian Centre for Management Development, 20 March 2002.
Within a period of just twenty years, the privacy issue has become a highly salient one in every advanced industrial state. As new intrusive technologies have entered public and private organizations so too have fears grown for the unregulated collection, use and disclosure of personally identifiable information and for the potential for unacceptable levels of surveillance. New practices, such as video-surveillance cameras, biometrics, smart identity cards, drug-testing, telemarketing, location-based services, genetic databases and so on, often introduced with good intentions, can have unintended consequences for the protection of personal information. In our roles as citizens, consumers, employees, travellers, patients, students, recipients of social benefits, or whatever, we continuously and unawares leave fragments of our data behind us as we go about our everyday lives. Some thirty different books have been published on privacy in the last two decades, most of which have claimed in their titles the "death" or "erosion" of personal privacy in the information society. If not "the defining issue of the next decade" – as the current privacy commissioner of Canada is fond of stating – privacy is nevertheless an "issue whose time has come."

At the centre of these fascinating policy and intellectual debates are situated the independent oversight agencies that have legislative authority in different countries to protect privacy rights. Most advanced industrial states, with the notable exception of the United States, have "privacy" or "data-protection" agencies that perform a variety of advisory, educational and enforcement functions within their respective jurisdictions. The Canadian privacy commissioner, and his counterparts in the provinces, operates within a large and increasing network of international actors whose roles are defined by this shifting and nebulous issue. The aim of this article is to analyse the responsibilities of the Office of the Privacy Commissioner (OPC) of Canada and to highlight the various dilemmas inherent in the exercise of these powers.
At the time of writing, the current commissioner was embroiled in a serious controversy that threatened the operation of the OPC. George Radwanski had been called to account by the house government operations and estimates committee for falsifying a document presented in evidence, for excessive foreign travel expenditures, and for a residential allowance negotiated through the Privacy Council Office, a perk that allegedly impinged on his independence and integrity. Issues had also been raised about the treatment of his staff, leading to an unprecedented media release by most members of his office calling on him to step aside. The auditor general was called in to study the financial administration and hiring practices within the office. In defense, Radwanski pointed to the increased importance of having a strong privacy watchdog in the wake of 11 September 2001 and even suggested a concerted political effort to discredit him for his forceful opposition to government surveillance schemes. The privacy commissioner of Canada has never received so much public, media or parliamentary attention. As a result of the intense pressure, he resigned his position on 23 June 2003.

This controversy supports the central thesis of this article. There are certain structural dilemmas inherent in the exercise of the powers of this office. The commissioner is nominally an “officer of Parliament,” and, yet, historically, Parliament has had very little role in choosing the appointees. That places the commissioner in a paradoxical position, informally beholden to the prime minister and the Prime Minister’s Office and yet formally responsible to Parliament. When the current crisis subsides, Parliament might want to take a close look at how the privacy commissioner is appointed, and how parliamentary committees might play a more active role in overseeing this office and in using its resources to scrutinise government surveillance schemes.

Moreover, the OPC is a hybrid and difficult to classify according to any of the traditional conceptions of regulatory or oversight agencies. The commissioner is an ombudsman for citizen complaints, an auditor of organizational practices, a consultant on new and existing information systems, an educator of the public, a policy adviser, a quasi-judge and a regulator of business. Incumbents are only given very partial guidance as to how to exercise these powers by the statutory frameworks themselves. This 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. Whether the commissioner acts as an advocate or a balancer, as a publicist of a private negotiator, or whether he acts in concert with, or isolation from, his colleagues in the provinces is up to him. And these are issues at the heart of the current controversy over George Radwanski.
The pattern of legislative development

The first privacy legislation at the federal level was contained in Part IV of the 1977 Canadian Human Rights Act, which established the Office of the Privacy Commissioner as a member of the Canadian Human Rights Commission. While this statute succeeded in codifying for the first time a set of privacy principles in legislation, privacy sat uneasily within a statute whose main focus was discrimination.8

The current 1982 Privacy Act in fact flows out of the parallel debates over a federal Access to Information Act, which raised immediate questions about the compatibility between such legislation and the privacy standards within Part IV. It stems from a belief that data protection should be a corollary to freedom of information and that the various exemptions in both pieces of legislation should be internally consistent. Bill C-43, incorporating an Access to Information Act and a revised Privacy Act, thus institutionalized the Canadian innovation of legislating access to information and privacy protection within the same statutory framework, at the same time that Quebec was developing a similar model. This model was later emulated by Ontario in 1988, by British Columbia in 1993, by Alberta in 1995 and by Manitoba in 1997. By the end of 2001, every province and territory had a statutory privacy protection policy for the personal information held by public agencies. Table 1 presents the current profile of access to information and privacy legislation with respect to the public sector in Canada.

Privacy protection for business, however, only arose as a result of commercial and trade-related pressures. In particular, the passage of the Data Protection Directive in 1995 from the European Union effectively meant that no jurisdiction in Canada (save Quebec) could plausibly claim an "adequate level of protection" and therefore safely process personal data transmitted from Europe. The domestic and international debates over the development and character of the "information highway" exposed the need for a common set of "rules of the road" for the networked and distributed computing and communications environment of the 21st century.10 These commercial emphases explain why the lead department for this policy initiative was Industry Canada, which issued a consultative document in 199911 and then proceeded with successive bills in the 1999 and 2000 parliamentary sessions. Bill C-6, the Protection of Personal Information and Electronic Documents Act (PIPEDA), was passed in 2000.12

The PIPEDA has come into force in stages. On 1 January 2001, the following businesses were obliged to comply: banking, telecommunications, broadcasting, airlines, and transportation companies, as well as any company that transfers personal information across provincial or international borders "for consideration." On 1 January 2004, the law will apply to all commercial activities by the private sector, including companies under provincial or ter-
<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Name of act</th>
<th>Date proclaimed</th>
<th>Oversight agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td>Privacy Act</td>
<td>1982</td>
<td>Privacy Commissioner of Canada</td>
</tr>
<tr>
<td>Manitoba</td>
<td>Freedom of Information and Protection of Privacy Act</td>
<td>1997</td>
<td>Office of the Manitoba Ombudsman</td>
</tr>
<tr>
<td>New Brunswick</td>
<td>Protection of Personal Information Act</td>
<td>2000</td>
<td>Office of the Ombudsman</td>
</tr>
<tr>
<td>Newfoundland</td>
<td>Privacy Act</td>
<td>1996</td>
<td>Director of Legal Services, Department of Justice</td>
</tr>
<tr>
<td>Ontario</td>
<td>Freedom of Information and Protection of Privacy Act</td>
<td>1988</td>
<td>Information and Privacy Commissioner/Ontario</td>
</tr>
<tr>
<td>Prince Edward Island</td>
<td>Freedom of Information and Protection of Privacy Act</td>
<td>2001</td>
<td>Assistant Clerk of the Committee Legislative Assembly</td>
</tr>
<tr>
<td>Quebec</td>
<td>An act respecting access to documents held by public bodies and the protection of personal information</td>
<td>1982</td>
<td>La Commission d’Accès à l’Information du Quebec</td>
</tr>
<tr>
<td>Saskatchewan</td>
<td>Freedom of Information and Protection of Privacy Act</td>
<td>1992</td>
<td>Information, Privacy and Conflict Of Interest Commissioner</td>
</tr>
<tr>
<td>North West Territories/Nunavut</td>
<td>Access to Information and Protection of Privacy Act</td>
<td>1996</td>
<td>Information and Privacy Commissioner</td>
</tr>
<tr>
<td>Yukon Territory</td>
<td>Access to Information and Protection of Privacy Act</td>
<td>1996</td>
<td>Office of the Ombudsman</td>
</tr>
</tbody>
</table>
The privacy commissioner of Canada: powers and functions

The privacy commissioner of Canada is appointed by the governor in council after approval by resolution of both Senate and House of Commons. The commissioner is appointed for a seven-year term that may be renewed. Four individuals have so far occupied this office: Inger Hansen (1977–82), John
Table 2. Status of General Privacy Protection Law for the Private Sector

<table>
<thead>
<tr>
<th>Jurisdiction</th>
<th>Act or other official action</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal</td>
<td>Protection of Personal Information and Electronic Documents Act</td>
<td>2001</td>
</tr>
<tr>
<td>Alberta</td>
<td>Bill 44, “The Personal Information Protection Act”</td>
<td>Introduced, May 2003</td>
</tr>
<tr>
<td>British Columbia</td>
<td>Bill 38, “The Personal Information Protection Act”</td>
<td>Introduced, March 2003</td>
</tr>
<tr>
<td>Manitoba</td>
<td>Discussion document published</td>
<td>1999</td>
</tr>
<tr>
<td>New Brunswick</td>
<td>Discussion document published</td>
<td>1998</td>
</tr>
<tr>
<td>New Brunswick</td>
<td>No known official action</td>
<td></td>
</tr>
<tr>
<td>Nova Scotia</td>
<td>No known official action</td>
<td></td>
</tr>
<tr>
<td>Ontario</td>
<td>Discussion document published. Bill introduced and withdrawn</td>
<td>2002</td>
</tr>
<tr>
<td>Prince Edward Island</td>
<td>No known action</td>
<td></td>
</tr>
<tr>
<td>Quebec</td>
<td>Bill C-68 (An Act respecting the Protection of Personal Information in the Private Sector)</td>
<td>1993 (amended 2001)</td>
</tr>
<tr>
<td>Saskatchewan</td>
<td>Internal consultations</td>
<td></td>
</tr>
<tr>
<td>North West Territories/Nunavut</td>
<td>No known action</td>
<td></td>
</tr>
<tr>
<td>Yukon</td>
<td>No known action</td>
<td></td>
</tr>
</tbody>
</table>

Grace (1983–90), Bruce Phillips (1990–2000) and the former occupant, George Radwanski. The appointment process has, on occasion, raised concerns about the independence of the appointee. Bruce Phillips, the former communications director within the Mulroney government, had to endure a lengthy process of parliamentary scrutiny before eventually being ratified. The OPC currently has a staff of around eighty people and a budget of around $11 million. There has been a significant increase in size and
resources as a result of the enactment of the **PIPEDA**. Staff have increased by 100 per cent; the budget has increased nearly fourfold.\(^\text{15}\)

The overall structure of the **OPC** is now divided into five branches. An Investigations and Inquiries Branch is responsible for investigating, on behalf of the commissioner, complaints received from individuals under Section 29 of the **Privacy Act** and Section 11 of the **PIPEDA**. The Privacy Practices and Reviews Branch attempts to assess how well organizations are complying with the requirements set out in two statutes, by conducting compliance reviews under Section 37 of the **Privacy Act** and audits under Section 18 of the **PIPEDA**. The Communications and Strategic Analysis Branch has been newly created to carry out the public education and research mandate of the office, strengthened under the **PIPEDA**. A Strategic Analysis Division serves as the centre of expertise on emerging privacy issues in Canada and abroad, by researching trends, providing analysis on key issues, and developing general positions on privacy-related issues. An expanded Legal Services Branch, headed by the general counsel, provides specialized legal and strategic advice and litigation support to the privacy commissioner. Finally, an integrated Corporate Services Branch provides administrative services (finance, personnel, IT and general administration) to both privacy and access-to-information commissioners.\(^\text{16}\)

The Office of the Privacy Commissioner is the main, but not the only, agency responsible for oversight of privacy protection policy. Day-to-day advice on the implementation of the **Privacy Act** is the responsibility of Treasury Board, which also compiles and publishes the list of personal information banks. With respect to the **PIPEDA**, Industry Canada performs some wider policy functions, although there is tension with the **OPC** on the appropriate division of responsibilities.\(^\text{17}\) The Information and Privacy Branch of the Department of Justice gives day-to-day legal advice on the interpretation of both privacy and access-to-information statutes. The **Privacy Act** is also clear that primary responsibility for implementation rests with the "designated minister" or "head" of the government institution in question.

Structurally, the office seems to have been organized to reflect the principal statutory functions of the commissioner under both laws. A closer examination of his functional responsibilities reveals, however, some subtle differences between the responsibilities for public-sector, versus private-sector, oversight.

**The receipt, investigation and resolution of complaints**

The federal privacy commissioner’s self-declared mission is first “to be an effective ombudsman’s office, providing thorough and timely complaint investigation to ensure Canadians enjoy the rights set out in the **Privacy Act**.”\(^\text{18}\) The federal **Privacy Act** is based squarely on the ombudsman
approach; complaints are received, investigated and findings and recommendations issued.\textsuperscript{19} Under this legislation, the privacy commissioner has the power to

- summon and enforce the appearance of persons before the privacy commissioner and compel them to give oral or written evidence on oath and to produce such documents and things as the commissioner deems requisite to the full investigation and consideration of the complaint, in the same manner and to the same extent as a superior court of record;
- administer oaths;
- receive and accept such evidence and other information ... whether or not such evidence or information is or would be admissible in a court of law;
- enter any premises occupied by any government institution on satisfying any security requirements of the institution relating to the premises;
- converse in private with any person in any premises entered and carry out inquiries within the authority of the privacy commissioner; and
- examine or obtain copies or extracts from books or other records found in any premises entered ... containing any matter relevant to the investigation.

Under certain circumstances, the commissioner may apply for review by a federal court, if his recommendations are not acted upon. For the most part, however, these powers are not used, because the commissioner typically relies on conciliation and mediation with the ultimate hope that the willingness to avoid bad publicity will encourage a satisfactory settlement of the complaint.

In his initial comments on the PIPEDA, the former commissioner, Bruce Phillips, was very careful to stress that neither he nor his staff wanted powers of enforcement: "The 15 years of experience that my office has had with an ombuds role for complaint investigation has shown that heavy-fisted enforcement is not necessary to secure the privacy rights of Canadians. Rather than emphasizing confrontation, the ombuds role emphasizes resolving complaints. Perhaps ultimately more important, it emphasizes correcting the underlying problems that lead to those complaints."\textsuperscript{20} Besides, it is argued that bad publicity for privacy protection can be a more effective sanction against business than it is against government. In contrast, others contend that the ability to negotiate with data users is facilitated by the existence of an enforcement power at the end of the day, even if those powers are rarely used.\textsuperscript{21}

Largely as a result of Bruce Phillips' influence, the investigative powers under the PIPEDA were deliberately drafted in a similar manner. But the process of complaints-handling seems to be operating in a rather different man-
ner as far as the private sector is concerned. The first principle of the CSA Model Code stipulates the designation of an individual or individuals within the organization who shall be responsible for compliance with the privacy principles. And the tenth principle mandates them to establish a complaints-handling process. Under certain circumstances, trade associations (such as those within the banking and direct-marketing industries) may also play a mediation role. There is, then, the implicit understanding that the privacy commissioner should be the avenue of last resort—the means of redress when resolution within the business, the trade or professional association, or even within a federal or provincial regulatory authority fails.  

On the other hand, Section 12 of the PIPEDA provides that the commissioner must investigate any complaint he receives, using similar powers as those bestowed under the Privacy Act. He is also explicitly empowered to seek resolution of any matter through mediation or other alternative dispute resolution mechanisms. It is expected that private-sector companies might have a considerable incentive to settle disputes without publicity and expense. Furthermore, many complaints relating to private-sector compliance may not involve a remedy or settlement for direct harm to the complainant. Many complaints will probably involve the more general breaches of Schedule 1 principles, such as failure to name a "responsible person," insufficient statement of the purposes for collection, inappropriate consent provisions, lax security provisions, and so on. These matters might be resolved through less formal negotiations, resulting in the organization changing its practices.

Under the PIPEDA, the commissioner has one year from the filing of the complaint to prepare a report, provided he is satisfied that the complainant has exhausted all other avenues available and that the complaint is not "trivial, frivolous or vexatious or is made in bad faith" (Section 13 (2)). Under both laws, the commissioner reaches a finding that may fall under any one of four categories: not well-founded, well-founded, well-founded/resolved, and resolved. Under the Privacy Act, he also has the discretion to settle the dispute during the course of the investigation, or to decide that the investigation be discontinued.

Further enforcement requires review by the federal court, to which the privacy commissioner may apply by himself, or on behalf of the complainant. Because the commissioner does not make binding decisions, he has a great deal of latitude to assist and advise a complainant who wishes judicial review. Under both statutes, the circumstances under which a review by the court may be requested are carefully outlined, and not every breach of these statutes may be judicially reviewed. Ultimately, the court has the power to order the organization to correct its practices and award damages to the complainant.
Audit powers

Each of these processes for complaints resolution at federal and provincial levels is inherently reactive. The larger question is whether or not the commissioner should be expressly empowered to conduct investigations in the absence of a complaint. Subsequent investigations would then take on the form of a more systemic "audits" of the personal information practices of an organization and would go beyond the particular grievance of the original complainant(s). Privacy commissioners may have suspicions about the personal-information practices of a particular organization that arise from a number of sources, including the media. The conduct of general audits of an organization or a technology can be a very effective way to implement fair information practices.24

Unlike in the Privacy Act, where the word "audit" does not appear, under the PIPEDA, the commissioner is given more explicit powers to "audit the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that the organization is contravening a provision of Division 1 or is not following a recommendation set out in Schedule 1" (Section 18 (1)). Reasonable notice must be given, and the commissioner must have reasonable grounds. According to some of the original drafters of this legislation, these powers are not meant to be used for investigations of isolated incidents, nor are they informal "site visits."25 Rather, they are supposed to be a more systemic analysis of an organization's entire personal-information handling practices.26

The legislation also explicitly empowers the commissioner to delegate the auditing function. Audits are also the kind of function that might be delegated to provincial commissioners, to accounting forms, to standards certification bodies, and so on. The innovation of including a certifiable standard within the body of the statute was deliberately intended to provide a built-in mechanism for self-regulation. A standard is more than a code of practice, because it also embraces a common conformity assessment methodology, by which compliance can be independently and regularly tested. This tool is potentially of enormous value to the privacy commissioner. He can advise a registration to the standard and therein be assured that a verifiable and independent audit program is conducted.27 To date, however, it is not clear that this innovative aspect of the Canadian approach to private-sector compliance has been fully appreciated.

Educational and advisory functions

We should make a distinction between the education of the general public, research into wider privacy and surveillance questions, and the provision of advice to organizations. The provincial commissioners in B.C., Alberta and Ontario are given an explicit statutory obligation to inform the public
about their legislation. 28 Under the Privacy Act, however, the federal commissioner has no mandate for public education and therefore no budget for such activities. Under Section 24 of the PIPEDA, the commissioner is empowered to "develop and conduct information programs to foster public understanding, and recognition of the purposes [of the Act]." To this end, the Communications and Strategic Analysis Branch of the office puts a lot of effort into news releases, media interviews, conference speeches, and so on and has also developed a series of guidance notes on how to protect one's privacy rights.

The commissioner can also carry out "special studies relating to the privacy of individuals" and has used this power in the past to commission substantial research reports on issues such as AIDS, drug testing, and genetic testing, though little original research has been published in the last ten years. 29 There is, of course, a fine line between the performance of wider educational and research roles, and the provision of advice on more specific projects and proposals. So this branch also publishes guidance notes for businesses on how to comply with the PIPEDA. 30 The law also allows the commissioner to encourage organizations to "develop detailed policies and practices, including organizational codes of practice." Commissioners in other countries, such as New Zealand and the Netherlands, are given more formal powers to receive and approve company and sectoral codes, a model that was considered but rejected during the drafting of Bill C-6.

Each commissioner, therefore, has to wrestle with some difficult dilemmas. How each of these conflicts is resolved will dictate how the privacy issue is reconciled within the larger contours of Canadian public policy and how the value is injected into debates about the processing of personal information and balanced against arguments for increased efficiency, security or profit.

All Canadian legislation grants responsibilities to the commissioners to comment on the privacy implications of proposed legislation or on new automated personal record systems. 31 Under the Privacy Act, the federal privacy commissioner is empowered to "make a special report to Parliament referring to and commenting on any matter within the scope of the powers, duties and functions of the Commissioner." 32 While not formally mentioned in the PIPEDA, the provision of advice on new schemes and proposals is clearly included in the general power (Section 24 (d)) to "promote, by any means that the Commissioner considers appropriate, the purposes [of this Act]." Privacy commissioners try to inject a privacy perspective at the earli-
est stages of the legislative process, technology development or service delivery. High-profile legislative changes that involve radical implications for the processing of personal information are often the circumstances under which consultation is the most serious; examples would be the proposal for a DNA databank, the permanent voters register, the firearms registry, or the organ-donor registry. Also the decennial census invariably brings the OPC into conflict with Statistics Canada. The commissioner can then act as a kind of “privacy consultant” to the organization concerned, warning of potential privacy implications before services and technologies are introduced, and sometimes requiring “privacy impact assessments.”

**Dilemmas of privacy protection oversight**

Privacy protection is a relatively new area of public policy. Its contours are constantly changing, and the issues that might require resolution from day to day are unpredictable. In this fluid context, the law can only give partial guidance to the incumbents of these offices. Each commissioner, therefore, has to wrestle with some difficult dilemmas. How each of these conflicts is resolved will dictate how the privacy issue is reconciled within the larger contours of Canadian public policy and how the value is injected into debates about the processing of personal information and balanced against arguments for increased efficiency, security or profit.

**Enforcers or educators?**

Both federal statutes invite the commissioner to be both an enforcer of the law and an educator. Both roles, to some extent, rely on an assumption that an “ounce of prevention” is better than a time-consuming and costly process of reactive investigation and enforcement.

To some extent, the educational functions rely on the premise that many organizations would want to do the “right thing” if only they knew what the right thing was. And commissioners have constantly used the rhetoric that good privacy protection practices are not only compatible with the human rights of the individual but are also consistent with good government and effective business. In a 2001 speech, George Radwanski articulated a familiar theme of recent commissioners: “In the ‘new business culture,’ clients and customers are seen as partners in the enterprise, partners whose needs and desires must be taken into account in any business decision. No business can afford to ignore the customer’s priorities. Things are just too competitive for that. Part of the new business culture is what I would call a ‘culture of privacy.’” This same argument is laid out in greater detail in a recent book co-authored by Ann Cavoukian, the current Ontario commissioner.

The larger issue about whether the implementation of the fair informa-
tion practices is indeed consistent with the business profit motive is, of course, controversial. Some measure of privacy protection is in the interests of some businesses at some point. But it is naïve to suppose that there are not interests that directly contradict the fair information practices doctrine. For example, gaining express or positive consent for the collection of sensitive personal information (as the PIPEDA mandates) costs time and money. To the extent that customers do not provide their consent, the value of the personal information for marketing purposes is diminished. Nevertheless, it is at least useful rhetoric for commissioners to attempt to argue that what the law requires is, indeed, in the interests of the enlightened organization.

The problem arises when the educational role and mandate conflicts with a commissioner’s duty to enforce the law and, in the case of the PIPEDA, to reach an impartial finding in response to a complaint. Educational comments and literature from the privacy commissioner need always, therefore, to be cognizant of the fact that many privacy issues will require the application of the powers of complaints investigation. Thus, he cannot be too specific in his public comments about the practices of any one organization, group of organizations, or sectors, lest he open himself up to the charge of bias. Even in private, there is only so far that the commissioner and his staff can go in giving concrete answers. Care in performing these educational roles is imperative if future findings are not to be influenced by the need to maintain a consistent story.

Advocates or balancers?
In his seminal study of data protection policy in six countries, David Flaherty concluded the following:

The data protection agency should not be a miniparliament that seeks to settle the appropriate balance internally, nor should it concentrate solely on presenting a balanced perspective of the competing interests to the external master, be it the government or the legislature. Its emphasis should be on the antisurveillance side of the balance, since the forces allied against privacy, or at least in favor of efficient surveillance, are generally so powerful. Flaherty articulates a classic dilemma. Should the privacy commissioner be an unequivocal champion of privacy, or a pragmatist, constantly striving for the right “balance” between individual rights and social good?

The PIPEDA legislation answers this question quite clearly. Its purpose is to “establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the
need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances” (Section 3, emphasis added). The emphasis on organizational interests stems from the government’s explicit attempt to link privacy protection to its more general effort to promote electronic commerce and the digital economy. There is no doubt that private-sector privacy protection would not have reached the federal agenda without the advent of the Internet and associated information transactions. On the other hand, some critics have also adopted the position that the PIPEDA is not really a privacy protection law at all but merely a strategy designed to support and legitimate existing business practices. This view has motivated one Canadian senator to introduce a “Privacy Rights Charter” that would, in her opinion, emphasize the importance of privacy as a human right and serve as an overarching framework for other legislation, including the PIPEDA.

At the provincial level, of course, the balancing function is inherent within the combined role of information and privacy commissioners. These offices need constantly to be aware of their dual responsibility to facilitate access to information to government documents. In large measure, these two functions are not contradictory; both privacy protection and access to information tend to regulate the processing and disclosure of different forms of information. However, the combined role does institutionalize, at least in the government’s mind, a belief that the commissioner cannot solely be a champion for the privacy interest.

At the federal level, no such constraints exist. And some of the initial comments by Commissioner Radwanski suggest that he believes that the Parliament created the position of privacy commissioner of Canada, not only to oversee Canadian privacy law “but also to serve as the champion of the privacy rights of all Canadians.” And he has not been shy about expressing opinions concerning any plan by a provincial government that has serious privacy implications. Earlier he concluded a speech by stating that “a Privacy Commissioner’s voice has to be raised in constant advocacy of privacy, reminding people of their rights and obligations, standing up for principle in the face of expediency and convenience, and strengthening one of the most critical elements of the social glue that binds us together – strengthening privacy.”

Commissioner Radwanski’s strident and public posture of privacy advocacy has been described by his critics as unnecessarily “confrontational” and designed more for catchy headlines than for the stable and conciliatory resolution of problems. It has even prompted his predecessors to publicly criticize his overblown rhetoric. In response, Radwanski has asserted that the post-9-11 September environment, combined with huge advances in technology, requires a new approach for the office: “I do have a more activist style and I’m, I think, much more involved than was my predecessor. I think
circumstances require it. I think one has to do this job in a very committed way."

Publicists or private negotiators?
A related dilemma concerns the extent of publicity with which the privacy commissioner carries out his functions. The educational and advocacy roles obviously require the maximum publicity that the budget will allow. But the investigative function also requires certain sensitivity to the interests of both parties in a complaint. Again, the legislation provides little guidance as to how he should resolve this dilemma.

Initial press reports on how the new commissioner would handle complaints under the PIPEDA suggested that he would not, as a matter of practice, publish the findings of his investigations. This prompted an open letter from a group of privacy lawyers and advocates lamenting this decision and arguing the nascent field of privacy law poses such novel and complex questions that the benefits of disclosure clearly outweigh confidentiality concerns. Whether this pressure worked or whether initial reports were inaccurate, the office did begin a practice of publishing a summary of its findings with respects to complaints and placing them on its web site. In few cases, however, has the name of the complainant or the organization been publicly identified, even though they may be a matter of public debate in other circles. This has led some advocates to wonder whether a significant weapon in the armoury of the OPC is being voluntarily and unnecessarily surrendered. Those defending the ombudsman approach have always argued that the threat of bad publicity and the significant harm to a company’s reputation was a significant inducement towards compliance.

There is a difficult dilemma about what, if anything, can or should be said publicly during the course of complaint investigation, and indeed afterwards. Basic respect for administrative justice would dictate that the commissioner should refrain from making any public comment on issues that are currently before him. But this rule is not always followed. While his investigation into a brochure released by Air Canada was still under way, he released an open letter to the company detailing his concern with some of their marketing practices and requesting that they cease their mailings until his investigation was completed:

While I cannot, of course, pre-judge this matter before I have completed my investigation on this issue, I would be remiss if I did not raise my concerns at the outset. Should I ultimately determine that the collection and disclosure of personal information is contrary to the PIPED Act, Air Canada might well already have caused irreparable damage to individual privacy rights. I have therefore respectfully requested that Air Canada suspend its activities in this regard pending the outcome of my investigation.
The publication of complaints, and the debate about their merits, may often be beyond the commissioner's control. There is, for example, nothing to stop the complainant from releasing his or her complaint to the media or to Internet listservers, as indeed happened in the case of a series of complaints by the Public Interest Advocacy Centre about the marketing practices of some of Canada's major financial and telecommunications companies. By the time the commissioner has concluded his investigation and reached a finding, there may already have been a good deal of publicity about a particular practice and the emergence of a powerful consensus on the appropriate way it should be resolved. The commissioner is not immune from this pressure.

Initial evidence of the PIPEDA's implementation suggests that the last commissioner was, by instinct, a publicist who understands the important role of the media in spotlighting privacy-invasive practices. Like his predecessor, Bruce Phillips, George Radwanski is a former journalist who has a keen instinct for what makes news, with a large number of contacts who might give him a sympathetic ear. Thus his persistent criticisms of many of the policy and legal changes introduced in the wake of 11 September have kept this commissioner in the news. Each privacy commissioner has also tried to make a big media event of the publication of the annual report.

Commissioner Radwanski was also far more prone to release his views in the form of "open letters" than were his predecessors. In addition to the Air Canada case quoted above, the investigation into the practice of customs officers opening letters and packages (without warrant) was also punctuated by press debate initiated by the release of "open letters," as has been the proposals for a "Big Brother" database on the travel behaviour of Canadians. Far more controversially, Mr. Radwanski released an open letter to John Reid, the access-to-information commissioner, criticizing in very strident language the latter's insistence on reviewing the contents of the prime minister's diaries. These examples, however, point up a contradiction at the heart of the privacy commissioner's role. He is both an educator and an adjudicator. The former role sometimes prompts the relaxation of some of the stricter standards of administrative due process.

Cooperative team or single actors?

A final issue relates to the extent to which the privacy commissioner can and should act as one of a team, in cooperation with his counterparts in the provinces. Each statute, and each agency, has been created independently and with little regard to cooperative action. Certainly there has been a good deal of policy emulation from province to province, leading to a degree of policy harmonization. And, of course, the federal structure provides a natural laboratory for policy learning. But, little in any of these distinct pieces of legislation, at either federal or provincial levels, contem-
plates a concerted approach to the implementation of privacy protection policy in Canada.

There is one important exception to this generalization. Because of the constitutional complexities of private-sector oversight, a provision was inserted into the PIPEDA to encourage and promote federal, provincial and territorial cooperation: "If the Commissioner considers it appropriate to do so, or on the request of an interested person, the Commissioner may, in order to ensure that personal information is protected in as consistent a manner as possible, consult with any person who, under provincial legislation that is substantially similar to this part, has powers and duties similar to those of the Commissioner" (Section 23 (1)). It is noteworthy that the consultation referred to can be undertaken at the request of an interested person, leaving scope for outside advocates, businesses and associations to attempt to foster cooperation and consistency. The legislation also specifies that such coordination may relate to procedures for complaints handling, the undertaking of research, and the development of model contracts.

The current reality with respect to the private sector is that there is no commissioner outside Quebec who is currently responsible for the oversight of "substantially similar" legislation. Thus, any cooperation of private-sector oversight will be with provincial commissioners who would need to take a more assertive posture than their formal legislative authority would permit. By the same token, the federal privacy commissioner's authority to oversee interprovincial and international transactions involving personal data is very limited, unless he can influence the behaviour of organizations under provincial jurisdiction. This recognition prompted the inclusion of Section 23 (2c), which contemplates the development of model contracts in association with provincial commissioners to convince organizations to use contractual means to protect personal information when it is transferred outside the originating jurisdiction.

Even before the PIPEDA, the commissioners have held annual meetings to discuss issues of common import. Rarely, however, have these occasions prompted any public statement or communiqué. There have been exceptions. In 1995, when the Information Highway Advisory Council was preparing its report, and contemplating a model of privacy protection based on self-regulation rather than legislation, a jointly signed letter from the then privacy commissioners was instrumental in strengthening a proposal for legislation, which ultimately influenced Industry Canada to pass Bill C-6.50 A more recent example occurred in November 2001, when seven provincial privacy commissioners sent a strongly worded letter to revenue minister Elinor Caplan protesting the federal government's plan to expand a database that stores details of the air travel of Canadians. For the most part, federal and provincial commissioners have often been hesitant to take concerted policy stances on common issues. Under most circumstances, there will always be at
least one commissioner for whom an assertion of a position beyond his legislative and jurisdictional competence will compromise his or her position with their respective governments on whom they rely for resources.

The initial examples of cooperation under the PIPEDA have involved requests by provincial commissioners to the federal commissioner to investigate a problem occurring in their jurisdictions. In May 2001, the commissioner of the Northwest Territories filed a complaint about the positioning of video-surveillance cameras at a particular intersection in Yellowknife, a complaint that led to a finding that video-surveillance by a commercial security firm in this manner was an unlawful collection of personal information under the PIPEDA. Following this finding, the B.C. commissioner, David Loukideli, complained under the Privacy Act about the lawfulness of RCMP public video-cameras in Kelowna. Again, George Radwanski found the program in violation of the legislation and is now engaged in a constitutional challenge of public video-surveillance under the Charter. Leaving aside these fascinating substantive and jurisdictional issues, both cases raise the question about the role of independent commissioners in drawing possible privacy violations to the attention of the federal commissioner. Both cases undoubtedly received more media attention as a result of the sources of the complaints. But, in effect, both commissioners were acting not as commissioners but as private citizens exercising their rights to complain under the laws of Canada. Letters of complaint from any citizen of Yellowknife or Kelowna could potentially have yielded the same results under law, though perhaps with less urgency.

On the whole, however, despite media rhetoric about the “privacy czar,” a pragmatic approach is unavoidable and explained by the properties of the issue with which commissioners are dealing.

Whether these examples signal higher levels of cooperation in the years ahead is too early to judge. It is certainly arguable that the progress of privacy protection in Canada will depend on the ability of the commissioners to act and speak with one voice. But they are not equals. The assertion by Commissioner Radwanski that he is the “champion of the privacy rights for all Canadians” suggests that, statutory and constitutional constraints aside, the institution will always be perceived as primus inter pares.

Conclusion: the co-production of privacy protection

Our recent comparative analysis of privacy protection policy has concluded that, regardless of legislative powers, every data-protection commissioner in
Canada and elsewhere is expected at some point to perform seven interrelated roles: ombudsman, auditor, consultant, educator, policy adviser, negotiator and enforcer. These roles may not be explicit in national legislation, and they obviously assume different weights in different contexts. But I would argue that every commissioner at some point needs to consider how each of these roles should be performed.

In the Canadian context, the formal designation of the privacy commissioner as an "officer of Parliament" hardly captures this flexible and extensive set of responsibilities. Unlike most other officers of Parliament, the privacy commissioner now has significant responsibilities for overseeing private-sector practice. He is not just an overseer of the state but a regulator of business. This broadening of power has enormous implications for the operation of the office, and indeed for the very definition of an "officer of Parliament."

This lengthy and adaptable set of roles might also lead observers to conclude that his office can wield a considerable amount of power. And, occasionally, commissioners can use their legislative authority and public position to take a forceful stance against an intrusive surveillance technology. Those postures can sometimes strike a responsive chord with political and/or public opinion and lead to significant pressures on organizations: the conflict in 1999–2000 over the Longitudinal Labour Force file administered by Human Resources Development Canada (HRDC) led to front-page stories and to the eventual dismantling of the system. On the whole, however, despite media rhetoric about the "privacy czar," a pragmatic approach is unavoidable and explained by the properties of the issue with which commissioners are dealing.

First, the enforcement of the privacy principles is, by and large, not amenable to clear judgements about right and wrong. The resolution of complaints and the promotion of compliance, under both statutes, takes place in some grey interpretive areas: whether X is indeed personal information; whether consent is indeed "informed"; whether the organization made bona fide efforts to respond to an access request; whether the security provisions are consistent with the "sensitivity of the data"; what a "reasonable person"
would consider an appropriate purpose; what is a "consistent use"; and so on. Any resistance to the implementation of privacy tends to focus on these more subtle issues of interpretation, which then lead to some quite complicated and technical debates about the balancing of risks within certain organizational and technical practices. Rhetoric aside, that reality inevitably produces a pragmatic regulatory style.

Secondly, and relatedly, the privacy commissioner and his colleagues must now attempt to comprehend the implications of a staggering range of new surveillance tools: smart cards, biometric identifiers, public-key infrastructures, video-surveillance, intrusive practices on the Internet, computer profiling, call-management services, location-based services, the tracking of mobile telephony, and so on. When the Privacy Act was proclaimed, the technological environment was relatively simple; personal data was processed in discrete databanks. Now, that environment is more distributed, networked, dynamic and complicated. Personal data is not processed in distinct stages (collection, storage, disclosure, etc.) and it knows fewer organizational attachments. Responsibility for those data is now far more difficult to locate. The pervasiveness and adaptability of the new technologies makes it increasingly difficult to determine which organizations in which location "hold" personal data and, therefore, which rules (if any) apply.

Standards by which the appropriate processing of personal information are judged are therefore increasingly complex and often reliant on careful and systematic research about how new technologies are, and may be, applied. And the more one knows about smart cards, cookies, biometrics, video-surveillance and so on, the more one realizes that none of these technologies is inherently privacy invasive. Judgements about unreasonable surveillance are always contingent on the context in which they are used and applied. Each privacy issue needs, therefore, to be judged on a case-by-case basis, requiring a careful and nuanced understanding of the technology concerned and the organizational context in which it is being used. In-depth knowledge of organizational and technological practices often produces an appreciation of the other side of the story, and more pragmatic judgements.

Finally, when more pressing programmatic goals override privacy protection (and they often do), then agencies have a wide latitude to treat the issue in a perfunctory manner. The perennial problem is that privacy can always be subordinated to other social and political goals and interests. Despite opinion polls to the contrary, voters and their elected representatives tend to be more concerned about effective law enforcement, national security, the efficient delivery of services, the responsible management of the government deficit, managed health care, and so on. Collective demands and interests still sustain the actors, policies and institutions of the Canadian state. And it is exactly these more collective policies that require the effective management of personal information and which then clash with the values that
are embraced by the term "privacy." This tension will subsume the implementation of privacy protection policy to a range of collective interests that provide more short-term benefits to elected and unelected public officials of all political persuasions. The contemporary debates about the appropriate security response to the tragic events of 11 September 2001 are just the latest manifestation of the continuous and pragmatic relegation of privacy protection to collective interests that capture the attention of the public and the governments which they elect.

On a larger theoretical level, the successful implementation of privacy protection policy involves a considerable degree of learning and mutual adjustment and readjustment. It is not characterized by a top-down process of command, control and sanction.

The foregoing review demonstrates that the privacy commissioner is ombudsman, auditor, consultant, educator, policy adviser, regulator and judge. Yet, the analysis of the experience of many privacy and data-protection agencies, in Canada and overseas, suggests that the most important powers are those that are general rather than specific, and proactive rather than reactive.\textsuperscript{54} The implementation of privacy protection law is as much an educational effort as a regulatory one; as much can be achieved in anticipation of policy and system development if privacy protection is built in at the outset rather than "added on" afterwards. Yet, the two laws would give the impression that the privacy commissioner's role is predominantly confined to the first, that of a complaints receiver and adjudicator. The structure of these laws tends to put their emphasis on complaints-resolution, a function that is less useful in promoting general compliance with the privacy principles.\textsuperscript{55}

On a larger theoretical level, the successful implementation of privacy protection policy involves a considerable degree of learning and mutual adjustment and readjustment. It is not characterized by a top-down process of command, control and sanction: "data protection should not be seen as a system producing outputs and outcomes, but as a process that involves organizational change and learning and that involves a large implementation network of persons and organizations engaged in the co-production of data protection."\textsuperscript{56} The privacy commissioner cannot be a lonely figure sitting in Ottawa issuing commands. He is one among many actors involved in privacy protection policy in Canada, and his success is dependent on the recognition that he has many policy instruments at his disposal, besides the law, to encourage a greater responsibility for the treatment of personal information by Canadian organizations.
Notes

7 In April 2000, I chaired a panel “Privacy Commissioners: Powermongers, Pragmatists, or Patsies?” at the “Computer Freedom Privacy” conference in Toronto at which commissioners from Ontario, Berlin, Australia and Hong Kong discussed their strategies for ensuring privacy compliance.
10 The influential Information Highway Advisory Council called on the federal government to “create a level playing field for the protection of personal information on the Information Highway by developing and implementing a flexible legislative framework for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA Model Code, while allowing the flexibility to determine how they will refine their own codes.” Information Highway Advisory Council, *Connection, Community, Content: The Challenge of the Information Highway* (Ottawa: Supply and Services Canada, 1995), p. 141.
13 The PIDEDA, for instance, is based on the Model Code for the Protection of Personal Information, negotiated in 1996 by the Canadian Standards Association. The standard is based on ten information-privacy principles: It requires companies to accept accountability for the personal information under their control; to identify the purposes for which that information is collected; to only collect personal information with the knowledge and consent of the individual; to limit collection to that which is necessary for the purposes; to not use that information for further purposes without consent; to maintain only accurate, complete and up-to-date information; to establish appropriate safeguards; to be open about policies and practices; to allow the individual a right of access and correction; and to have a process by which individuals can challenge compliance. Similar principles are found in the Privacy Act.
15 At writing, George Radwanski had been facing tough questions from the house government operations committee about the scale of his spending, especially on foreign travel. Paco Francoli, “Radwanski hauled before gov’t ops committee,” The Hill Times (Ottawa), 9 June 2003.


19 Privacy Act, Section 35 (1).

20 Speech to the Centrum Conference on Bill C-6, Toronto, 10 December 1999, at http://www.privcom.gc.ca/english/02_05_a_991210_e.htm.


23 The emphasis on mediation to settle requests for access and correction of personal information is also apparent in the provincial legislation in B.C., Ontario and Alberta. Mediation has become a standard operating procedure in the administration of these laws before the commissioner conducts an oral or written inquiry. However, provincial commissioners also have explicit-order making powers.


25 David Flaherty, when commissioner in B.C., instigated a series of informal and supposedly non-threatening “site visits” to many of the larger public institutions in the province.


27 Colin J. Bennett, Implementing Privacy Codes of Practice: A Report to the Canadian Standards Association (Rexdale, Ont.: CSA, PLUS 8830, 1995).

28 B.C. FOIPPA, Section 42 (1)(c); Alberta FOIPPA, Section 51 (1)(c); Ontario FOIPPA, Section 59 (e).


30 See, for example, Your Privacy Responsibilities: A Guide for Businesses and Organizations to Canada's Personal Information and Electronic Documents Act, at http://www.privcom.gc.ca/information/guide_e.asp.

31 B.C. FOIPPA, Section 42 (f) (g) (h); Alberta FOIPPA, Section 51 (1) (g)(h); Ontario FOIPPA, Section 59 (a).

32 Privacy Act, Section 39 (1).


39 Flaherty, Protecting Privacy in Surveillance Societies, p. 391.
mation/speech/02_05_a_011001_e.asp.
speech/ 02_05_a_010702_e.asp.
43 See, for example, a February 2003 speech by Bruce Phillips at http://www.mser.gov.bc.ca/
44 Bill Curry, “Radwanski under political fire,” The Hill Times (Ottawa), 27 May 2002.
45 Published on the National Privacy Coalition listserver, 6 April 2001.
46 See http://www.privcom.gc.ca/wn_e.asp.
47 See http://www.privcom.gc.ca/media/nt-c/02_05_b_010718_e.asp.
48 See www.piac.ca.
49 George Radwanski has been critical of virtually every new proposal introduced in the wake
of 11 September 2001: the new procedures for the detention of individuals suspected of “ter-
rorist” activities; the “Lawful Access” proposals for the interception of communications; as
well as the extensive changes in the surveillance of travellers to and from Canada. See the
news releases at http://www.privcom.gc.ca/media/nt-c_e.asp.
50 See the text of note 10 above.
51 See http://www.privcom.gc.ca/media/nt-c/nt_010620_e.asp.
54 See Flaherty, Protection Privacy in Surveillance Societies; and Bennett and Raab, The Governance
of Privacy, Chapter 5.
55 I argued this point in my testimony before the standing committee on industry on Bill C-54
in February 1999. See also “The First Year of the Personal Information Protection and Elec-
tronic Documents Act: Was This The Way It Was Supposed to Be?” Address to FIPA confer-
56 Charles D. Raab and Colin J. Bennett, “Taking the measure of privacy: Can data protection
be evaluated?” International Review of Administrative Sciences 62, no. 4 (December 1996),
p. 553.