Privacy Protection

Beyond the Blueprint

Paul-André Comeau
École nationale d'administration publique
Québec

2009

Commission d'accès à l'information du Québec
www.cai.gouv.qc.ca

Ombudsman
www.gnb.ca

Office of the Privacy Commissioner of Canada
www.priv.gc.ca

TABLE OF CONTENTS

MESSAGE FROM JENNIFER STODDART, COMMISSIONER, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA

From September 25 to 28, 2007, Canada hosted the 29th International Conference of Data Protection and Privacy Commissioners. During the conference, which I hosted under the theme *Terra Incognita*, many of us saw an urgent need for some kind of formal learning on the subject. Following the first Conference of Francophonie Personal Data Protection Commissioners, also held in Montreal, on September 24, 2007, and hosted by Jacques Saint-Laurent, President of the Commission d'accès à l'information du Québec, we found that the cooperation and sharing created by the Association francophone des autorités de protection des données personnelles (AFAPDP) provided the ideal conditions for promoting the pluralism and diversity of Canadian institutional models.

Contributing to formal education is precisely the objective of the work undertaken by Paul-André Comeau, the author of this report, who received funding and support from the Commission d'accès à l'information du Québec, the Office of the Ombudsman of New Brunswick and the Office of the Privacy Commissioner of Canada.

We hope that readers will take some central ideas from the report, particularly the importance of dynamic institutions in a constantly changing field and a range of effective models for protecting privacy rights.

We hope that this report sparks a dialogue among all those involved in establishing what forms privacy should take in the face of globalization, information technology, and the new security, health and social justice environments.

Jennifer Stoddart

MESSAGE FROM JACQUES SAINT-LAURENT, PRESIDENT OF THE COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC

Globalization of information technologies is a fundamental component of economic growth and a major driver of activity. However, in allowing ourselves to be dazzled by the ability of information technologies to make borders and time zones disappear, we forget that those same technologies can also pose a threat to our most basic democratic values.

Through the globalization of information flows, countries lose some of their sovereignty over privacy and personal information protection. Increasing the number of independent authorities charged with monitoring and enforcing privacy legislation in each country is thus very desirable. As a result, legislation and independent control authorities have become the fundamental components of the right to protection of information in democratic societies.

When a society proposes to establish a system for the protection of privacy and personal information, it would do well to consider the decisions made by countries that already have such regimes in place.

For the member countries of La Francophonie that are seeking to respond in a positive manner to the demands of democracy by developing privacy and personal information legislation, we humbly present this document, which analyses the laws in effect in French-speaking Canada.

It is against this backdrop that the report prepared by Paul-André Comeau is situated. His aim is to provide food for thought and contribute to the search for solutions that take into account the historical and institutional characteristics of the cultural heritage of societies grappling with the need to protect the personal information of their citizens.

This report also serves to mark the first anniversary of the *Association francophone des autorités de protection des données personnelles* (AFAPDP) and comes on the heels of the 2nd Francophonie Data Protection Commissioners' Conference, held in Strasbourg on October 17, 2008.

Barely one year after submitting his report entitled *Control Authorities: Personal Information in the French-speaking World*, prepared on behalf of the Privacy Commissioner of Canada, Paul-André Comeau is back with another study that will prove just as constructive for the French-speaking community thanks to its perspicacious analysis and its skilful approach to an ever-changing field.

It is our hope that political officials, civil society representatives, and the citizens and governments of La Francophonie member countries pondering the overarching issue of privacy and personal information will find much of value in this report.

Lastly, I would like to extend my sincere thanks to Paul-André Comeau and his associates for presenting this work.

Jacques Saint-Laurent
Quebec, February 26th 2009

MESSAGE FROM BERNARD RICHARD, OMBUDSMAN, OFFICE OF THE OMBUDSMAN OF NEW BRUNSWICK

Ever since the Bamako Convention, the Francophonie has become an ideal forum for democratic development. We believe that in the digital age, it is more important than ever before that respect for the rule of law be firmly anchored in the rights to privacy and access to information. This is why the Office of the Ombudsman of New Brunswick readily supported the Association francophone des autorités de protection des données personnelles (AFAPDP) project since the Monaco Declaration, the founding conference in Montreal and subsequent activities. Through its actions, the AFAPDF will allow French-speaking nations to continue to be pioneers in this area of emerging rights that is so closely tied to economic, social and democratic development.

I am delighted to share with you, my Canadian colleagues, three institutional models that are very different yet still compatible and effective in terms of promoting and protecting the privacy of Canadians. I am sure that Paul-André Comeau's reports and analysis will be great help to all those in the Francophonie and elsewhere interested in advancing their own national legislation in these areas.

New Brunswick law on these issues continues to develop, and recent trends have confirmed that access to information and privacy are closely linked to essential safeguards against impunity and abuse of authority.

We would all benefit from learning from one another and pooling our knowledge and experience, all the more so since technology is progressing at a rate that surpasses our individual institutional capacities, both large and small. It is in this spirit of cooperation that we will be presenting this work. We hope that it will help strengthen our existing institutional ties and forge new ones.

Bernard Richard
Ombudsman

THREE ISSUES, THREE SOLUTIONS

For years, large numbers of files have been added to and retained in exempt data banks held by the Royal Canadian Mounted Police (RCMP) when they did not belong there. Citizens' names can end up in these top-secret files as the result of mistakes, administrative oversight, or even suspicions. Such was the alarming finding made by the Privacy Commissioner of Canada following an audit of these personal data banks sheltered from public access. The audit was conducted by the Office of the Privacy Commissioner in fall 2007 and winter 2008. These data banks are exempt from information requests because, in theory, they contain information pertaining to crime and matters of national security. In the days following the tabling of the Commissioner's report in the House of Commons, the RCMP publicly declared that it planned to implement all of the Commissioner's recommendations. Accordingly, the RCMP announced that it would immediately remove from these secret data banks files that had been compiled in the wake of the events of September 11, 2001, and no longer met national security criteria.

Personal information of more than 485 New Brunswick residents and 149 British Columbia residents went missing in fall 2007, including their name, gender, date of birth and health card number—exactly what is needed to commit identity theft, one of the major problems in this early part of the 21st century. The Office of the Information and Privacy Commissioner of British Columbia and the New Brunswick Ombudsman both investigated the disappearance of the information, which was to have been sent from Fredericton to Vancouver. The data, compiled by the New Brunswick Department of Health, had been stored on computer cartridges, a common practice that had never been questioned. The investigation by the New Brunswick Ombudsman uncovered the absence of even the most basic security measures.[1] For example, the data had not been encrypted in any way. As a result of the incident the Department had to contact each affected individual and set up a rapid response system in case of identify theft, with credit monitoring a particular concern.

A divorcing father asked for a complete copy of his personal file and the file of the child over whom he continued to have parental authority. His request was directed to a private-sector agency tasked by public authorities with arranging and supervising parents' right of visitation with their minor-age child. When the agency would not accede to his request, the father turned to the Commission d'accès à l'information du Québec. At a due hearing of the parties, the petitioner and agency representatives presented their arguments before the appointed Commissioner. After examining the file at the heart of the dispute, the Commissioner determined that the information it contained did indeed concern both father and child. It was personal

[1] Investigation into Lost Personal Information by the Department of Health – Medicare Billing Cartridges, April 2008: 14 pages. Reference: NBPPIA–2008–01.

information that was available to the father by law as holder of parental authority. The Commission therefore ordered that the file be turned over to the petitioner.[2]

[2] *Boudreau v. Maison de la famille DVS*, Commission d'accès à l'information (C.A.I.), 04 12 89, SOQUIJ AZ-50339620.

Introduction

Privacy issues are common news fodder. Some cases are mind-boggling and span the globe; for example, there was the disappearance of data on millions of British citizens in the winter of 2008. Often, they are isolated incidents whose consequences are no less unfortunate for their victims.

These problems and incidents stem indirectly from an imperative of life in society: the need to collect personal information for purposes that can seem disarmingly trivial. From the issuance of driver's licences to the delivery of household appliances, the reasons for disclosing basic information are multiplying on a daily basis and on a global scale. On the flipside, data gathering such as this can have unforeseeable consequences in the face of negligence or malevolent acts.

How can we cope with the demands of modern life and protect this information, which range from ordinary mailing addresses to medical information and identifiers that provide access to services such as social security and credit card numbers? This question is prompting more and more countries on virtually every continent to establish privacy legislation.

Is it possible to facilitate an understanding of the fundamental goals inherent in the adoption of such legislation? Is it possible to propose benchmarks in order to inspire the creation of control authorities that can ensure compliance with the principles and procedures in this field? Such questions inevitably arise when the establishment of a personal information protection regime is being considered within a society. The impetus may come from civil society or from the political and administrative framework. It may also be driven by an international authority, as was the case for countries in eastern and central Europe during negotiations over their entry into the European Union.

Rather than propose a theoretical process (which would still be highly useful), this report will draw on the experience of the founding Canadian members of the *Association francophone des autorités de protection des données personnelles*, namely, the federal government and the provinces of Quebec and New Brunswick. The goal here is not to retrace the history of those three entities with regard to the implementation and oversight of this new legislation. Instead, this report will succinctly examine the choices that were made and the mechanisms that were crafted by these three jurisdictions as a privacy framework. The objective is to provide food for thought and contribute to the search for solutions that take into account the historical and institutional characteristics of the cultural heritage of societies grappling with the protection—and the need to protect—the personal information of its citizens.

This report will favour a relatively simple approach by taking a chronological look at these three privacy legislation frameworks. Out of necessity we will begin by reviewing the circumstances surrounding, and the reasons behind, the adoption of such regimes, which will also shed light on the role of the various players and, where applicable, outside influences.

Similarly, we will look at the creation and implementation of what are referred to today as "control authorities." This approach is indeed comparative in nature, in that institutional heritage and legal traditions have to be taken into consideration in order to appraise the nature and powers of these entities.

How do these privacy regimes meet today's challenges, which arise, among other things, from the ramifications of globalization, the incredible impact of new information technologies, and the 9/11 shockwave, in US?

Where is our place in this uncertain trend? How can we propose solutions and accommodations that ensure the initial goal will live on as it must in societies having already put such regimes into place? How can countries that are asked—urged even—to embark on this same course begin their thought process today? How can Canadian models be of assistance to them? These questions are in fact addressed to all societies wishing to provide their citizens with assurances that an integral part of their core individuality will be protected. While this aim is ambitious, the tack taken is more modest. We will primarily be reviewing the choices made and the actions taken by the federal government, the province of Quebec, and the province of New Brunswick.

This report seeks to propose ideas for further consideration and to suggest processes that could lead to legislative and institutional mechanisms for privacy protection.

The author wishes to sincerely thank Maxime Laverdière, Esq., and Marie-Pierre Busson for their invaluable assistance.

1. CIRCUMSTANCES AND PROPOSAL

Contrary to Western Europe, privacy protection was established in Canada in two stages. In the beginning—that is, in the 1970s—only the public sector came within the sights of proponents of such initiatives. The movement emerged in government at the federal level and in Quebec at roughly the same time and gave rise to virtually simultaneous legislation in both cases. It would be some 20 years before there would be legislative measures targeting the private sector.

This movement was accompanied by efforts to adopt regimes governing access to information, or more specifically, access to records held by the public administration.[3] Protection and access initiatives are closely connected, at least where projects and tangible measures are concerned, even though at first blush the two undertakings may seem to have opposing aims, with the transparency inherent in access to information possibly working against protection of personal information. Further, the governments in question tended to emulate each other somewhat in that regard.

1.1 The Public Sector

Not surprisingly, the introduction and proliferation of computers in government gave rise to a certain degree of uneasiness regarding the protection of personal information or, more broadly, privacy. Computers and their potential, the scope of which people had only begun to suspect, were an object of concern at least in a number of countries on both sides of the Atlantic, in the US, Sweden and Germany.

Two international organizations, one headquartered in Paris and the other in Strasburg, embarked on their own projects in that same field in the late 1970s. The Council of Europe developed and submitted for ratification the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*.[4] The treaty, now referred to as Convention 108, contains binding provisions. For its part, the OECD developed and released in 1980 its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,*[5] which serve strictly to provide guidance. It is in their wake that the three jurisdictions in Canada took their first steps.

[3] These regimes, inspired by a quest for administrative transparency, are concerned with records held by the various components of the political apparatus. The now accepted expression "access to information" is patterned after "freedom of information".
[4] Council of Europe, *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, January 28, 1981, S.T.E. 108.
[5] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980.

The tone had been set in 1973 following the release of *Privacy and Computers,*[6] a study commissioned by the Government of Canada. Work continued in government for a few years after that, and the first tangible proposals emerged. The civil servants in charge of the file were obviously in tune with what was happening elsewhere, beginning with the United States, which embarked on a process to protect personal information through legislative means in 1974.

A few MPs and former ministers took over the helm to give substance to the objective of a form of protection tentatively initiated in 1977 in the *Canadian Human Rights Act.*[7] The current *Privacy Act*[8] was passed in 1982. The Parliament of Canada therefore adopted two successive pieces of legislation to enact measures and provisions governing the public sector.

The process in Quebec was similar, save for the fact that political leaders spearheaded the file. The minister responsible for institutional reform launched within government a proposal for equipping Quebec with access-to-information legislation. California would be the most direct source of influence in that field. The file was subsequently taken over by Premier René Lévesque, who had been deeply affected by the Watergate affair and the ensuing resignation of US President Richard Nixon. Aside from a few demands made by the fledgling *Fédération professionnelle des journalistes du Québec*, the process was exclusively driven by the political class.

To make this proposal a reality, the government charged a task force, chaired by an eminent journalist, with studying the issue of access to information. In fact, the task force had a dual mandate, as it also had to examine the issue of protection of personal information. That decision can be attributed to a form of emulation following the passage by the Parliament of Canada of the Act of 1977[9], which laid the foundation for the regime governing the protection of personal information.

The task force, set up in 1980, got the job done. After eight months of deliberations, it tabled a comprehensive report in which it recommended the adoption of legislation governing both access to information and protection of personal information. Surprisingly, the task force took the initiative of including a draft bill with its report. It would take Quebec's National Assembly a few months to review the report and ultimately adopt in 1982 the *Act respecting access to documents held by public bodies and the protection of personal information.*[10] With it, Quebec became the fourth province in Canada after Nova Scotia, New Brunswick, and Newfoundland to legislate access to information but the first to take such a step regarding protection of personal information, within a single piece of framework legislation. Quebec's legislative model would subsequently be emulated by other governments.

1.2 The Private Sector

Quebec also holds the distinction of launching in the early 1990s the movement to extend protection of personal information to the private sector. Internal factors and international developments converged, leading Quebec to set a precedent in North America.

[6] Department of Communications and Department of Justice, *Privacy and Computers: Report of the Task Force*, Ottawa, Information Canada, 1972.
[7] *Canadian Human Rights Act*, R.S.C. 1985, c. H-6.
[8] *Privacy Act*, R.S.C. 1985, c. P-21.
[9] Ibid.
[10] *An Act respecting access to documents held by public bodies and the protection of personal information*, R.S.Q., c. A-2.1.

The trigger for this movement was the overhaul of the *Civil Code of Quebec*, completed in 1994. The newly revamped Civil Code, which sets Quebec apart from the other provinces in the Canadian federation, guarantees each person respect for his or her privacy and protection of his or her personal information.[11] It in fact clarifies the principles previously recognized in Quebec's *Charter of human rights and freedoms,*[12] adopted in 1975. Within government, there quickly emerged a movement to craft legislation with a view to framing protection of personal information in the private sector.

At the same time, the European Union, seeking to finalize the Common Market, laid the foundation that would lead to adopting a directive aimed at standardizing the protection of personal information in each member state.[13] The proceedings in Brussels caught Quebec's eye immediately, especially since the proposed directive was to include an external component whereby the flow of personal information to and from countries outside the European Union would be subject to a series of conditions to maintain the level of protection afforded by the member countries. It was a major signal just as globalization was beginning to take shape.

Through parliamentary proceedings in which large numbers of representatives from the private sector and civil society took part and made their views known, Quebec's National Assembly fine-tuned what would become in 1993 the first piece of legislation in North America governing the protection of personal information in the private sector.[14]

The work being done in the European Union was being closely watched by the federal government. Similarly, the precedent set by Quebec raised a number of questions that would lead to what were also novel initiatives. Those reflections arose against a backdrop of almost frenetic activity in the face of the promises and challenges of the imminent implementation of what was referred to at the time as the "information highway," an expression that captured one of the fundamental aspects of the rollout of the new information and communication technologies.

The federal government had to consider opposing initiatives regarding the fate of personal information in cyberspace. Civil society and control authorities in a few provinces favoured the adoption of formal legislation. Conversely, the private sector, including the business community, was in favour of self-regulation and designated the Canadian Standards Association (CSA) to pilot the process.

There began on both sides a veritable race to come up with a tangible proposal that everyone could agree on. For its part, the government began working to draft legislation, whereas the private sector proposed a code developed following intensive deliberations within the CSA.

Self-regulation or legislative control? The federal government would ultimately decide in favour of a legislative approach incorporating the standards and principles hammered out and approved by CSA members. Thus was born the *Personal Information Protection and Electronic Documents Act,*[15] adopted by the Parliament of Canada in 2000.

[11] Arts. 35 to 41, *C.C.Q.*
[12] *Charter of human rights and freedoms*, R.S.Q., c. C-12.
[13] EC, *Directive 95/46/CE of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] J.O.L. 281/31.
[14] *An Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1.
[15] *Personal Information Protection and Electronic Documents Act*, R.S.C. 2000, c. P-8.6.

That legislation would give rise to a series of initiatives in other provinces in Canada. Taking Quebec's lead, Alberta[16] and British Columbia[17] would pass legislation governing the fate of personal information throughout the private sector.

New Brunswick's legislation on the protection of personal information owes its origins more or less to those same influences across the Atlantic. While New Brunswick did enact a *Right to Information Act* in 1978 providing for recourse to the Ombudsman or the Superior Court, it was, however, one of the last provinces to legislate the protection of personal information. In 1994, the government set up a task force to take a closer look at the entire issue.

The task force members, noting the coming into force of Quebec's legislation in 1993, made the following interim finding: "While the Task Force is not recommending legislation of the private sector it is important that these trends be monitored, particularly to ensure that New Brunswick is not at a competitive disadvantage in the information economy." Accordingly, the task force called for the adoption of legislation governing the public sector alone and self-regulation in the private sector.[18]

In 1996 the Department of Justice made public the highlights of a draft bill on the protection of personal information, in line with the principles set forth by the OECD. It also endorsed the findings of the Canadian Standards Association, which had just finalized its 10-point code.

Lastly, in 1998, the Legislative Assembly adopted legislation governing the public sector alone.[19] However, the new legislation did not come into force until 2001 following a change of government in Fredericton. In terms of both form and content, the legislation is much closer to the federal legislation governing the private sector than to any other Canadian legislation covering the public sector. It is even more succinct, and it simply enacts the OECD and CSA standards in a statutory code and provides for recourse in the form of complaints to the Ombudsman. There is no *a priori* control of how data is handled by the public sector. There is also no general audit system. The mechanism was meant to be flexible and easily transferable to the private sector if the latter failed to voluntarily follow in the government's footsteps. However, even before the legislation could be enacted, the federal government bowed to the pressure of the European directive and decided otherwise. Therefore, the federal legislation applied henceforth to New Brunswick's private sector.

Early legislative attempts in both Ottawa and Quebec City were framed by a quasi-constitutional structure and were aimed at protecting the fundamental right to privacy. Economic conditions and the growth of computerization and markets fuelled other specialized legislation on privacy in relation to information. At the federal level, the Minister of Industry continued to be in charge of the file. In New Brunswick, management and follow-up leading to adoption of the draft bill was the responsibility of the Information Highway Secretariat, a branch of the Department of Economic Development. This explains in part Canada's less interventionist approach and the absence of any New Brunswick legislation governing the private sector. Had it not been for the federal government's legislative intervention, the province would have undoubtedly relied longer on the virtues of self-regulation.

[16] *Personal Information Protection Act*, S.A. 2003, c. P-6.5.
[17] *Personal Information Protection Act*, S.B.C. 2003, c. 63.
[18] New Brunswick Government Task Force on Data Sharing and Protection of Personal Privacy (1994) – *Protecting Privacy in an Information-Sharing Environment: Report of the New Brunswick Government Task Force on Data Sharing and Protection of Personal Privacy,* Fredericton.
[19] *Protection of Personal Information Act*, S.N.B. 1998, c. P-19.1.

In conclusion, spurred on by domestic influences and developments on the international scene, the federal government, Quebec and New Brunswick followed basically similar paths.

In short, efforts aimed at protecting personal information recognized the value of this substantive right and incorporated it into the concept of the right to privacy. The development of that right was strongly influenced by the rising tide of computerization.

Crafting privacy legislation was in a way connected with setting up access-to-information regimes.

Contrary to what happened in Europe, protection of personal information was implemented in a two-step process, first in the public sector and then in the private sector.

2. LAWS AND THEIR INTENT

It is not surprising at all to note that the regimes for the protection of personal information instituted by Ottawa, Quebec City, and Fredericton followed not only a particular path but also specific legislative traditions. In the early 1980s, i.e. when the Parliament of Canada and Quebec's National Assembly enacted the first privacy laws in Canada, the process unfolded under precisely those conditions. There were few models to refer to, and what relatively recent examples there were came from outside Canada's borders. Flexibility would have to emerge by itself.

A review of the legislation implemented in the three political systems hinges initially on an examination of their architecture. This step is essential in order to better understand the intent and aims of the legislation. Here, too, we must defer to the chronology of the legislative initiatives that targeted the public sector alone in the beginning.

2.1 The Public Sector

In Quebec, the government quickly embraced the proposal of the task force that had been set up to do the necessary ground work. It tabled in the National Assembly a bill that combined both protection of personal information and access to information. The statute adopted in 198220 in fact set a precedent that would subsequently be referred to as the "Quebec model."

Most Canadian jurisdictions and some European countries, such as Hungary, the United Kingdom, and Switzerland, would follow in Quebec's footsteps by combining these two regimes, whose aims might seem different, if not contradictory. First, the National Assembly established transparency by acknowledging the right to access records held by components of the political system. At the same time, it afforded special protection to personal information.

A dual objective gave coherence to this legislative process: provide adequate protection for personal information and guarantee citizens access to information concerning them. That particularity noted, the *Act respecting access to documents held by public bodies and the protection of personal information* answers the fundamental questions that arise when establishing a regime for the protection of personal information: What are we trying to protect? Who will this affect? How will this objective be achieved? What recourses have been put into place to ensure compliance with the principles and provisions of the Act?

[20] *Act respecting access to documents held by public bodies and the protection of personal information*, R.S.Q., c. A-2.1.

Personal information can be defined in relatively simple terms. Basically, it is any data or symbol that identifies a person or differentiates him or her from any other person.[21] The characteristics of that person, symbols or identifiers, and information about his or her health, philosophical allegiances, and religious beliefs, to name only the most obvious, fit this generic concept.

The Act encompasses the various media on which this information may be kept, from traditional paper forms to the electronic files of our virtual era, not to mention films, videos, and other audiovisual derivatives. Such is quite simply the object of the provisions and conditions that embody the protection of personal information not only in Quebec but also in most legislation.

This legislative regime enjoys special status in Quebec's legislative machinery, as the Act takes precedence over all other provisions adopted by the National Assembly unless that provision expressly states that it applies notwithstanding this Act.[22] That constitutes an explicit expression of the rights granted to citizens under the *Charter of Human Rights and Freedoms* (1975).[23]

This regime covers the entire public sector and is not limited to the machinery of government alone. It takes in the various components of the public administration, including Crown corporations as well as the decentralized and local agencies that, for example, manage all public schools.[24]

The 1982 Act covers the various stages in the life cycle of personal information and establishes the framework for its protection, from initial collection to disposal. The principles governing the use of such personal information can be summed up schematically as follows:

- The data must be collected or produced for a very specific and explicit purpose. Further, only the information required for that purpose may be collected. It must also be ensured that the information is accurate.[25]

- Retention of the information must be accompanied by precautionary and security measures that put the information out of reach of unlawful access and inquisitive eyes.[26]

- Personal information may be used only for the purpose for which it was collected.[27]

- Any disclosure of this information to other bodies must meet specific criteria and, in certain cases, be subject to an agreement in the prescribed form.[28]

- Lastly, when the purpose for which personal information was collected has been achieved, the information must be destroyed.[29]

These principles and conditions are premised on the right of every person to have access to personal information which concerns him or her and is held by any public body.[30] This right does

[21] Ibid., s. 54.
[22] Ibid., s. 168.
[23] *Charter of human rights and freedoms*, R.S.Q., c. C-12.
[24] *Act respecting access to documents held by public bodies and the protection of personal information*, *supra* note 20, ss. 3 to 7.
[25] Ibid., in particular ss. 64 and 72.
[26] Ibid., ss. 63.1 and 63.2.
[27] Ibid., s. 65.1.
[28] Ibid., ss. 64 to 70.
[29] Ibid., s. 73.
[30] Ibid., s. 83 et seq.

not extend to exceptional files that may be excluded following a special procedure.[31] Lastly, a person may request that personal information concerning him or her be corrected if the information is inaccurate, incorrect or false.[32]

Citizens may also avail themselves of specific recourses to enforce the rights afforded them under the Act. Those recourses may ultimately and solely be exercised with the Commission d'accès à l'information,[33] whose status is that of an administrative tribunal and which, as its name indicates, also has responsibilities regarding access to information.

That, in a nutshell, is the framework of the Act which, it must be noted, encompasses both protection of personal information and access to information in the public sector.

A few weeks after the adoption of this Act by Quebec's National Assembly, the Parliament of Canada passed similar legislation for the protection of personal information in government.[34] In so doing it also approved legislation instituting a regime governing access to information.

The *Privacy Act* shares the same general objectives. It reflects the style of legislation adopted by the Parliament of Canada. Consequently, "personal information" is defined by a long list that specifies its scope.[35] For example, it includes a person's blood group, criminal record, and correspondence with a federal institution.

The Act must be implemented by all departments, ministries of state, and federal institutions expressly named in a schedule.[36]

Similarly, it establishes the requirements for the protection of personal information based on the life cycle of the information, from its collection to its disposal or transfer to the National Archives of Canada. No personal information may be collected or used unless it relates to the aims of the programs administered by the departments or agencies.[37] Those measures frame as it were the way in which agencies must undertake these various phases, including the establishment of data banks in which this personal information is stored.

Lastly, Canadian citizens, permanent residents, and any person present in Canada have a right to be given access to and correct personal information concerning them, and they alone may exercise that right.[38] A significant exception is made for federal Members of Parliament to allow them to obtain information on a constituent requesting special action in order to resolve a problem.[39] However, certain so-called exempt banks,[40] such as those that may be established by the Royal Canadian Mounted Police, are sheltered from access.

Any problems or disputes arising from the exercise of this right of access may be brought before the Privacy Commissioner. The incumbent of this office, a specialized ombudsman, can issue recommendations following an investigation of such complaints.[41]

---

[31] Ibid., ss. 80 to 82 and 86.
[32] Ibid., s. 89 et seq.
[33] Ibid., s. 134.2.
[34] *Privacy Act*, R.S.C. 1985, c. P-21.
[35] Ibid., s. 3, *s.v.* "personal information".
[36] Ibid., *s.v.* "federal institution"; see also Ibid., schedule.
[37] Ibid., ss. 4 to 6.
[38] Ibid., s. 12.
[39] Ibid., s. 8(2)(*g*).
[40] Ibid., s. 18.
[41] Ibid., ss. 29 to 35.

In short, both regimes for the protection of personal information were established at the same time and have obvious similarities. They concern only the public sector, unlike the legislation adopted in Western Europe in the 1970s and 1980s.

2.2 Private Sector

In North America, Quebec would launch the movement to extend the system for the protection of personal information to the private sector. The process originated in the reform of the *Civil Code*, in which the principles of personal information protection are expressly set out and guaranteed.[42]

After examining various options gleaned from experiments conducted in other countries, Quebec decided in favour of continuity. The *Act respecting the protection of personal information in the private sector,*[43] adopted in 1993*,* follows the path charted by the National Assembly a decade earlier. It also meets the requirements stipulated by the OECD in its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,*[44] enacted in 1980.

The broad and generic notion of "personal information" did not differ from that which had been decided upon in 1982: personal information was any information that could identify a person, regardless of the medium on which the information was stored.[45]

"Enterprises" established in Quebec or that conduct business in the province are subject to the legislation.[46] Under the *Civil Code*, the carrying on of an enterprise is the key criterion for establishing the scope of application of the Act.[47] In the same vein, virtually all organizations, bodies, and agencies that collect, retain and use personal information are included in the enterprise category.

These enterprises must adhere to the principles and conditions governing the use of personal information set out in the Act. These principles and conditions do not differ significantly from those implemented for the public sector.

In a significant innovation, the 1993 Act addresses the issue of the transfer outside Quebec of personal information held by bodies in the private sector.[48] The latter are obliged to ensure that information collected is used only for its intended purpose outside the province's borders. In a way, the provision addresses the concerns that prevailed in the field when the European Union established its directive in 1995.

Every person has the right to access information which concerns him or her and is held by any enterprise, as defined in the *Civil Code*.[49] By conferring upon the Commission d'accès à l'information du Québec the exclusive mandate to resolve disputes[50] that may arise from this right of access (or "disagreements", which was the term decided upon), the National Assembly in a way unified the system for the protection of personal information.

---

[42] Arts. 35 to 41, *C.C.Q.*
[43] *Act respecting the protection of personal information in the private sector*, R.S.Q., c. P-39.1.
[44] Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, September 23, 1980.
[45] *Act respecting the protection of personal information in the private sector,* note 43, s. 2.
[46] Ibid., s. 4.
[47] Art. 1525, para. 3, *C.C.Q.*
[48] *Act respecting the protection of personal information in the private sector*, *supra* note 43, s. 17.
[49] Ibid., s. 27 and ss.; see also art. 1525, para. 3, *C.C.Q*.
[50] *Act respecting access to documents held by public bodies and the protection of personal information*, *supra* note 20, s. 134.2.

In the federal arena, the movement took a different—and very novel—path. The new Act resulted from a collaborative effort with the private sector. It bore the imprint of the impact of new technologies. And lastly, adoption of the legislation stemmed from a choice based on the constitutional regime of the Canadian federation.
The *Personal Information Protection and Electronic Documents Act* (2000)[51] is concerned with exactly the same kind of information that can identify a person.[52] The concept remains broad and comprehensive. Nonetheless, Parliament accorded special attention to personal health information, reflecting in fact, in a very specific field, the concept and reality of so-called sensitive information embodied in most European legislation.

The question of "electronic" media, the foundation for this legislative process, is given rather specific treatment. The Act explains concepts pertaining to the nature of electronic documents, electronic signatures, and electronic payments, to name but these aspects.[53]

And who should be responsible for implementing and enforcing this Act? That question forced the Parliament of Canada to reconcile its goals with the characteristics of Canada's constitution regarding the sharing of jurisdiction between the federal parliament and the provincial legislative assemblies. The federal parliament was chosen on the basis of the powers granted to the federal government in the area of interprovincial trade.[54]

Accordingly, the Act applies to organizations that come under the legislative jurisdiction of the Parliament of Canada, such as banks, radio and television stations, and, broadly, corporations that carry on business in two or more provinces.[55]

In a significant innovation that surprised many a jurist, the principles for application of the legislation were set out in a schedule to the Act itself.[56] It is in fact the Model Code for the Protection of Personal Information, which was developed and negotiated by the Canadian Standards Association. The Code bears little resemblance to a legal document; it even contains examples and recommendations. The Code was inspired by the principles laid down by the OECD in its *Guidelines* of 1980, mentioned previously.

The Code consists in a set of ten principles. It sets out the conditions that must henceforth be met by all organizations subject to the Act.

1. **Accountability:** statement and explanation of the obligations to be met by organizations subject to the Act.

2. **Identifying Purposes:** the purposes for which personal information is collected must be identified by the organization at the time the information is collected.

3. **Consent:** this principle must govern the collection of information. It also clarifies procedures and the nature of the consent to be obtained from the individual.

---

[51] *Personal Information Protection and Electronic Documents Act*, R.S.C. 2000, c. P-8.6.
[52] Ibid., s. 2, *s.v.* "personal information" and "personal health information".
[53] Ibid., Part 2; see in particular Ibid., s. 31.
[54] That choice is also the subject of an action brought before the Quebec Court of Appeal by the Government of Quebec. In the latter's view, the federal government has encroached upon an area of jurisdiction that is exclusive to it. Briefly, the Government of Quebec maintains that legislation governing personal information is the preserve of the National Assembly, as the matter is covered by the *Civil Code*.
[55] *Personal Information Protection and Electronic Documents Act*, *supra* note 51, s. 4; In fact, the federal legislation covers those bodies under federal jurisdiction pursuant to section 91 of the *Constitution Act of 1867* (U.K.), 30 & 31 Victoria, c. 3, reproduced in R.S.C. 1985, Second Schedule, no. 5.
[56] *Personal Information Protection and Electronic Documents Act*, *supra* note 51, Schedule 1.

4. **Limiting Collection:** the collection of personal information must be limited to that which is necessary for the purposes identified by the organization.

5. **Limiting Use, Disclosure, and Retention:** the collection of information solely for the intended purposes imposes measures encompassing the life cycle and uses of personal information, including the ultimate destruction of the information.

6. **Accuracy:** one of the aims of this requirement is to prevent decisions concerning individuals from being made on the basis of inaccurate or false information.

7. **Safeguards:** the Code sets out requirements concerning the sensitivity of information that is collected and retained.

8. **Openness:** the purposes of the collection of information must be laid down in a policy statement or the like and be accessible.

9. **Individual Access:** individuals must be given access to personal information concerning them that is held by organizations.

10. **Challenging Compliance:** organizations must establish mechanisms for dealing with complaints from citizens or consumers.

While this list might seem comprehensive, it is in fact rounded off by Parliament's decision to confer upon citizens the right to refer to the Privacy Commissioner any problem or dispute they have encountered in this area.[57] Here as well, the system for protection of personal information is unified as regards compliance with the principles and obligations governing the protection of the personal information of individuals.

This legislation is very innovative in one respect when it comes to the Canadian federal context. As we have seen, it applies to all organizations that come under federal jurisdiction. This pan-Canadian aspect is coupled with a special provision. The Act applies throughout Canada, unless legislation enacted by a legislature of a province is deemed "substantially similar."[58] This aspect of equivalency has since been recognized in legislation on the subject adopted by Quebec[59] and two other provinces, Alberta[60] and British Columbia[61]. The same holds true for custodians of health information in Ontario.[62]

2.3 A Look at New Brunswick

New Brunswick's *Protection of Personal Information Act*, which covers only the public sector, was enacted in 1998.[63] It is at once a succinct, flexible, and novel piece of legislation.

While subscribing to the habitual concepts for defining "personal information," the Act is not limited solely to the objective and obvious information used to identify individuals and to

[57] Ibid., ss. 11 to 13.
[58] Ibid., s. 26(2)(*b*).
[59] *Organizations in the Province of Quebec Exemption Order*, SOR/2003-374.
[60] *Organizations in the Province of British Columbia Exemption Order*, SOR/2004-220; see also *Personal Information Protection Act*, S.B.C. 2003, c. 63.
[61] *Organizations in the Province of Alberta Exemption Order*, SOR/2004-219; see also *Personal Information Protection Act*, S.A. 2003, c. P-6.5.
[62] *Health Information Custodians in the Province of Ontario Exemption Order*, SOR/2005-399; see also *Personal Health Information Protection Act, 2004*, S.O. 2004, c. 3.
[63] *Protection of Personal Information Act,* c. P-19.1.

differentiate them from other persons. The Legislative Assembly included in this category information which, by association, would lead to such an outcome, even in the absence of the person's identity or specific data concerning him or her.

New Brunswick's statute covers all public-sector organizations already subject to the *Right to Information Act* of 1978. Consequently, there is a sort of linkage with the administrative transparency regime in place in the province for the past 30 years.

The Legislative Assembly of New Brunswick set a precedent in terms of the protection of personal information. It introduced under a "Statutory Code of Practice" a simplified version of the principles that had just been crafted by the Canadian Standards Association for private-sector enterprises. The proposal for the private sector was thus transposed onto the public sector by the Legislative Assembly. The Parliament of Canada also incorporated the original version of the same code developed by the Canadian Standards Association into its 2001 Act governing the private sector.

For its part, the Legislative Assembly in Fredericton did not impose legislation on the private sector regarding the protection of personal information. In the government's view, enterprises in the private sector had to embark on that path by voluntarily applying the same standards. They were thus encouraged, more or less explicitly, to adopt a form of self-regulation. This system of "setting a good example" would not be given a chance to prove itself. Adoption of the federal Act of 2001, which extends to all of Canada's private sector, replaced the self-regulation proposal contemplated by Fredericton.

The mandate for receiving and investigating complaints and disputes in connection with this legislation was conferred upon the Ombudsman of New Brunswick.[64] Correlative amendments guaranteeing transparency were made to the Act in order to better protect personal information. The Legislative Assembly chose to maintain two separate legislative systems for the transparency and protection of personal information. The scope of these two pieces of legislation covering the public sector, the vesting of both investigation and judicial submission functions in a single control authority, and cross-references to the principles of law established in each legislative system help to better coordinate and reconcile these two major trends in public law.

This overview sheds light on a number of characteristics of the privacy protection regimes established in the three political systems under review.

- These pieces of legislation acknowledge, as it were, the legality of the collection and use of personal information.

- They clarify and set out guidelines for the ways in which this information is to be handled, from the time it is gathered until it is destroyed.

- They are tailored to the private and public sectors.

- They guarantee citizens the right to access personal information concerning them.

- Lastly, these pieces of legislation confer upon a control authority the mandate to ensure compliance with these principles and the rights afforded citizens.

[64] Ibid., s. 3.

3. CONTROL MECHANISMS

The need to give an agency responsibility for overseeing citizens' rights regarding their personal information was virtually self-evident to the drafters of the bills conceived for the public and private sectors. The choices made by the Parliament of Canada and the legislative assemblies in Quebec and New Brunswick were in a way dictated by the establishment of an access-to-information regime.

In the late 1970s, the case review was rather limited. Barely a handful of countries had ventured along this path. The US opted for the minimalist approach, deciding that the courts would address any issues stemming from implementation of the *Privacy Act*. In Europe, France, Sweden, and the German province of Westphalia established new bodies.

3.1 The Commission d'accès à l'information du Québec

In Quebec, the government accepted the task force's recommendation and decided to entrust oversight of both the access-to-information and the privacy-protection components of the 1982 Act to a new agency, the *Commission d'accès à l'information.*

A core objective underpinned the creation of the Commission. It was given the mandate to see in a consistent manner to the inevitable arbitration between the two rights enshrined in a single piece of legislation: access to records in the public sector and protection of personal information held by entities in the public sector.

The fundamental elements of the Commission's status and powers were taken from the still recent tradition of "administrative tribunals." The *Commission d'accès à l'information du Québec*, elevated to the rank of a quasi-judicial agency, is in fact a multifunctional organization that fulfils a number of objectives in both fields.[65]

The Commission is a collegial body whose administration is entrusted to a chair, who may be seconded by a vice-chair. The Commission has a maximum of five members, whose terms may be renewed every five years.[66]

[65] This presentation concerns the powers in fact held by the Commission under the original legislation of 1982, and amendments made in 1989 and 2006.
[66] *Act respecting access to documents held by public bodies and the protection of personal information*, R.S.Q., c. A-2.1, s. 103 et seq.

The chair and members of the Commission are appointed by resolution of the National Assembly that must be approved by not less than two thirds of its members.[67] The mandate of selecting candidates following a public call for nominations was recently transferred to a committee of the National Assembly.

The Commission enjoys special status within the machinery of government. While the Commission is vested with powers inherent in its status as an administrative tribunal and is thus in that sense truly independent, it is nonetheless attached to a member of cabinet for budget purposes. The minister in question is backed by a group of civil servants tasked with identifying measures and procedures to ensure that the objectives of the law are met.

The Commission has substantive measures at its disposal to ensure compliance with the legislation throughout the public sector. It can give opinions and make recommendations covering the public sector as a whole.[68] Similarly, it is charged with promoting the objectives of the legislation among the public.[69] Lastly, it can refer important issues to the National Assembly by tabling a special report.[70]

In its day-to-day operations the Commission is divided into two branches. The mission of the first branch is to oversee implementation of the Act, while the second branch has adjudicative powers to settle disputes that may arise from citizens being denied the opportunity to have access to their personal information or to have their personal information corrected or even destroyed. This structure reflects the will of the National Assembly to make these two functions truly independent.

The so-called oversight branch is responsible for ensuring application of the procedures for protecting personal information and keeping it secure.

In the public sector, this mandate is carried out initially through the laying down of conditions that must be met regarding the creation and management of personal data banks. For study purposes the Commission may also grant researchers access to personal information without the consent of the individuals concerned—a cardinal principle of the protection of this information. Lastly, it has the right to formulate comments or even objections with regard to proposals for sharing personal information between departments, government entities, and agencies.

The oversight branch, headed by at least one Commission member, also intervenes when citizens complain about misuse of their personal information in the public and private sectors. One of the Commission's staff members may be assigned a genuine investigation mandate under the powers conferred by the Act to an investigation commissioner. He or she may demand access to all of the information needed to clarify the alleged problem. Once the investigation is complete, a Commission member takes possession of the report and must then obtain the viewpoints of the parties in question before making a decision that is binding in both the public and private sectors.

The adjudicative function is exercised when persons seeking to obtain their personal information are denied the opportunity to access that information or to have it corrected or destroyed, or, in matters of access, when requests for documents have been denied. Most of the time, a mediation process is initiated as soon as complaints are received. If no agreement can be reached, the file is entrusted to one of the Commission members, who will then hear representations from the

[67] Ibid., s. 104, para. 2.
[68] Ibid., s. 123.
[69] Ibid., s. 122.1, para. 2.
[70] Ibid., s. 133.

parties in question at a public hearing. Once this adjudicative process is complete, the Commission member issues a binding written decision. That is precisely what is shown by the case described at the start of this report, i.e. the father requesting to see his son's file.

The decisions rendered by the Commission may be appealed to the Court of Quebec as regards questions of law or jurisdiction. The National Assembly, looking to the framework in place throughout Quebec's administrative tribunals, thus built a bridge to the legal system. Subject to certain conditions, decisions rendered by the *Commission d'accès à l'information* may therefore be referred to higher tribunals.[71] This judicial framework has in fact given rise to case law on the protection of personal information.

3.2 Office of the Privacy Commissioner of Canada

During the federal legislation's development phase, jurists and experts considered the few models in place in Europe but opted instead to take their inspiration from the precedents established in Ottawa in the late 1960s and adapt the so-called ombudsman model that had been tested in particular when the position of the Commissioner of Official Languages was created.

At the time when public sector privacy legislation was adopted, there did not seem to be any hesitation as to the ultimate control authority. It followed almost as a matter of course that the Privacy Commissioner would perform this function, especially since the then-Commissioner had played a major role in the process that led to the enactment of the *Personal Information Protection and Electronic Documents Act.*

The incumbent of this office, an ombudsman or mediator, is a officer of Parliament,[72] just like the Auditor General and the Chief Electoral Officer. These individuals partake of the control mission that Parliament exercises over the government and its administrative machinery. They enjoy the prestige, immunity, and flexibility conferred upon them by the legislative branch.

The process for appointing the Privacy Commissioner has also evolved. At the Prime Minister's request, candidates for the position are heard by the Standing Committee on Access to Information, Privacy and Ethics. Candidates for the Supreme Court have recently begun following the same approach. The Privacy Commissioner has a renewable seven-year term,[73] an indication of the importance attached to this function.

With regard to protection of personal information, the Commissioner acts as advisor to the Parliament of Canada, most often before the Standing Committee on Access to Information, Privacy and Ethics. The Commissioner must also report on his or her administration to Parliament.[74]

The Commissioner exercises his or her authority in the public and private sectors in more or less the same way, by virtue of the same powers and in accordance with very similar mandates. Where the private sector is concerned, the Commissioner has been charged by the Parliament of Canada with promoting knowledge of, and compliance with, this Act,[75] hence the education and awareness campaigns aimed at organizations and enterprises subject to the Act. In the public

[71] A decision of Quebec's *Commission d'accès à l'information* was even appealed to the Supreme Court of Canada, which, in the case at issue, established that the decision was well-founded.
[72] *Privacy Act*, R.S.C. 1985, c. P-21, ss. 53 and 54.
[73] Ibid., s. 53(2).
[74] Ibid., s. 72.
[75] *Personal Information Protection and Electronic Documents Act*, R.S.C. 2000, c. P-8.6, s. 24(*a*).

sector, the Treasury Board Secretariat develops and communicates directives and policies with a view to enabling departments and agencies to fulfil their obligations.

In practical terms, the Commissioner takes action in three ways, by receiving complaints, initiating investigations, and conducting audits.
Citizens whose requests to access or correct their personal information have been rebuffed in the public or private sector may seek redress with the Commissioner.[76] Complaints may also relate to non-adherence to the principles governing the handling of personal information. The Commissioner may take it upon himself or herself to intervene and review a problem that has come to his or her attention.[77] Mediation and conciliation are the two procedures contained in the Act.

Similarly, the Commissioner may launch veritable "compliance reviews" to closely inspect how departments and agencies are ensuring implementation of the principles and rules that must govern the protection of personal information. In the private sector, "audit" was the preferred term for designating the same process.[78] It was under this authority that the current Privacy Commissioner conducted a review of the exempt data banks held by the Royal Canadian Mounted Police, as indicated at the beginning of this report.[79]

The Commissioner has significant powers to carry out these investigations and audits.[80] The Commissioner's officials may enter buildings and offices to initiate the various stages of an investigation. They may have access to all documents they deem it necessary to consult. They may also summon witnesses and question them under oath. In short, they can get to the bottom of things.

Investigations, audits, and reviews of complaints can lead to findings.[81] Like all ombudsmen, the Commissioner may only issue recommendations pursuant to complaints brought forward by citizens and his or her investigations and audits. These recommendations have an obvious moral authority, which stems from the prestige of the office and reflects the will of Parliament.

This power of recommendation has two possible extensions. Citizens who are dissatisfied with the follow-up given to the Commissioner's recommendations may initiate proceedings before the Federal Court.[82] The Commissioner may initiate a similar procedure on behalf of the citizen in question or on his or her own initiative.[83] The Commissioner may also seek the court's intervention to ensure compliance with the principles and aims of the Act.[84]
Lastly, the Commissioner may refer any of these issues to Parliament in his or her annual report.[85] The Commissioner may also table a special report in Parliament,[86] as happened in February 2008 following the Commissioner's investigation into the exempt data banks held by the

[76] *Privacy Act*, *supra* note 72, s. 29 et seq.; *Personal Information Protection and Electronic Documents Act*, *supra* note 75, s. 11 et seq.
[77] *Privacy Act*, *supra* note 72, s. 29(3); *Personal Information Protection and Electronic Documents Act*, *supra* note 75, s. 11(2).
[78] *Privacy Act*, *supra* note 72, ss. 36 and 37; *Personal Information Protection and Electronic Documents Act*, *supra* note 75, s. 18.
[79] Privacy Commissioner of Canada, *Audit Report of the Privacy Commissioner of Canada on the Examination of RCMP Exempt Data Banks*, Minister of Public Works and Government Services Canada, IP54-8/2008.
[80] *Privacy Act*, *supra* note 72, s. 34.
[81] *Privacy Act*, *supra* note 72, ss. 35 to 37; *Personal Information Protection and Electronic Documents Act*, *supra* note 75, ss. 13 and 19.
[82] *Privacy Act*, *supra* note 72, s. 41; *Personal Information Protection and Electronic Documents Act*, *supra* note 75, s. 14.
[83] *Privacy Act*, *supra* note 72, s. 42; *Personal Information Protection and Electronic Documents Act*, *supra* note 75, s. 15.
[84] Ibid.
[85] *Privacy Act*, *supra* note 72, s. 38; *Personal Information Protection and Electronic Documents Act*, *supra* note 75, s. 25.
[86] *Privacy Act*, *supra* note 72, s. 39.

Royal Canadian Mounted Police. That provides an opportunity for the Commissioner to draw the public's attention to an issue of importance.

Under the legislation governing the private sector, the Commissioner plays a very unique role where the provinces and territories are concerned. In the Commissioner's annual report, he or she can in fact mention the enactment by any legislative assembly of legislation that he or she deems "substantially similar."[87] The Commissioner may enter into agreements with the control authorities of any province or territory to ensure that personal information is afforded the same level of protection across Canada.[88]

3.3 The Ombudsman of New Brunswick

In New Brunswick, the government decided to give the province's ombudsman the mandate to oversee the new *Protection of Personal Information Act*, which covers the public sector only.[89] That was also the option chosen in 1978 when New Brunswick became the second province in Canada to adopt a regime governing access to information.[90]

Over the years, these new responsibilities were tacked on to the Ombudsman's other duties. Besides his access-to-information role, the Ombudsman also acts as Child and Youth Advocate and performs important functions in the Archives sector. In addition, the Ombudsman's office manages complaints and problems in connection with hirings and appointments within the civil service. In short, this position can aptly be described as "generalist" in nature.

Normally, the Premier calls upon the Legislative Assembly to review his or her choice of candidate for this role. The Legislative Assembly's recommendation is then forwarded to the government, which ratifies it and then proceeds with the appointment.[91]

The Ombudsman holds the status of "appointee" of the Legislative Assembly, just like the Auditor General, the Commissioner of Official Languages, the Conflict of Interest Commissioner, and the Consumer Advocate for Insurance. These "officers of the Legislative Assembly" carry out their mandate with regard to the administrative and governmental apparatus as a whole and enjoy considerable independence.

The Ombudsman's scope of action where personal information is concerned is of course circumscribed by the Act. The Ombudsman has considerable latitude in terms of the matters that he or she may review. The Ombudsman may also be instructed by the Legislative Assembly itself to launch an investigation.[92]

In the performance of his or her duties, the Ombudsman is vested with the powers of an investigation commissioner set out in a specific Act.[93] The Ombudsman has every freedom as to the choice of methods for studying problems brought before him or her. In carrying out his or her investigations, the Ombudsman may authorize his or her officials to enter buildings housing the services that are cited in a complaint or are the object of an investigation. The Ombudsman may summon and question under oath any member of the civil service and, under certain conditions, persons outside it. It was by virtue of these powers that the Ombudsman investigated the matter

[87] *Personal Information Protection and Electronic Documents Act*, *supra* note 75, s. 25.
[88] Ibid., ss. 22 and 23.
[89] *Protection of Personal Information Act*, S.N.B. 1998, c. P-19.1, s. 3.
[90] *Right to Information Act*, S.N.B. 1978, c. R-10.3, s. 7.
[91] *Ombudsman Act*, R.S.N.B. 1973, c. O-5, s. 2.
[92] Ibid., s. 13(2).
[93] Ibid., ss. 10, 17 and 20.

of the computer tapes of health information that went missing somewhere between New Brunswick and British Columbia, as recounted at the beginning of this report.[94]

Like other ombudsmen in most jurisdictions, the Ombudsman's investigations and reviews of complaints take the form of a report in which the Ombudsman can make specific and tangible recommendations.[95] The Legislative Assembly counted on the Ombudsman's moral authority to facilitate the resolution of problems and disputes that come under his or her authority. If the Ombudsman is dissatisfied with the action taken with respect to any of his or her recommendations, he or she may submit a report to the government and, if need be, to the Legislative Assembly.[96] Consequently, besides the Ombudsman's moral authority, there is also the weight of political or quasi-political intervention as a last resort.

The Ombudsman's annual report is also an opportunity to make public problems or difficulties he or she may have encountered in resolving issues he or she feels are important or exemplary or with regard to any matter of the Ombudsman's choosing.

In addition, for 30 years now, the Ombudsman has had the mandate to review petitions under the *Right to Information Act*. The Ombudsman does not have the power to issue orders but instead exercises oversight by way of recommendation.

The Ombudsman is first and foremost a parliamentary mediator who investigates complaints under the *Archives Act* and the *Civil Service Act.* As such, the Ombudsman has enjoyed a right of review over the entire administrative machinery of the provincial government for 40 years now. All public agencies are subject to the Ombudsman's oversight, and the Ombudsman may not be obstructed by any confidentiality clauses or government secrets. In that regard, the functions of information protection control officer are also ensured through the Ombudsman's experience, autonomy, and statutory, moral, and institutional independence.

The Ombudsman model also has the advantage of placing oversight of information protection in the hands of a parliamentary officer specializing in the transparency of procedural fairness and the smooth operation of government departments and agencies.

Since 2006, the Ombudsman has also played a new, specialized role as Child and Youth Advocate. In that capacity, the Ombudsman is often called upon to tackle thorny issues in which transparency objectives conflict with those of information protection, e.g., in relation to the coordination of public services for youth and their families. In such cases, the duty to maintain confidentiality is often heightened, but the best interests of a child may demand that information be shared. For those who are concerned about the prospect of excessive strictness with regard to information protection, New Brunswick's legislative model offers the advantages of a powerful, benevolent generalist. For a province with a population of some 700,000 people, that legislative model has proven to be flexible and consistent, no doubt a consequence of its being tailor-made.

From this overview of the fundamental characteristics of the control authorities put in place by Ottawa, Quebec City and Fredericton, we see that they have a number of traits in common.

[94] Ombudsman of New Brunswick, *Investigation into Lost Personal Information by the Department of Health – Medicare Billing Cartridges* (April 2008), NBPPIA-2008-01.
[95] *Ombudsman Act*, *supra* note 91, ss. 21 and 22.
[96] Ibid., s. 21(3).

- The incumbents of these three agencies are subject to a special appointment process in which the respective parliaments play a key role. That approach testifies to the importance of the office and gives the incumbents undeniable prestige.

- Similarly, the linkage of this person with the institution of parliament is explicit at the federal level and in New Brunswick. In Quebec, it is more complex. In any event, that association bestows a definite and very valuable moral authority on any measures taken by the incumbents.

- The Office of the Privacy Commissioner, the Office of the Ombudsman of New Brunswick, and the Commission d'accès à l'information du Québec have considerable powers when it comes to the steps that can be taken to resolve the problems brought to their attention.

- Lastly, with regard to the control authorities in Quebec and at the federal level, intervention by the courts, as a last resort, contributes to the development of case law bolstering the weight and scope of the principles and conditions relating to the protection of personal information.

4. IF AT FIRST YOU DON'T SUCCEED

Legislation and institutions rarely evolve along straight lines, a fact all the more true when it comes to personal information and privacy. The tremendous changes brought about by communications technologies have profoundly shaken the sectors targeted by legislation established more than 25 years ago both in Quebec and in the rest of Canada.

Over the past two years, legislation governing the protection of personal information has been systematically reviewed at the federal level and in Quebec and New Brunswick.

4.1 New Brunswick

In early June 2008, the government tabled in the Legislative Assembly a bill whose major provisions called for, among other things, the establishment of the position of information and privacy commissioner. A good part of the bill was patterned after the model in force in other Canadian provinces which, since Quebec enacted its Act in 1982, have combined these two functions.

In so doing, the government followed up on most of the recommendations made by a task force that had been given the dual mandate to study the *Right to Information Act*, in force for exactly 30 years, and the 2001 legislation concerning the protection of personal information in the public sector.[97] This mandate resulted from the commitments made by the new government during the election campaign that saw it come to power.

The members of the task force quickly launched a broad public consultation process by posting a detailed questionnaire for interested groups and citizens on a website. The initiative proved successful. Municipal councillors, newspaper editors, former ministers, planning commission representatives, senior government and Legislative Assembly officials, private agencies, citizens from various spheres of society, and the Advisory Council on the Status of Women, to name but a few, contributed their views on the subject.

[97] Right to Information and Protection of Personal Information Review Task Force (2007) – *Access to Information and Privacy Review Discussion Paper*, Fredericton, 18 pages.

The Ombudsman, responsible for oversight of legislation governing the protection of personal information and privacy, took part in the process by submitting a detailed brief in which he recommended numerous changes to the two acts.[98] Specifically, he recommended that the Legislative Assembly establish the position of a commissioner who would have the power to issue orders. He also called for the adoption of an information and privacy rights code that would explicitly recognize the fundamental nature of these two rights.

The task force took note of the Ombudsman's criticisms concerning New Brunswick's legislative silence on the protection of personal information in the private sector. It acknowledged that this was an issue "that requires further review as part of a separate exercise."[99] The Legislative Assembly has nonetheless made progress as regards the Ombudsman's recommendations concerning the scope and application of the legislation governing the public sector. For the first time, the proposed new legislation would apply to universities and municipalities.

As of early 2009, the bill is currently being reviewed by a committee of the Legislative Assembly. It is anticipated that an amended bill could be tabled in the spring and could come into force by the end of the year.

4.2 On the Federal Scene

As of this writing, the House of Commons Standing Committee on Access to Information, Privacy and Ethics is continuing its review of the 1982 public sector privacy act. Barely a year ago, the Committee tabled its report following an examination of the 2000 Act covering the private sector.[100]

In winter 2006–2007, the Standing Committee was tasked with reviewing the *Personal Information Protection and Electronic Documents Act,*[101] five years after its enactment. The recent coming into force of legislation governing the private sector in British Columbia and Alberta, in the wake of the legislation already in effect in Quebec, also argues in favour of returning to the drawing board.

The process was quite impressive. No fewer than 67 witnesses were summoned before the Committee, which also received 34 briefs from various segments of society, represented by the Canadian Medical Association, the Credit Union Central of Canada, the Canadian Bar Association, the Canadian Chamber of Commerce, representatives of federal government departments and agencies, the Insurance Bureau of Canada, the Canadian Resource Centre for Victims of Crime, the Canadian Association of Chiefs of Police, the Public Interest Advocacy Centre, numerous experts, and information and privacy commissioners from other provinces in Canada, just to name a few. From this list of participants one thing is clear: virtually all sectors of the business community, civil society, and government circles wanted to make their views known.

The Standing Committee tabled its report less than three months after completing its deliberations. While recommending basically that the legislation enacted in 2000 be maintained,

[98] Bernard RICHARD, Ombudsman (2007) – *Inside and Outside the Box: Proposals for an* Information and Privacy Rights Code *for New Brunswick (A Submission to the New Brunswick Task Force on Right to Information and Protection of Personal Information),* Fredericton (July 5): 30 pages.
[99] Right to Information and Protection of Personal Information Review Task Force –*Access to Information and Privacy Review Final Report*, Fredericton, September: 46 pages.
[100] Canada, Standing Committee on Access to Information, Privacy and Ethics, *Statutory Review of the Personal Information and Protection and Electronic Documents Act (PIPEDA) – Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, chaired by Tom Wappel (May 2007).
[101] *Personal Information Protection and Electronic Documents Act*, R.S.C. 2000, c. P-8.6.

the Committee also mentioned a number of minor changes that could be made to the Act. Such was also the thrust of the report made public, on behalf of the Government of Canada, by the Minister of Industry, who had introduced the legislation back in 2000; the Minister said in essence that the Act would stand the test of time. In response to the amendments proposed by the House of Commons Standing Committee, the government undertook to hold consultations in a number of circles, including with the Privacy Commissioner, with a view to forging a consensus in that regard.

In 2003, the government decided to re-examine the relevance of the administrative and legislative separation of the regimes governing access to information and privacy. In each of the provinces, those two regimes are joined, after the precedent set by Quebec in 1982. Following a study during which the Honourable Gérard La Forest, a former justice of the Supreme Court of Canada, heard testimonies from experts, senior civil servants, and civil society representatives, the status quo was recommended. As a result, the Privacy Commissioner continues to be an independent entity responsible for oversight of legislation governing the protection of personal information in the public and private sectors.

When the *Privacy Act* was enacted in 1982*,* Parliament committed to reviewing its relevance after five years had elapsed. In 1987, it kept its word: a House of Commons committee spent several sessions studying the Act, which was still seen as pioneering legislation in the western world. For a variety of reasons, no further action was taken.

A short while ago, in the fall of 2005, the committee responsible for following up on the personal information file took up the torch once again. At the committee's invitation, the Privacy Commissioner compiled a detailed report in 2006 to give tangible impetus to the MPs' work. In April 2008, the Commissioner tabled another report in which she proposed 10 amendments to the *Privacy Act* of 1982.

All of these documents testify to the need to update a quarter-century old Act. The Commissioner based her proposals on the major changes that in a way compromise the protection of personal information today. While some of those changes are indeed technological ones, there are also novel problems caused by events in recent years, such as the terrorist attacks of September 11, 2001. Such is the backdrop for the need to update the 1982 legislation.

In its work, the House of Commons committee zeroed in on the 10 recommendations that the Privacy Commissioner herself hoped to see quickly passed by the Parliament of Canada. Pending a major overhaul of the Act, those measures would make it possible to meet the most urgent challenges regarding protection of personal information. The measures all stem from problems encountered over the years in implementing the principles relating to the protection of citizens' rights in that area.

At its sessions, the committee had already heard the testimony of senior federal civil servants, experts in the field of protection of personal information, former provincial commissioners, the Minister of Justice, representatives of the Canadian Bar Association, the Royal Canadian Mounted Police, and the Treasury Board Secretariat, to name but a few. The Privacy Commissioner of Canada and members of her office appeared before the Committee on several occasions.

The Committee is slated to wrap up its work when Parliament resumes at the end of the summer and will likely table a report a few months later.

In both cases, the House of Commons committee's review of the two pieces of privacy legislation mobilized a significant number of representatives from the main sectors of Canadian society.

4.3 Quebec

In June 2006, the National Assembly enacted major changes to the two statutes governing the protection of personal information in the public and private sectors.[102] A similar process had been completed only once before, in 1987, pursuant to the 1982 Act, which expressly provides for a review of the legislation by the National Assembly every five years. The legislation governing the private sector, which came into force in 1994, contains an equally mandatory provision.

In 1992 and 1997, the National Assembly certainly received the report drafted by the *Commission d'accès à l'information* which, in accordance with the Act, sets in motion the five-year review process. In both cases, various circumstances, including the holding of elections, brought the process to a halt and made it impossible to respect the will of the National Assembly. In the end, it was on the basis of a report entitled *Reforming Access to Information: Choosing Transparency,*[103] tabled in 2002, that the systematic review of the *Act respecting access to documents held by public bodies and the protection of personal information* (1982) and the *Act respecting the protection of personal information in the private sector* (1993) was initiated and completed.

The Commission d'accès à l'information du Québec drafted this last report in the light of the lessons learned over the years in its control activities. It also drew on the changes that had occurred in other provinces. Its report covers the two facets paired by the National Assembly: access to information and protection of personal information. Some 15 of the 53 recommendations made by the Commission d'accès à l'information in fact deal with the protection of personal information in both the public and private sectors.

In the fall of 2003, the culture commission of the National Assembly launched an initial series of consultations. No fewer than 45 persons and organizations tabled briefs in the National Assembly, setting out their positions on the recommendations made by the Commission d'accès à l'information. At public sessions held over several days, the members of the culture commission heard testimony from 37 individuals and spokespersons for organizations, departments, and companies.

Parties testifying before the culture commission included the Canadian Life and Health Insurance Association, the Association des établissements de santé du Québec, the Association des témoins spéciaux du Québec, the College of Physicians and Surgeons, Option consommateur, SOS Déchets (Groupe d'Enviro-action), the Conseil de Presse, the daily *La Presse*, the Commission des syndicats nationaux, the Association de l'accès et la protection de l'information, the Protectrice du citoyen, the Fédération des établissements d'enseignement privé, and a number of independent experts, to name but a few. The long list is an indication of the interest generated by this process in many sectors in Quebec.

Following this round of consultations, in May 2004, the culture commission tabled its report containing 24 recommendations. Fifteen months later, the Minister responsible for the application

[102] *Act amending the Act respecting access to documents held by public bodies and the protection of personal information and other legislative provisions*, S.Q. 2006, c. 22.
[103] Commission d'accès à l'information du Québec, *Reforming Access to Information: Choosing Transparency*, Report on the implementation of the *Act respecting access to documents held by public bodies and the protection of personal information* and the *Act respecting the protection of personal information in the private sector* (November 2002).

of the two acts introduced in the National Assembly a bill whose provisions were modelled by the public consultations.

September 2005 marked the start of another round of public consultations, again under the auspices of the National Assembly's culture commission. In all, some 27 witnesses commented publicly on the Minister's intentions. These were more or less the same individuals and spokespersons who had appeared before the members of the National Assembly during the previous round. The interested sectors thus followed up in a tangible way.

Then, in winter 2006, the reworked bill (Bill 86) was brought once again before the National Assembly, where it took the traditional legislative route: readings in plenary session, detailed review of the bill in committee sessions and, finally, adoption by the National Assembly in June 2006.

In updating these acts—which, in their own way, had set precedents in terms of privacy protection in North America—the National Assembly evidently preferred to defer to continuity. While the two original acts underwent significant changes, their general intent remained unchanged. They were amended to take into account not only technological changes, but also transformations in the international arena. Accordingly, enterprises are now required to take all the necessary steps to ensure that personal information is afforded similar protection prior to the transfer of such information to other jurisdictions.[104] That provision is thus a response to the internationalization of flows of personal information in this era of globalization.

In short, reviewing privacy legislation in these three political systems is necessary. Such reviews are in fact a complex process, given the sensitive nature of the principles and interests at issue.

The control authorities—the Ombudsman of New Brunswick, the Privacy Commissioner of Canada and the Commission d'accès à l'information du Québec—play a key role at all stages of parliamentary review regarding privacy legislation.

Moreover, it is also important that members of civil society, representatives of the private sector and experts be involved in this process.

[104] S. 70.1, *Act respecting access to documents held by public bodies and the protection of personal information*, *supra*; s. 17, *Act respecting the protection of personal information in the private sector*, *supra*.

5. SOME PARTING WORDS

The paths taken by the federal government and the provinces of Quebec and New Brunswick with respect to privacy protection are a reflection of both unique circumstances and institutional traditions. The implementation of laws governing access to information and the proliferation of computers form the backdrop for the decisions made by these three jurisdictions.

Accordingly, three systems have been put into place in these three political systems. They subscribe to the fundamental characteristics of the legislation introduced in western countries beginning in the mid-1970s. Each of the three laws adopted by Ottawa, Quebec City, and Fredericton and the three control authorities instituted as a result reflect a specific political culture.

Since their coming into force, these systems have become more defined and have developed practices to meet the fundamental objectives of privacy protection. They devised procedures that characterize them and, in certain ways, set them apart from each other. Briefly put, these legislative and institutional innovations have been incorporated into the models shaped, over the decades, in the three settings.

Tailoring these regimes to new realities is unquestionably one of the most complex issues facing both the control authorities and the legislators. Problems encountered in implementing these laws raise important questions and call for answers and adaptations.

The extent and speed of the changes brought about by the growth of information technologies make the protection of personal information even more complex. The flow of personal information takes place in a context where borders are no longer an impediment or hindrance. It is an integral part of the phenomenon of globalization, whose ramifications on the protection of personal information are numerous and significant.

How can we take into account the considerable challenges posed, for instance, by the spectre of global terrorism? How can we reconcile security measures and respect for individual freedoms, from which the protection of personal information and privacy originates? How can we meet the requirements of certain countries, starting with the US, which are increasing their demands for personal information, precisely for security reasons?

The list of such questions keeps getting longer, each question challenging the basic principles governing the protection of personal information. There have already been many calls for the

adoption of binding international instruments aimed at providing genuine protection for information and data serving to identify any individual.

At present, some countries are being pressed by their own citizens or are being strongly encouraged by international organizations to develop legislation for the protection of personal information. Policy makers, jurists, and civil society representatives normally draw on their own customs and traditions. Additionally, they may be inspired by the experiences, initiatives, and track records of other countries having preceded them on this path.

Since the federal government and the provinces of Quebec and New Brunswick first subscribed to this objective, more research has been done, bringing a clearer sense of the challenges to be met. Some international organizations have clarified the legal foundations of privacy protection systems by fleshing out their fundamental characteristics.

Twenty five years ago, "independent authorities," as they were thus newly called, were launched in a fever of improvisation. A number of questions always arise when it comes to identifying the nature and scope of the mandates to be conferred upon the control authorities created under these systems. Should they be given binding powers? Would it be preferable to opt for authorities having only the mandate to make recommendations, like ombudsmen?

Should we establish a system combining both access to information and protection of personal information, as has been the trend noted in Europe over the past few years?

By examining the paths taken by other countries and the initiatives carried out by international forums, privacy advocates can look to precedents and experiences to help answer their questions. They can expand their horizons by drawing from the accomplishments of other countries. Cultural heritage and institutional traditions will necessarily enrich this intellectual quest.

6. COURSES OF ACTION AND BENCHMARKS

A critical review of the paths taken by Canada, Quebec and New Brunswick with respect to privacy protection points to a number of courses of action and questions that will likely prove helpful to those who are contemplating establishing such systems in their own countries.

A simple comparison of the models crafted by the legislators in each of these cases leads to a first observation. The Canadian federal system is characterized by the co-existence of legislative systems that are slightly different from one another, at least in some ways. Such is the case in particular with the three control authorities in place in Ottawa, Fredericton, and Quebec City. The scope and powers of these three entities stem from choices rooted in different institutional cultures. These control authorities nonetheless all have the same objective: to ensure compliance with the principles of the legislation and to give concrete expression to the right of recourse that is guaranteed to citizens and, in fact, to every individual.

In that same vein, a comparative review of the legislation and institutions put into place in these jurisdictions, as in other countries engaged in the legal protection of personal information, can almost serve as a laboratory. Such a review makes it possible to come up with a series of very specific suggestions intended for political leaders, public administrators, and civil society representatives interested in embarking on this path. The goal, a modest one, is to contribute to the concerted effort being made on every continent to ensure respect for personal information, a fundamental component of privacy.

Before drafting legislation, it would be wise to attempt answering some fundamental questions aimed at identifying the objectives and conditions of a potential system designed for the protection of personal information.

6.1 Some Basic Questions

What should the purpose of such a system be?

When it comes to personal information, the most helpful definitions would seem to boil down to a statement of that which characterizes, both aptly and simply, those data, numbers, symbols, and traits that differentiate a person and identify him or her. Of course, that notion will be qualified by the distinctive characteristics imposed by the community or society in question. The objective is to cast a wide net and make this notion part of an evolving process that takes technological changes into account. It would not appropriate to be overly precise here.

To whom should this system apply? Should it target all of the entities and enterprises that gather and use personal information?

The general trend advocates in favour of the public and private sectors being immediately and systematically subject to such a system. Particular circumstances, and judgments based on common sense and caution, may argue in favour of a two-step process.

How can this information be protected?

This question has two sides. On the one hand, it is a matter of devising and framing principles that will render the objectives and the ultimate aim of the emerging system. On the other hand, those principles have to reflect the intent of the country's laws and conform to the expectations agreed upon in most legislation. Efforts should be made to use language that is easily understood both in the public sector and by enterprises and organizations in the private sector.

6.2 From Principles to Procedures

The next step is to specify the actual procedures that will have to be implemented in order to afford personal information the necessary protection. These procedures must flow directly from the principles that are chosen and must be expressed simply and clearly. The danger would be to lapse into technicalities. Accordingly, those concerned may, for example, take their cue from the life cycle of personal information and seek to identify the problems that arise successively when it comes to protecting those data and come up with solutions.

Definitions of the basic principles and statements of terms can indeed draw on the accumulated experience of the past 35 years or more during which privacy legislation has emerged and the number of laws have grown, first in Western Europe and North America, then in many other countries around the world. Depending on the objectives sought, different laws may give rise to initiatives that take local realities and practices into account. The storehouse of experience currently available favours a broad, comparative process.

Consequently, even a superficial review of the laws enacted by Canada, Quebec and New Brunswick yields some interesting possibilities in terms of their architecture. Those laws are driven by four objectives:

- definition of the rights conferred upon citizens or any person who may benefit from the legislation;
- statement and clarification of the rights and responsibilities incumbent upon the holders of personal information;
- creation of a control authority responsible for ensuring that the rights conferred upon individuals are respected;
- rights of recourse granted to these same persons.

Even today, it is impossible to disregard the directions mapped out more than a quarter century ago by the Council of Europe and the OECD. The *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* released in 1980 by the OECD, and the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Convention 108, Council of Europe) prompt us to go back to the basics, to the consensual foundations of the protection of personal information. Everyone will benefit: policy makers whose motivation is to

develop simple and efficient systems; jurists in search of "comparables" or reference models; and civil society organizations seeking tangible, dynamic proposals that meet their expectations.

6.3 Control Authorities

This legal structure must of course be overseen by a control authority which, among other things, affords citizens recourse in the event of problems or disputes with holders of personal information. This entity must reflect the spirit that prevailed over the construction of the entire public apparatus. A predominant trend favours linkage of this "independent authority," using the expression that has garnered consensus, with Parliament. The status of this entity will depend on the objectives and powers to be given to it within the public administration, in a broad sense, and with regard to the public sector. The entities set up in various countries, Canada included, testify to this quest for harmonization or "congruency," to borrow the term used in the social sciences.

The three Canadian examples highlight an issue that continues to be the subject of debate when setting up such a control agency or authority. Is it better to rely on moral authority or the power of persuasion, as the Parliament of Canada and the Legislative Assembly of New Brunswick have done? Or, taking a page from Quebec's National Assembly, should this entity be vested with powers that would enable it to issue orders or to constrain, as it were, public entities or enterprises in the private sector that violate the principles, conditions, and requirements of the Act? Is it necessary to establish a control agency specializing in information protection? Should protection of information be dissociated from protection of the transparency of public authorities? Can these two functions be taken on by a generalist parliamentary control officer such as an ombudsman, a national human rights commission, or an auditor general?

This control authority must especially enjoy true autonomy and independence from the other components of the political system, and must be perceived as such. This question has been systematically examined by various international bodies since the early 1990s. The Paris Principles,[105] ratified by resolution of the United Nations General Assembly in 1993, pertain to all "national institutions for the protection and promotion of human rights." They form, as it were, the cornerstone for subsequent discussion.[106]

It is in this spirit that the Council of Europe recently added an explicit provision to a protocol of Convention 108. Similarly, the 1995 directive adopted by the European Union insists on the need to guarantee these control authorities "complete independence." The European Union Charter of Fundamental Rights sees the provision of true independent status as an essential condition for implementing a genuine system for personal information protection.

6.4 Technology, Globalization, and Cooperation

Lastly, efforts aimed at creating a system for the protection of personal information must be supported by a vision that extends beyond borders and is open to change.

Globalization has increased the flow of personal information. Multinationals pay no heed to borders. Governments wanting to know more about the travelling public invoke security requirements. At the end of the first decade of the 21st century, personal information protection systems must take that aspect into account and strive to minimize its impact on privacy. In that

[105] United Nations (1993) – Resolution A/RES/48/134 of 20 December 1993, of the General Assembly.
[106] Exact title of this text: Paris Principles – Principles relating to the Status and Functioning of National Institutions for the Protection and Promotion of Human Rights.

regard, the proceedings engaged in at annual meetings of the heads of control authorities are opening up new avenues and suggesting forms of international dialogue for taking these trends into account.
Technological advances, particularly in the information and communications sector, have shaken today's certainties. Most of all, they pose a major challenge to maintainting a significant level of protection for personal information. However, it would be wise to refrain from associating a piece of legislation with any particular phase of technological development.

Launching legal preparatory work with a view to establishing systems for the protection of personal information will inevitably be on the agenda in some countries. With it comes the opportunity for active and vigilant co-operation between the architects of such a process and the various control authorities in place within the French-speaking world. Useful and innovative projects could emerge from such a collaboration that focuses on a common destiny.

APPENDICES

APPENDIX 1

Commission d'accès à l'information du Québec

The *Commission d'accès à l'information* is the control authority instituted in 1982 by the *Act respecting access to documents held by public bodies and the protection of personal information*. The Commission's mission is to settle disputes involving access to documents held by public bodies and personal information in the public sector. Further, since the adoption of the *Act respecting the protection of personal information in the private sector* in 1993, the Commission has been discharging the same obligations with regard to personal information held by bodies in the private sector.

Table 1 – Commission d'accès à l'information du Québec

	Basic Data
Population served	7,651,500
Administrative framework	A President, responsible for the conduct and business of the Commission, aided by a minimum of four Commission members and a Secretary.
Acts administered	*Act respecting access to documents held by public bodies and the protection of personal information* (R.S.Q., c. A-2.1) *Act respecting the protection of personal information in the private sector* (R.S.Q., c. P-39.1) Excerpts of the *Civil Code of Quebec*, arts. 35 to 41 (S.Q., 1991, c. 64). And other sectoral Acts.

Table 2 – Missions of the Commission d'accès à l'information du Québec

	Description
Jurisdictional function	Examines applications for review under the *Act respecting access to documents held by public bodies and the protection of personal information* and applications for examination of disagreements made under the *Act respecting the protection of personal information in the private sector;* following an independent review and a hearing, renders a binding decision on any issue of law or jurisdiction that may be appealed to the Court of Quebec; may instruct any of its mediators to attempt to bring the parties to an agreement.
Oversight function	Oversees the application and promotion of, and compliance with, the *Act respecting access to documents held by public bodies and the protection of personal information* and the *Act respecting the protection of personal information in the private sector;* may, on its own initiative or following a request or complaint, investigate the application of, and compliance with, these two Acts; may following an investigation issue an order or make recommendations; authorizes a person or entity to receive personal information without the consent of the persons concerned for review, research, or statistical purposes; provides advice on draft agreements concerning the transfer of personal information and establishes rules for keeping records on the communication of personal information.
Advice	At the request of the Minister responsible for these two Acts, provides advice on draft bills and regulations impacting on access to information and/or protection of personal information; promotes transparency by taking action in matters of application of the Act as regards the provision on a website of information and/or documents accessible under the Act.
Awareness	Organizes presentations on transparency and respect for privacy; educates the public about legislation and issues pertaining to access to information and protection of information; takes part in events whose stakes (e.g., biometrics and video surveillance) affect protection of personal information.

Table 3 – Commission d'accès à l'information du Québec, Data (2006–2007)

	Data
Population	7,651,500
Total budget (minus rent)	$3,362,370
per million population	$439,439
Total F.T.E.s	44.5
per million population	5.8
Number of files resolved	1,933
per million population	253
access to information	547 (28%)
protection of personal information	1,342 (69%)
areas of intervention not identified	44
concerning the public sector	1343 (69%)
concerning the private sector	569 (29%)
unidentified sectors	21

APPENDIX 2

Privacy Commissioner of Canada

The Privacy Commissioner of Canada, who is both an educator and ombudsman, has been playing a key role in ensuring compliance with federal legislation on the protection of personal information since 1977.

With the aid of two assistant commissioners, the Commissioner responds to citizens' complaints concerning the federal public sector (*Privacy Act* – 1982) and the private sector (*Personal Information Protection and Electronic Documents Act* – 2000). While such complaints are settled most often through negotiation and persuasion, the Federal Court may also intervene if mediation and conciliation are unsuccessful. The Commissioner also plays a surrogate role in provinces where legislation on protection of personal information in the private sector has yet to be developed.

Table 1 – Privacy Commissioner of Canada

	Basic data
Population served	32,976,026
Administrative framework	A Commissioner and two Assistant Commissioners – one for application of the legislation governing the public sector (PA), and the other for the legislation governing the private sector (PIPEDA). Also, establishment of an External Advisory Committee.
Acts administered	*Privacy Act* (R.S., 1985, c. P-21) – public sector. *Personal Information Protection and Electronic Documents Act* (2000, c. 5) – private sector.

Table 2 – Missions of the Privacy Commissioner of Canada

	Description
Ombudsman	Investigates complaints made by citizens and incidents involving protection of personal information; serves as mediator between complainants and organizations; makes recommendations; represents the Office of the Commissioner and/or citizens in disputes before higher courts.
Oversight	Conducts audits of organizations to assess their compliance with legislation, as well as analyses; reviews Privacy Impact Assessment reports referred to him or her to identify potential risks to protection of personal information;
Advice	Researches issues relating to privacy and use of NICTs; serves as advisor to the Parliament of Canada and more specifically to the Standing Committee on Access to Information, Privacy and Ethics; consults with departments and agencies and appears before parliamentary committees; co-operates with other countries.
Awareness	In an educational capacity, focuses on providing strategic advice and promoting public awareness.

Table 3 – Privacy Commissioner of Canada, Data (2006–2007)

	Data
Population	32,976,026
Total budget	$15,716,000
per million population	$476,589
Total F.T.E.s	105
per million population	3.3
Number of files resolved	1,266
per million population	38.5
concerning the public sector	957 (75.6%)
concerning the private sector	309 (24.4%)

APPENDIX 3

Office of the Ombudsman of New Brunswick

The Ombudsman of New Brunswick, as an independent officer of the Legislative Assembly, is the authority that, under the *Access to Information Act* of 1978 and the *Protection of Personal Information Act* of 2001, examines complaints pertaining to access to information and protection of personal information. Those complaints may concern departments, school boards, hospital corporations, municipalities, or other entities reporting to government.

The Ombudsman may conduct independent investigations and reviews concerning the refusal by a government department or agency to release information to members of the public. These reviews take place in private. The Ombudsman has the authority to make recommendations, but not to issue binding orders.

New Brunswick does not have legislation governing the protection of personal information in the private sector. Consequently, the *Personal Information Protection and Electronic Documents Act*, enacted by the Parliament of Canada, applies to all commercial and private entities in the province.

Table 1 – Office of the Ombudsman of New Brunswick

	Basic Data
Population served	749,800
Administrative framework	One Ombudsman, who also serves as Child and Youth Advocate, supported by a team of investigators and legal advisors.
Acts administered	*Right to Information Act* – 1978 *Protection of Personal Information Act* – 2001

Table 2 – Missions of the Office of the Ombudsman of New Brunswick

	Description
Ombudsman	Investigates complaints filed by citizens and incidents pertaining to access to information and/or protection of personal information; makes recommendations; represents citizens in disputes before higher courts.
Advice	Researches issues concerning access to information and protection of personal information; supports the development of government policies.
Awareness	Focuses on prevention through a website providing an array of information (guides, reports, statistics).

Table 3 – Office of the Ombudsman of New Brunswick, Data (2006–2007)

	Data
Population	749,800
Total budget	$1,075,500
per million population	$1,434,000
Total F.T.E.s	13 persons, 2 of whom work part time
per million population	17.3
Number of files resolved	104
per million population	138.7
access to information	65
protection of information	39

BIBLIOGRAPHY

NEW BRUNSWICK

Bernard Richard, Ombudsman (2007) – *Inside and Outside the Box: Proposals for an Information and Privacy Rights Code for New Brunswick (A Submission to the New Brunswick Task Force on Right to Information and Protection of Personal Information),* Fredericton: 30 pages.

New Brunswick (1998) – *Protection of Personal Information Act,* c. P-19.1.

New Brunswick Government Task Force on Data Sharing and Protection of Personal Privacy (1994) – *Protecting Privacy in an Information-Sharing Environment: Report of the New Brunswick Government Task Force on Data Sharing and Protection of Personal Privacy*, Fredericton.

Office of the Ombudsman (2008) – *Investigation into Lost Personal Information by the Department of Health – Medicare Billing Cartridges,* Fredericton: NBPPIA-2008-01, 12 pages.

Right to Information and Protection of Personal Information Review Task Force (2007) – *Access to Information and Privacy Review Final Report,* Fredericton: 46 pages.

CANADA

Colin J. Bennett (1990) – "The Formation of a Canadian Privacy Policy: The Art and Craft of Lesson-Drawing," *Canadian Public Administration,* Vol. 33, No. 4 (winter), pp. 551–570.

Colin J. Bennett (2003) – "The Privacy Commissioner of Canada: Multiple Roles, Diverse Expectations and Structural Dilemmas," *Canadian Public Administration,* Vol. 46, No. 2 (summer).

David FLAHERTY (1989) **–** *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States,* Chapel Hill, University of North Carolina Press.

Government of Canada (2008) – *Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics:* Ottawa, 12 pages.

House of Commons, Canada (2007) – *Statutory Review of the Personal Information Protection and Electronic Documents Act* (*Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics)*, Ottawa, 70 pages.

Office of the Privacy Commissioner of Canada (2008) – *Privacy: Audit Report of the Privacy Commissioner of Canada: Examination of RCMP Exempt Data Banks- Section 36 of the* Privacy Act*,* Ottawa, 38 pages*.*

Office of the Privacy Commissioner of Canada (2008) – *Proposed Immediate Changes to the Privacy Act (Appearance before the Standing Committee on Access to Information, Privacy and Ethics),* Ottawa, 30 pages.

Privacy Commissioner of Canada (2008) – *Leading by Example: Key Developments in the First Seven Years of PIPEDA,* Ottawa, 63 pages.

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

QUEBEC

Paul-André Comeau and Maurice Couture (2003) – Accès à l'information et protection des renseignements personnels : le précédent québécois, *Canadian Public Administration,* Vol. 46, No. 3, fall: pages 364–389.

Commission d'accès à l'information du Québec (1992) – *Un passé éloquent, un avenir à protéger (Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels), Québec*: 49 pages.

Commission d'accès à l'information du Québec (1997) – *Vie privée et transparence administrative au tournant du siècle (Rapport sur la mise en œuvre de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels dans le secteur privé), Quebec*, 169 pages.

Commission d'accès à l'information du Québec (2002) – *: Choosing Transparency (Report on the Implementation of the* Access Act *and the* Private Sector Act*),* Quebec: 184 pages and appendices.

Raymond Doray, François Charrette (2001) – *Accès à l'information – loi annotée, jurisprudence, analyse et commentaires*, Montreal, Éditions Yvon Blais: 2,314 pages (2 vol.).

Lukasz Granosik (2008) – *Loi sur la protection des renseignements personnels dans le secteur privé (Édition annotée – Législation, jurisprudence*), Montreal, Éditions Yvon Blais: 196 pages.

National Assembly – Quebec - Commission de la culture (2004) – *Observations, conclusions et recommandations à la suite de la consultation générale et des auditions publiques à l'égard du document intitulé :* Une réforme de l'accès à l'information : le choix de la transparence, Quebec, 43 pages.

Quebec (province), Commission d'étude sur l'accès du citoyen à l'information gouvernementale et sur la protection des renseignements personnels (1981) – *Information et liberté,* Quebec: 225 pages. *(*Known as the *Rapport Paré).*