Access to Information and Protection of Privacy in Canadian Democracy

Remarks of the Right Honourable Beverley McLachlin, P.C.
Chief Justice of Canada
Ottawa, Ontario
May 5, 2009
http://www.scc-csc.ca/judges-juges/spe-dis/bm-2009-05-05-eng.aspx

Introduction

The *Access to Information*[1] and *Privacy Acts*[2] came into force together on Canada Day 1983, almost twenty-six years ago, not long after Canada adopted its *Charter of Rights and Freedoms*. It was a heady time for Canadian constitutional development. The country had just, after long travail and discussion, repatriated its constitution to make it truly independent and at the same time, enshrined in its constitution a powerful affirmation of rights. The capstone of this new constitutional edifice – less well known but nevertheless important – was the adoption of twin laws of quasi-constitutional status, aimed at protecting Canadians' right to access to information and privacy.

In my remarks today, I propose to discuss first, the importance of access to information and privacy to Canadian democracy; second, how the *Access to Information* and *Privacy Acts* attempt to protect these vital rights; and finally, the challenges we face in applying these laws in a way that meets the goal of the statutory scheme.

1. The Importance of Access to Information and Privacy to Canadian Democracy

The Canadian constitution divides power between three branches of governance – the legislative branch (Parliament and the provincial legislatures); the executive branch, which is responsible to the legislature (the Prime Minister and Cabinet); and the judiciary.

The legislative branch is the foundational element of democracy. It is built on the premise that power flows from the people to their elected representatives who are empowered to make the laws that govern the people. The legislative branch represents the will of the people. It derives its powers from the people, via the ballot box.

The executive branch, under the principle of responsible government, is responsible to the legislature, or Parliament. The Prime Minister and the cabinet are chosen from elected members (although appointments from the Senate are permitted), and enjoy power only so long as they command the power to obtain Parliament's assent to critical legislation. The executive

branch, in this way is also dependent on the will of the people as expressed at the ballot box.

The judicial branch stands to the side, independent of the legislative and executive branches of governance. Its role is to decide the disputes and define constitutional powers and their boundaries. It acts as a referee. It does not second-guess Parliament and the executive, but ensures, when called upon, that the powers these bodies exercise are constitutional.

This is a skeletal sketch of Canadian governance. It has emerged from centuries of experience and has proved fundamentally sound. We call it democracy. Yet we have discovered that for this democracy to function well in the complex context of the modern world, two rights must be safeguarded – the right to access to information and the right to privacy. Let me deal with each in turn.

First, access to information. The argument that access to information is essential to democracy is simply put.

Informed voting depends on informed debate. Parliament and the executive branch derive their power from the people, who exercise that power by voting for or against particular people at the ballot box. For the people to effectively participate and vote, they must know and understand what the government is doing. Laws are published. But without additional information, the people cannot know how the executive branch of government is administering those laws – what the government is actually doing. And without that knowledge, informed debate is impossible. Accountable, transparent governance thus depends on the people having information about what the government is doing.

Not only is responsible voting dependent on information – so is the effective exercise of restraint through the judicial branch of governance. Citizens cannot challenge unlawful government action unless they know about it. Constitutional and judicial administrative review also depend on access to information.

Finally, information itself – or the possibility of information coming to light – acts as a check on abuse of powers. Public opinion and debate operate as an immediate check on potential abuse of government power.

The need for information is compounded by the inevitable tendency of governments, and those exercising powers on behalf of the government, to disclose only as much as they deem necessary. Despotic secrecy is the historic norm. Democracy sets its face against this. Yet, unchecked, the tendency is always there. And unchecked, it will inevitably undermine democracy.

This proposition has been recognized by statesmen and scholars.

Pierre Elliott Trudeau said this:

> ...the democratic process 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.[3]

In milder form, James Madison, one of the American founding fathers said:

> A popular government without popular information or the means of acquiring it is but a prologue to a farce or a tragedy, or perhaps both. Knowledge will forever govern ignorance; and the people who mean to be their own Governors, must arm themselves with the power which knowledge gives.[4]

And Professor J. R. Mallory, in his seminal work on the Canadian system of government, stated simply this:

> ...[the] major problem in modern constitutional democracy is to obtain effective control, by public opinion and by legal restraints, of the apparatus of the state which continually expands.[5]

In sum, in any system, democracy included, the apparatus of the state must be controlled. Without controls, the natural tendency to increase power will not be restrained. And without information, the necessary controls, whether at the ballot box or through judicial challenge, are absent. Constraining the "apparatus of the state", to borrow Mallory's term, depends on the people being informed about what government is doing.

While the tendency to secrecy — tell the people what they need to know and no more — is arguably inherent in any system of governance, in the early days of democracy it posed less a problem than it does today. When Ministers decided everything, questioning by the opposition in the legislative chamber provided an effective tool to ferret out information as to what the government was doing and a measure of transparency to how government policies were exercised.

But in the modern administrative state, where government powers are distributed amongst a hive of agencies and delegates, question period may prove inadequate to the task of informing the press and the citizenry. Ministers cannot, and largely do not, answer for the myriad of decisions administrative tribunals make, acting under delegated executive powers.

It is thus no coincidence that the demand for access to information coincided with the rise of the modern administrative state that developed after World War II.

In the 1960's and 70's, acceptance grew in western democracies that more must be done to provide the people with access to information.

> Sweden, far ahead of its times, provided the model; for almost 250 years its constitution has provided for open access to government documents.
>
> Finland in 1951 adopted access to information laws.
>
> By 1970, Denmark and Norway had similar laws.

The United States passed a *Freedom of Information Act* in 1966.

France passed its access to information law in 1978.

It was these developments that led to the recognition in Canada of the need for special protections for access to information.

The link between access to information and democratic governance is thus clear. But what about privacy, the second part of the Canadian scheme?

Privacy is linked to two goods in a democratic society – individual liberty and good governance. Individual liberty, guaranteed by s.7 of the Canadian *Charter*, depends on and mandates respect for the individual and his or her right to be free from government restraint, except as authorized by law. We do not have to look far to see how lack of privacy – the use of information for improper purposes – can constrain liberty. Some of you may have seen Florian Henckel von Donnersmarck's movie *Das Leben der Anderen* (2006) (*The Lives of Others*) set in East Germany before the fall of the wall. The movie graphically illustrates how the possession of private information by individuals and government acting in complicity systematically erodes liberty and replaces it with terror.

This invasion of individual liberty, in turn, is inevitably linked to abuse of government power, as the East German example illustrates. People who possess power, even small administrative powers, may use information they should not have improperly. And even if they don't, the individual's fear that they may use it, often leads to unwilling compliance.

The phrase "Big Brother is Watching You", prophetically used in George Orwell's novel *1984*, became part of the public consciousness in the 1960's and 70's, and led to the realization that protection of privacy rights was essential to individual liberty and good democratic governance. Consequently, privacy became a recognized social good, as evidenced by the proliferation of laws covering this issue:

Article 8 of the *European Convention on Human Rights*, adopted in 1950, guarantees a "right to respect for privacy and family life".

In the United States adopted a code of fair information practices in 1974.[6]

In 1988, Australia adopted principles in relation to the collection, use, disclosure, security and access to personal information.[7]

The philosophical underpinnings of these laws is an awareness that reduced levels of privacy may in fact make us less secure. Priscilla Regan, for instance, notes that one aspect of the social value of privacy is that it sets boundaries that the state, in its exercise of power, should not transgress in order to preserve, for example, freedom of speech and association within a democratic political system.[8]

Consistent with this view, research by sociologists, political scientists and others has shown how the dilution of the social value of privacy can

stifle political dissent as individuals fear reprisal by government actors;

> inhibit freedom of expression as individuals fear public scrutiny of their views or behaviour;
>
> result in political complacency to the extent that ubiquitous surveillance eliminates any subjective expectation of privacy and discourages citizens from questioning more and more state scrutiny; and
>
> make it harder to hold state agents accountable for their potentially abusive behaviour in part because of the surreptitious nature of the new technologies.[9]

The concern is that an erosion of privacy dilutes important shared values within a free and democratic state. As Robert Post has argued, privacy is not merely a set of restraints on society's rules and norms. Instead, privacy constitutes a society's common attempt to promote rules of behaviour, accountability, decorum, and civility.[10]

To recap, after World War II, western democracies one by one concluded that if democracy was to continue to flourish, guarantees of access to information and protection of privacy must be put in place. This is the backdrop against which Canada in 1983 adopted access to information and privacy legislation.

2. The Canadian Response

Awareness of the need for access to information legislation came to a head in Canada in the 1970's. In 1978, Professor Donald C. Rowat acknowledged the need for action in these terms:

> The most advanced democracies have been gradually coming to realize that they have inherited from earlier times a tradition of governmental secrecy which is incompatible with the people's right to know how they are being governed. The principle embodied in this tradition is that all administrative information is to remain secret except that which the government decides to release. . . By now, several democratic countries have reached the conclusion that this principle is wrong and ought to be stated the other way around: all administrative information is to be open to the public except that which needs to be kept secret as defined by law.[11]

At the same time, it was recognized that complete access to information might prejudice other interests, notably privacy. The debate on access to information thus became inevitably linked to the issue of privacy. Along the way it was recognized that access to information must be limited not only by privacy rights, but by certain exceptions, or "privileges" essential to ensuring that government decisions could effectively protect public security.

The Canadian Bar Association urged the creation of "a meaningful legislative right", deploring "the aura of secrecy which surrounds the business of government" and the "[erosion of] the trust relationship that should exist between the people and their government".[12] A number of private members' bills in Parliament were followed by a Green Paper in 1977. A rigorous debate took place. The result was the *Access to Information Act* and the *Privacy Act*,

twin pieces of legislation aimed at striking a balance between open accountability, effective governance and privacy.

We are all familiar with the thrust of the legislative scheme. Under the *Access to Information Act*, any Canadian citizen or permanent resident may, for a small fee, apply to a federal institution falling under the *Act* and request disclosure of information. In addition to individuals, the right of access has been exercised by businesses and other organizations, the media, and academic researchers. Over the past twenty-five years, the *Access to Information Act* has become part of our democratic landscape. Today's young people have grown up in a world where access to government information is taken for granted. The availability of information on government activities has become a given, part of the background against which societal discussions are conducted.

This is clear from observing the numbers alone. In 2006-2007, federal institutions received almost 30,000 access to information requests, 73% of which led to full or partial disclosures. This represents more than twice the number of requests received ten years ago.[13] Most notable in this increase is the rise in media requests: in 2007, almost 13% of all information requests originated with journalists, up from 7.7% ten years ago. By enriching the sources available to the media, the *Act* enhances the quality of reporting, the flow of information, and the exchange of ideas in our society. Indeed, learning to draft access to information requests now forms a part of every journalism school's syllabus. An assumption of information availability and governmental openness creates exactly the kind of democratic atmosphere which the drafters of the *Act* envisioned.

Creating new rights of access to information was the simple part of the exercise. The more complicated part was working out how to deal with the fact that access to information itself must be restrained. The debate surrounding the passage of the *Access to Information Act* concerned not the principle of access to information, upon which everyone agreed, but what limits should be placed on access to information.

As I suggested a moment ago, two countervailing interests had to be considered. The first was the interest of government in keeping secret information, the release of which would or could threaten the **public** interest. This included discussions in cabinet essential to effective governance and decision-making, i.e. the principle of cabinet confidentiality, and matters touching on national security.

The second countervailing interest was the privacy of those whose private names and activities might be disclosed in the information to be released. In a modern administrative state like Canada, government agencies possess an enormous amount of private information – from financial records to intimate details of medical treatment.

To accommodate these countervailing interests while protecting a broad right of access to information, Parliament introduced a series of exemptions into the *Access to Information Act*, and passed a complimentary law, the *Privacy Act*.

The right protected by the *Privacy Act*, like the right of access to information, is also firmly anchored in the Canadian consciousness. Indeed, over the past fifteen years, Canadians have made even more privacy requests than access to information requests. Since 1983, federal institutions have responded to over a million privacy requests, on average 35,000 a year, and over 333,000 access to information requests. Half of the privacy requests, and one third of the information requests made during that period obtained full disclosure.[14]

The *Privacy Act* restricts the right of access, by prohibiting the disclosure of personal information to third parties. However, it also enhances the right to know by granting individuals the right to access, correct, and supervise the use of any personal information in the government's possession. Neither *Act* can be read without the other. This is why the Supreme Court of Canada has described them as a "seamless code with complementary provisions that can and should be interpreted harmoniously".[15]

It is obvious by now that applying the exemptions to access to information and protecting the privacy of individuals involves a complicated balancing exercise between open access on the one hand, and the protection of countervailing public and private interests on the other hand. The statutory scheme provides two complementary mechanisms by which this balance is worked out.

The first mechanism is through the creation of commissioners, an Information Commissioner and a Privacy Commissioner. The twin commissioners play triple roles that are in their interplay unique to Canada: monitoring information disclosed and countervailing interests; investigating alleged breaches and mediating differences arising in the operation of the scheme; and advocacy on behalf of access to information and privacy respectively.

As independent experts, the Commissioners are watchdogs of the fundamental rights protected by the *Acts*. The Commissioners' responsibilities make them the first to become aware of compliance patterns, as well as any systemic problems of non-compliance. As independent investigators and mediators, the Commissioners promote negotiated solutions, avoiding a lengthy and costly recourse to the court system – the only recourse open to complainants in many other jurisdictions, such as the United States. Finally, as advocates of the right to access information and the right to privacy, their experience should translate into more effective enforcement, and ultimately, better information and privacy laws.

The second and complementary mechanism for balancing the broad right to access to information against countervailing concerns, is the courts.

The courts are the final line of review. The recommendations made by the Information and Privacy Commissioners are not binding. The federal courts independently review the government's disclosure and privacy decisions, guaranteeing that the *Access to Information* and *Privacy Acts* are applied in a way to provide meaningful and enforceable protection of these rights.

The Supreme Court of Canada has interpreted these Acts as quasi-constitutional legislation.[16] It follows that as fundamental rights, the rights to access and to privacy are interpreted generously, while the exceptions to

these rights must be understood strictly. Rather than government information being kept secret, except for what the government wants to disclose, the principle of the *Access to Information Act* is that all government information is open to the public, except that which needs to be kept secret, as defined by law and interpreted strictly by the courts. As the Supreme Court has stated, "[a]ccess laws operate on the premise that politically relevant information should be distributed as widely as reasonably possible." Similarly, the *Privacy Act* enshrines a broad right to privacy, with narrow exceptions.[17]

3. Challenges for the Future

We have been discussing the need for access to information and privacy protection in Canadian democracy and Canada's response in the form of a dual statutory scheme protecting access to information and privacy directed by dual commissioners, and subject to judicial review.

In the final portion of my talk, I would like to focus on the problems those charged with implementing this complex legislative scheme are currently grappling with. The problems, as I see it, are three:

1. How to resolve the balance between to information rights and privacy rights when they conflict.
2. Coping with emerging communication technology; and
3. Coping with the security threat.

Resolving the Balance

The first and most fundamental challenge is the ongoing task of resolving tensions between the right to access and countervailing interests and rights, notably the right to personal privacy.

This tension is inherent in the scheme passed by Parliament. The structure of the *Access to Information* and *Privacy Acts* mirrors the inherent tension between the public's general right to access information, and the individual's right to restrict the disclosure of information for privacy reasons. Indeed, the legislator's choice to enact these two pieces of legislation together, to draft them so that they share definitions and exemptions — in the Court's words, to design them as a 'seamless code' — places this tension at the heart of any interpretative exercise of the *Acts*.

The jurisprudence, based on the apparent intention of each Act, requires that both access to information and privacy be broadly construed, and that exceptions be narrowly construed. But how can this be done when access and privacy rights conflict? In such cases, it is logically impossible to give both rights a dominant position. On the one hand, as a "right", one would expect the right to personal privacy to be understood broadly. On the other hand, because personal privacy is cast as an **exception** to the right of access to government information, it must be interpreted narrowly – or so, at least, logic would suggest. The challenge for courts is to give equal protection to both rights. Attempting to meet this challenge, the Supreme Court held in 2003, "that the *Privacy Act* and the *Access Act* have to be read jointly and that

neither takes precedence over the other".[18] Yet in reality, choices must sometimes be made. Those who administer the Acts, and the courts that review their operation, continue to wrestle with this problem.

The challenge of reconciling the right to personal privacy and the right to access plays out most clearly in cases which involve a dispute about the definition of "personal information". A good example of this is the 2003 case to which I just referred, involving the RCMP. The question in that case was whether job-related information concerning RCMP officers, such as historical records of successive postings, ranks, and statuses, fell into the definition of "personal information" and should therefore be withheld from disclosure. The RCMP had refused to follow the Information Commissioner's recommendation to release this information. The Supreme Court agreed with the Information Commissioner, deciding that, although this was indeed personal information, it was associated with the general characteristics of a federal employee position, such that it might figure in a job-posting, and that it should be disclosed. It was, in effect, information about the **position**, not about the **person**. Information on the competence or characteristics of an individual employee, on the other hand, would be protected from disclosure for privacy reasons. In this way the Court was able to draw a line between government employee information which may be accessed by the public, and employee information which should be withheld in the interests of privacy.

Balancing is also required from time to time between access to information and countervailing public interests, such as cabinet privilege, public interest privilege and security concerns. For example, the *Act* allows the government to refuse to disclose any information that could harm the defence of our country[19] or threaten the safety of individuals.[20] As well, information subject to certain forms of privilege, such as solicitor-client, are exempted from disclosure.[21]

In the first instance, much of the exercise of balancing falls to the parties involved and the Commissioners. Courts, when called on, may give guidance in the balancing. What results is a multi-layered dialogue within government agencies, in the offices of the Information and Privacy Commissioners, and in courtrooms. From their different vantage points, the institutional actors on the information and privacy stage play their parts in maintaining a viable balance between government accountability and conflicting rights and interests, for the greater benefit of Canadian democracy.

Technological Change

A second challenge in the interpretation and application of the Acts is the need to cope with changing technology. The quarter century since the Acts were passed has seen vast technological change. We have gone from a day when government records were kept on paper, to the age of electronics and host of new document forms — recordings, computers, blackberries, digital video files, and the internet, to name but some. These changes have vastly multiplied the amount of data in the hands of government, and at the same time created new problems of how to save and access it.

These changes impact both the right to privacy and the right of access to information. The Privacy Commissioner, commenting on the changes since 1983 when the *Privacy Act* was enacted, put it this way:

Times have changed — so too has the privacy environment. Technology has created new and complex privacy issues.

> *In 1982, the internet, global positioning systems, radio frequency identification devices, cross-border outsourcing and data mining were novel ideas. Today, these technologies are commonplace and are the key issues keeping privacy advocates up at night. Another generation of technologies that carry privacy risks – brain scans and smart dust, for example – is just around the corner.*
>
> *. . .*
>
> *The Privacy Act was not designed to address the era we now live in and it is not up to the job of protecting Canadians in this changed world. In fact, it has been desperately out of date for many years.*[22]

Other technological changes impact directly on access to information. The goal — indeed, the fundamental purpose — of the *Access to Information Act* — is to inform the press and the Canadian people about the workings of the government. This in turn, is premised on the conviction that unless the public (subject to limited exceptions with public interests) is informed about the workings of government and government agencies, democratic debate will be stifled and democracy itself undermined by the inability of the electorate to judge, and hence to control what Mallory called the constantly expanding "apparatus of the state".

The question this poses is whether modern digital ways of conducting government business have effectively undercut the goal of Parliament in 1983 of informing the electorate on the workings of government?

One problem is that much government business that once would have been reduced to writing is now done "below the radar screen", by emails that are erased and in many cases lost. It may be that at great expense and effort, the lost information could be retrieved. This is attempted in the context of lawsuits, where a party is by law entitled to "discovery" of all relevant documents in the hands of the opponent. Yet the problems of e-discovery, as it is known, are legion. Great effort, expense and technical expertise are required to ensure that all documents have been found and reproduced. All this takes time, delaying proceedings. How is a public access to information system, with limited funds and commitment to prompt — or at least relatively prompt — disclosure, to meet this challenge?

A related challenge relates to the decline in the culture of record-keeping that has accompanied the digitalization of our world, coupled with the ubiquitous shredder.

I recently visited the Archives of Canada building and was given a tour of its facilities. I viewed record after record from the past, meticulously kept in beautiful handwriting. There, beneath the glass, I viewed daily attendance records of first nations children of residential schools, taken a century or so

ago. These records are now proving indispensable to our nation's attempt to accord a measure of justice to these children and their descendants and to better understand our history. But I found myself asking, would these records have been kept today? If so, would they have been shredded at some point along the years that have intervened? Indeed, some suggest that the very existence of access to information legislation may deter government officials, agents and agencies from making and keeping complete records.

If we truly believe, as evidently did in 1983, that democracy depends on the people and the press having access to information, I believe we must examine these issues. We are faced with a choice. Either we meet the challenge of keeping our legislation relevant in the 21st century, or we abandon our goal of access to information and privacy.

Security

A final challenge in interpreting the *Access to Information* and *Privacy Acts* is claims of national security. One of government's primary responsibilities is to protect its citizens. This responsibility sometimes involves claims of national security. Both the *Access to Information* and *Privacy Acts* recognize national security as a valid ground for the government to exempt information from disclosure. With respect to access to information, there is a danger that claims of national security may unduly limit the openness and transparency needed in a democratic society. With respect to privacy, the Privacy Commissioner has raised the concern that there is a risk that increased powers of surveillance given to law enforcement and national security agencies may unduly invade personal privacy.[23]

The courts have held that national security concerns may limit the extent of disclosure of information to an individual, and may permit intrusions into individuals' privacy. However, in response to the need to ensure that claims of national security do not overwhelm other fundamental societal interests, the courts have required, in a variety of different contexts, measures to ensure that people are treated with procedural fairness.[24]

These are real concerns that face not only the courts, but all government employees who deal with issues of access to information and privacy. Ultimately, they are concerns of fundamental importance to the Canadian people. And they are not going to go away. We must, at the risk of undermining access to information and privacy, face them.

Conclusion

With a quarter of a century's experience behind us, we have reason to be proud of the fact that we have acknowledged the fundamental links between democratic governance on the one hand, and access to information and privacy on the other. We should also be proud of the concerted efforts we have made over the last quarter century to ensure that these rights are not merely theoretical, but have significance for Canadian women and men. Most importantly, we have reason to take pride in the fact that we have developed a culture that accepts information as the norm and that places a prime on transparency and accountability in government operations – a culture that at

the same time values privacy and takes account of countervailing public interests.

But we should not take these accomplishments for granted. The temptation of greater secrecy is ever present; the technological and security challenges to individual privacy ever advancing. These realities complicate the task of meeting the underlying challenge of finding the right balance between access to information and countervailing public and private interests, on a case-to-case basis.

I congratulate you, who struggle to achieve that right balance, whether it be in government, the bar, or the media, on your contributions to the development of this field over the past 25 years, and wish you success in the times that lie ahead.

Notes

1. R.S.C. 1985, c. A-1.
2. R.S.C. 1985, c. P-21.
3. Pierre Elliott Trudeau, quoted by G. Baldwin, M.P. in Standing Joint Committee on Regulations and other Statutory Instruments, *Minutes of Proceedings and Evidence*, 30th Parl., 1st Sess. (1974–75), 22:7 as cited in T. Murray Rankin, *Freedom of Information in Canada: Will the Doors Stay Shut*? (Ottawa: Canadian Bar Association, 1979).
4. Letter from James Madison to W.T. Barry, August 4, 1822, cited in Rankin, supra at p. 1.
5. J.R. Mallory, *The Structure of Canadian Government* (Toronto: Macmillan of Canada, 1971).
6. *Privacy Act of 1974*, 5 U.S.C. § 552a.
7. *Privacy Act 1988* (Cth.).
8. Priscilla Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: The University of North Carolina Press, 1995) at 221-30.
9. David Lyon & Elia Zureik, "Surveillance, Privacy, and the New Technology" in David Lyon & Elia Zureik, eds., *Computers, Surveillance & Privacy* (Minneapolis: University of Minnesota Press, 1996) 1; James R. Beniger, *The Control Revolution: Technological and Economic Origins of the Information Society* (Cambridge, Mass.: Harvard University Press, 1986); Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca, NY: Cornell University Press, 1992); Gary T. Trotter, "The Anti-terrorism Bill and Preventative Restraints on Liberty" in Ronald J. Daniels, Patrick Macklem & Kent Roach, eds., *The Security of Freedom : Essays on Canada's Anti-terrorism Bill* 246 (Toronto: University of Toronto Press) 239; Arthur J. Cockfield, "Who Watches the Watchers? A Law and Technology Perspective on Growing Government and Private Sector Surveillance" (2003) 29 Queen's L.J. 364 at 391-398; Kevin D. Haggerty & Amber Gazso, "Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats" (2005) 30 Can. J. Soc. 169 at 180-185.
10. Robert C. Post, "The Social Foundations of Privacy: Community and Self in the Common Law Tort" (1989) 77 Cal. L. Rev. 957 at 968.

11. Donald C. Rowat, *Public Access to Government Documents: A Comparative Perspective: A Research Study Prepared for the Ontario Commission on Freedom of Information and Individual Privacy* (Toronto: Commission on Freedom of Information and Individual Privacy, 1978), at p. 1.
12. T. Murray Rankin, *Freedom of Information in Canada: Will the Doors Stay Shut?: A Research Study Prepared for the Canadian Bar Association* (Ottawa: Canadian Bar Association, 1977), at p. 155.
13. See the Treasury Board's Infosource website. For 2006-2007: <http://infosource.gc.ca/bulletin/2008/bulletin03-eng.asp>. For 1996-1997: <http://infosource.gc.ca/bulletin/1998-bulletin-eng.pdf>.
14. See the Treasury Board's Infosource website. For the *Privacy Act* statistics: <http://infosource.gc.ca/bulletin/2008/bulletin06-eng.asp#Toc182879765>. For the *Access to Information Act* statistics: <http://infosource.gc.ca/bulletin/2008/bulletin05-eng.asp#Toc182879764>.
15. *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66, 2003 SCC 8, at para. 22, per Gonthier J.
16. *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 773, at para. 24.
17. *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403.
18. *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, [2003] 1 S.C.R. 66, at para. 21.
19. Section 15.
20. Section 17.
21. Section 23.
22. Privacy Commissioner of Canada, *Annual Report to Parliament 2006-2007: Report on the Privacy Act* (Ottawa: Office of the Privacy Commissioner of Canada, 2007).
23. *Ibid*.
24. *Charkaoui v. Canada*, [2007] 1 S.C.R. 350 at paras. 58-61.