Access to Information and Privacy in the Post September 11 Context*

Elizabeth SANDERSON**

---

* Originally presented by Elizabeth Sanderson (Senior General Counsel, Public Law Policy Section, Department of Justice) on March 26, 2002 in Montreal at a Special Conference sponsored by the *Canadian Institute for the Administration of Justice* entitled "Terrorism, Law & Democracy: How is Canada Changing Following September 11?"

** Senior General Counsel, Public Law Policy, Justice Canada, Ottawa, Ontario.

Ms. Sanderson would like to thank Ed Morgan (Counsel, Public Law Policy Section, Department of Justice) for his assistance in the preparation of this paper.

The Right Honourable Pierre Trudeau (1964) once said:

> "Democratic progress requires the ready availability of true and complete information. In this way people can objectively evaluate the Government's policies. To act otherwise is to give way to despotic secrecy."[1]

This elegantly sums up one of the fundamental principles driving our access to information and privacy legislation.

However, common sense tells us that nothing—in policy, law or life—is that simple or straightforward. I feel quite confident that the man largely responsible for section 1 of the Charter,[2] if pressed, would tell you that the hallmark of good policy—and good law—is, in fact, reasonable limits.

We all understand that we do not live in a world of absolutes. Accordingly, there are no absolutes in the access and privacy arenas. For example, no one would suggest that all information held by the Government should be automatically released.

Rather, access to information and privacy legislation is about finding a proper balance. Often, limited exceptions must be made in some areas in order to further a greater public interest. Highly sensitive information is one such exception—a reasonable limit to access and privacy legislation—the necessity of which has been recognized since it was first passed.

---

1 M. Drapeau & M.A. Racicot, *The Complete Annotated Guide to Federal Access to Information* (Toronto: Thomson, 2001) at ix.

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

In the post September 11 period, *Bill C-36*[3] adjusted the existing balance between access and security. It introduced a new tool—the Attorney General certificate—to help us deal with a new, immediate threat to our security by strengthening existing protections for highly sensitive information. Although, at first glance, the certificate may appear to be an innovation—it is only a slight modification to (and quite consistent with) both the philosophy and schemes of the *Access to Information,*[4] *Privacy*[5] and *Personal Information Protection and Electronic Documents*[6] *Acts*.

To provide a little context, I will first briefly discuss the history and structure of access and privacy legislation in Canada. I will then move on to deal with the impact of the changes made post September 11 before explaining how the Government got the balance right.

I. ORIGINS

Access to information and privacy legislation has had an interesting history in this country.

II. ACCESS

The seeds of our current *Access to Information Act* were first sown in the 1960s and 70s—after the US adopted a freedom of information law. Very soon, increasing numbers of Canadians wanted their Government to follow suit. There were also a flurry of academic articles linking more open Government and freedom of information.[7] In response to this groundswell, backbench members of Parliament introduced several private members bills that were direct forerunners of our present act.

The right to access to information became inextricably linked to a broader debate over fundamental civil rights going on at the time. People began to question their Government's actions and motives—especially its

---

3 *Anti-terrorism Act*, S.C. 2001, c. 41 [hereinafter *Bill C-36* or *Bill*].

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

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

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

7 See Canada, *Discussion Paper: Freedom of Information Legislation* (Ottawa: Privy Council Office, 1979).

secrecy. Canadians became more and more insistent on greater transparency in the decision-making process.

The Government of the day realized that decisive action was required.

In 1980, after a number of false starts, the Honourable Francis Fox, Minister of Communications, introduced Bill C-43[8] (containing our current Access to Information and Privacy Acts) into the House of Commons. In moving the second reading of *Bill C-43* and its referral to the Standing Committee on Communications and Culture, Minister Fox said:

> "This legislation will, over time, become one of the cornerstones of Canadian democracy. The access legislation will become an important tool of accountability to Parliament and the electorate […]."[9]

Parliament passed *Bill C-43* in June of 1982 and it was finally proclaimed into force on the following Canada Day—July 1, 1983. The Federal Government finally had access to information legislation.

Its stated purpose was to provide a right of access to information in records under the control of a Government institution in accordance with the principles that:

- Government information should be available to the public;
- necessary exceptions to the right of access should be limited and specific; and
- decisions on the disclosure of Government information should be reviewed independently of Government.[10]

---

[8] Bill C-43, *An Act to enact the Access to Information Act and the Privacy Act, to amend the Federal Court Act and the Canada Evidence Act, and to amend certain other Acts in consequence thereof,* 1st Sess., 32nd Parl., 1982 (assented to July 7, 1982, S.C. 1982-81-82-83, c. 111) [hereinafter *Bill C-43*].

[9] *House of Commons Debates* (July 17, 1980).

[10] *Access to Information Act*, *supra* note 4, s. 2.

III. PRIVACY

The *Privacy Act* had its immediate origins in the mid-1970s. At that time, around the world, there was less trust of Government. Canadians began demanding more safeguards to ensure that Government couldn't arbitrarily violate their rights. The right to privacy turned into a touchstone issue.

On July 21, 1975, Bill C-72, *An Act to Extend the Present Laws in Canada that Proscribe Discrimination and that Protect the Privacy of Individuals,*[11] died on the order paper with the end of the Parliamentary session—along with the Government's first stab at privacy legislation. Fortunately, a revised version—the *Canadian Human Rights Act*[12]—was passed by Parliament and proclaimed in force in 1978. Part IV of that Act contained familiar measures of privacy protection, including a code of fair information practices and the creation of a Federal Privacy Commissioner (as part of the Canadian Human Rights Commission).[13]

In 1980, the Liberal Government considered privacy protection to be of sufficient importance as to justify its own Act—and it was included in *Bill C-43*. Its stated purpose was to assure the protection of Canadian's privacy with respect to personal information about them held by Government institutions.

IV. BALANCING

Although access and privacy rights may, at first, appear contradictory, we learned during the legislative process that they are in fact complementary. Access legislation ensures Government transparency and accountability. Privacy is also an accountability mechanism—ensuring that individuals have some control over information provided to Government.

---

[11] 1st Sess., 30th Parl., 1975 (1st reading July 21, 1975).

[12] R.S.C. 1985, c. H-6.

[13] See Canada, *Legislation on Public Access to Government Documents (Green Paper)* (Ottawa: Minister of Heritage, 1977) at p. 7-11.

As a result, review of the Federal Acts reveals that they are in many ways similar in both structure and approach.

As I mentioned earlier, one of their most important similarities is the fact that they both recognize that access and privacy are—of course—not unlimited rights. They are subject to limited exceptions—exemptions and exclusions—where overshadowed by a greater public interest.

Within each, a series of exemptions protects a variety of interests—both Governmental and non-Governmental. If either a record or personal information—or part thereof—comes within a specific exemption, the Acts recognize that the Government will be justified—or in some cases required—to refuse to disclose all or part of the information sought.

Exemptions are based on either an injury test or a class test. Injury tests require a reasonable expectation of harm to a specific interest to be shown while class tests refer to situation where a category of information is exemptible because it is *deemed* that injury would occur if they were disclosed.

Information obtained in confidence from the Government of a province is an example of an exemption covered by a class test. An important example of an injury-based exemption—and its relevance will become apparent later on—is information relating to security, national defence or international relations.

Exemptions can also be discretionary or mandatory. Discretionary exemptions allow the head of a Government institution to decide whether the exemption needs to be invoked. Mandatory exemptions provide no such discretion and must be invoked.

Where an exemption is invoked, the information is still reviewable by the Information Commissioner and/or the Federal Court. If the Commissioner thinks the exemption has been improperly applied he can note his disagreement in his Annual Report and ask the Federal Court to have the information released. If the Court disagrees with the application of the exemption, it can order the information to be released.

Exclusions were the ultimate limit to access and privacy Acts, in that documents excluded from do not fall under their ambit at all. Neither the Information Commissioner nor the Courts can review them. The best example of these would be Cabinet Confidences.

The *Access to Information Act* and *Privacy Act* are well-crafted schemes—but, of course, not written in stone. Like all good legislation, they are flexible and designed to adapt, where necessary, to the exigencies of the day.

V. SEPTEMBER 11

Shortly after the horrific events of September 11, nations to which we regularly compare ourselves—the United States, the United Kingdom, and many of our European allies—took a second look at the legal framework and investigative tools available to them.

As an international community, we recognized that the insidious nature of terrorism demanded an appropriate and measured but forceful response. Parliamentarians, academics, the media and individual Canadians called for stronger measures to ensure that Canada could deal effectively with the threat of terrorism.

The Canadian Government responded to this call by introducing *Bill C-36*—a balanced, comprehensive package of legislative reforms providing law enforcement with specifically tailored powers to ensure that terrorists would find neither refuge nor comfort within our borders.

VI. CANADA EVIDENCE ACT

This paper deals with one particular threat dealt with by *Bill C-36*—the possibility that highly sensitive information could inadvertently be compromised due to vagueness in pre-existing safeguards.

As discussed above, Canadians have always understood that the public has an interest in ensuring that such information be protected at all times, that inadvertent disclosure could potentially compromise important operations and cost lives, that our international allies must be able to trust that Canada is not the weak link in the chain and that information shared with us in the course of joint efforts to protect our citizens will continue to be protected. Given the immediate threat to our mutual domestic safety, this became all the more important.

As time passed, the sophistication of the terrorists involved in the September 11 attack became clearer. They had used advanced techniques and technology to collect intelligence on their targets and coordinate their efforts. We were faced with a formidable menace—international terrorists intent on and capable of gathering information to further their terrorist activities.

Bill C-36 introduced a dedicated tool specifically designed to prevent its accidental disclosure—*Canada Evidence Act*[14] Attorney General certificates and related changes under the *Access to Information Act*, *Privacy Act*, *Personal Information Protection and Electronic Documents Act* and the *Canadian Human Rights Act*.

Bill C-36 amended section 38 of the *Canada Evidence Act* to introduce greater flexibility into the system, offer the opportunity for evidentiary issues to be resolved early on in the process, and to give the Government an absolute guarantee against the disclosure of very sensitive information, while still providing fair trial protections.

VII. AG CERTIFICATES

The amendments provided the Attorney General of Canada with the power to issue a prohibition certificate in proceedings to prevent the disclosure of information injurious to international relations or national defence or security. The purpose of these certificates was to provide, *where necessary*, an absolute bar to the disclosure of certain highly sensitive information.

It was always anticipated that the certificate would be used only in exceptional circumstances; while still providing the ultimate guarantee required by our allies and all Canadians that sensitive information would be safe.

However, the Government was careful not to unfairly impinge on an individual's rights to justice—it established intricate safeguards.

The amendments made it clear from the start that, where a certificate was used, the Federal Court, in considering its ruling—in balancing the public interest in disclosure versus the public interest in

---

[14] R.S.C. 1985, c. C-5.

non-disclosure—could choose from a variety of options, including providing summaries and agreed statements of facts.

The intention here was to have this information available for use in proceedings in ways that would serve, to the extent possible, both the public interest in disclosure and the public interest in non-disclosure. In the rare event that an Attorney General's certificate were used, there would be consequences that would possibly accompany its use.

The proposed section 38.14 of the *Canada Evidence Act* provided that the person presiding at a criminal proceeding may make any order that he or she considered appropriate in the circumstances. For example, the proceedings could be dismissed if the judge takes the view that the accused would not otherwise get a fair trial. But the information protected by the certificate would not be disclosed.

During the development of the certificate scheme, it was thought that to ensure the integrity of this prohibition against disclosure of highly sensitive information, it was necessary to add them to other pieces of legislation under which information could potentially be disclosed.

That is why prohibition certificates also cover matters falling under the Access to Information, Privacy, Personal Information Protection and Electronic Documents and the *Canadian Human Rights Acts*.

VIII. CONSEQUENTIAL AMENDMENTS

While drafting section 38, the Government became concerned that information made inaccessible through the front door—that is to say a court of law—could still be accessible through the back door.

The Government recognized that information relating to security, national defence and international relations was already exemptible under the Acts. However, there was concern that the discretionary exemptions did not provide a sufficient guarantee of security against accidental disclosure. The fear was that important information, perhaps entrusted to us by allies, could accidentally be disclosed due to the uncertainty surrounding the current safeguards.

Furthermore, the Government felt that it would be absurd to, on the one hand, prohibit disclosure of information in a court of law while the potential still existed that it could be released under access or privacy legislation. To ensure that this did not occur, and to reassure our international allies, *Bill C-36* toughened up the pre-existing safeguards.

As originally drafted, where an Attorney General decided to issue a certificate, it excluded the highly sensitive information covered from the ambit of the access and privacy schemes.

IX. SAFEGUARDS

However, the Government also made sure that the certificates were designed with several specific procedural safeguards establishing a regime that ensured that certificates would only interfere with the access and privacy regimes in the narrowest of circumstances.

These safeguards included the following:

- only the Attorney General of Canada would be authorized to issue a certificate;
- the Attorney General would be required to personally issue the certificate and could not delegate the responsibility to someone else;
- the Attorney General would be required to serve certificates on all interested parties and file them with relevant decision makers;
- where certificates are issued, fair trials are ensured (for example, a judge could issue an order dismissing specified counts of the indictment or information, or effecting a stay of the proceedings); and
- finally, the legislation ensures that certificates would only be issued for the narrow purpose of protecting our national defence, our national security or information obtained in confidence from international allies.

After the introduction of *Bill C-36*, the Government listened closely to the advice of the Special Senate Committee, the House Committee and the various stakeholders who expressed their opinions on the issue of Attorney General Certificates. Further, officials consulted both the Information and Privacy Commissioners and their staff on several occasions so that the Government thoroughly understood their concerns.

In response to these concerns, amendments were accepted that strengthen protections by creating additional safeguards. Under these amendments, the certificate would only be issued after the following conditions are met:

- an order or decision for disclosure of the defined information has been made in the course of a proceeding before a court or body with the jurisdiction to compel the production of information;
- the certificate would be published without delay in the Canada Gazette;
- any party to a proceeding could apply to the Federal Court of Appeal for a review of the certificate;
- the judge reviewing the certificate would have the power to confirm, vary or cancel the certificate; and
- the certificate would be limited to a specific time period of 15 years.

In the original *Bill*, a certificate could have been issued at any time, the *Access to Information Act* and *Privacy Act* would not have applied and the Commissioners would have been removed from the process. Now, as a result of the amendments, much of the Commissioners' powers have been preserved, while still remaining faithful to our original goal of protecting information, which may help in our fight against terrorism.

We are pleased that the amendments to the *Bill* fully responded to the Privacy Commissioner's concerns. He was satisfied that *Bill C-36* struck a fair and reasonable balance between the need for enhanced security and the importance of maintaining the maximum possible protection for privacy. In fact, the Government received a letter from the Privacy Commissioner indicating his support for the Government's amendments to the *Bill* with respect to the certificate process. He also appeared before the Senate Committee studying the *Bill* and testified that his concerns had been met.

CONCLUSION

Bill C-36 is about balance in the post September 11 Canada and the Government got that balance right. Recognizing a potential threat to the security of all Canadians, the Government tightened pre-existing exceptions to the access and privacy regimes to reflect a higher public interest. The House of Commons and Senate agreed with this approach and the new provisions came into force on December 24, 2001.