

**Accountability Through Transparency:
Or,
How I Learned to Love Access and Privacy
Legislation**

Ann Cavoukian, Ph.D.

Transparency: Foundation of Democracy

**Management Board Secretariat
Access and Privacy Workshop 2002**



**Information and Privacy
Commissioner/Ontario**

September 19, 2002



**Information and Privacy
Commissioner/Ontario**

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: <http://www.ipc.on.ca>

This presentation is also available on the IPC Web site.

Accountability Through Transparency: Or, How I Learned to Love Access and Privacy Legislation

Good morning everyone. I would like to offer my sincere thanks to Kathy Bouey for her kind introduction. As Secretary of Management Board of Cabinet, Kathy is well acquainted with the important values of open government and privacy, and I am very pleased that she agreed to participate in today's conference. As the Ministry responsible for FOI and privacy in Ontario, MBS has a vital leadership role to play. I know that in Kathy Bouey, MBS has a Deputy Minister who understands the importance of access and privacy. Our two organizations (through the Access and Privacy Office of MBS) have undertaken a number of joint projects over the years and I plan to continue this important relationship in the future.

I want to say how pleased I am to be here with you this year. As some of you know, I was unable to attend this conference last year, so I am doubly pleased to be back with you again. I am well aware of how much effort goes into putting on this conference, and how many people are involved, from my office, from MBS and many other organizations. For a number of you, this is one of the few times in the year you get to meet and spend time with others who believe that access and privacy represents more than an odd little office tucked off in the corner of each ministry.

Let me start by applauding your continued professionalism and dedication to supporting the access and privacy scheme in Ontario. I know that it can be a thankless job at times, and I'm here to thank you. I want to recognize publicly how seriously you take your jobs – your attendance here today is testament to that. Congratulations to you all and my sincere thanks for all of your hard work.

From the outset, I would like to acknowledge last week's anniversary of the September 11 tragedy. Everyone knows how devastating that event was, and how traumatic it was for people, not just in New York or in America, but all around the world. Beyond the human toll and property loss, there was also a real loss of innocence, and in the days and months that have passed, a loss, not only of freedom, but both privacy and access to information. The events of 9/11 have had a significant impact on legislation that has been enacted in the U.S., Canada, the United Kingdom, Australia and elsewhere – and these laws have affected the privacy of the citizens these governments have sworn to uphold – including expanded powers of surveillance and diminished independent judicial oversight.

Equally, these government actions have had a very significant effect on access to information. If anyone is interested in finding out more on these issues, please feel free to contact my office, or visit our Web site (www.ipc.on.ca). We have produced a number of documents on the privacy impacts of 9/11 legislation – reframing the security vs. privacy debate, and the impact of 9/11 on access to information. Assistant Commissioner Tom Mitchinson will be presenting a paper on this last issue at the upcoming Council on Government Ethics Laws (COGEL) conference, in early October, in Ottawa. Look for it on our Web site in a few weeks.

In our efforts to increase public safety and security, we must remain ever vigilant to protect the basic civil rights that form the foundation of our society – otherwise, we erode the very rights that we are attempting to protect.

Let me give you a few examples. At the federal level, the Canadian government introduced anti-terrorism legislation that had the laudable goal of providing authorities with the power to combat terrorist activities. However, I joined other information and privacy commissioners in pointing out that the broad wording of the legislation raised the real possibility of abuse.

In addition, the legislation has the potential to erode existing rights of access to information and the power of the federal Information Commissioner. The legislation gives the federal justice minister sweeping powers to withhold government-held information. Under the Act, the Attorney General of Canada may personally issue a certificate that prohibits the disclosure of information “in connection with a proceeding” for the purpose of protecting information received in confidence from a foreign entity or for the purpose of protecting national defence or national security. The federal Information Commissioner criticized the bill as an attack on the independence of his office because it would give the Attorney General the power to halt any investigation being conducted by the Commissioner. The federal government, in its attempt to preserve the fundamental values of our society, in my view, went some distance to undermining them.

The terrorist attacks of September 11 also induced governments, in Canada, the United States and around the world, to review their access to information laws and policies, and the types of information they make routinely available to the public, particularly on government Web sites. The challenge facing governments is to balance the public’s right of access to government records, with the need to protect society against terrorist attacks.

In Canada, the federal, provincial and municipal governments have not acted as aggressively as their U.S. counterparts in cutting off access to information that was routinely available to the public before September 11. However, there have been some notable instances where access has been curtailed to information that was previously in the public domain.

For example, the City of Toronto is now restricting access to building plans. These documents, which were routinely available to the public for viewing before September 11, may now only be accessed with the written consent of the building owner. In addition, an individual who wants to view building plans must file a formal freedom-of-information request, where before it was routinely disclosed – whither RD/AD?

In another example, the federal Department of Transport is refusing to release the results of airport security screening tests (Department inspectors routinely test the effectiveness of security at Canadian air terminals by trying to slip materials past staff responsible for searching passengers and carry-on baggage). Previously, similar records were routinely released to the media under the federal *Access to Information Act*.

Now, these examples are relatively straightforward, and perhaps, not surprising. I think we can all understand how unfettered access to building plans may no longer be an unquestioned right, in light of the unprecedented threats to security that exist today. However, it is vital that we remain vigilant to ensure that efforts to limit the public's right to information are legitimately connected to real security threats. Fears of terrorist attack should not be used as a way for government to prevent the release of information that may be embarrassing or inconvenient, but that is unlikely to be dangerous – the government is there at the pleasure of the governed. Their activities must remain open and accountable – let's not lose sight of that.

There is also a perception that privacy rights have taken a significant hit. Governments, on both sides of the border, have passed anti-terrorism legislation that has eroded previously enjoyed privacy rights. How often have you heard that since September 11, privacy is no longer a concern?

Allow me to set the record straight. We must distinguish between the public's willingness to accept government limiting its privacy rights in the pursuit of legitimate security interests vs. business and consumer privacy-related issues. Clearly, September 11 had an impact on the former, but I assure you, not on the latter. Make no mistake, the public will not accept business practices that abuse its personal information. Businesses would be seriously misguided if they believed that privacy, in the commercial context, was no longer important. A desire for national security has not reduced the importance of privacy in the minds of consumers. Quite the opposite.

And I want to take a moment to stress this point. While public reaction to government actions in support of public safety has been generally supportive, there has been **no** commensurate easing of consumer privacy concerns regarding the uses of their personal information by business. In fact, according to the latest Harris/Westin poll numbers, public concern over privacy has increased, not decreased, over the last number of months. Let me give you the before and after: In May, 2001, Privacy Fundamentalists made up 25% of the population; Privacy Pragmatists had increased to 63% from 55%; the Privacy Unconcerned had dropped to 12% from 20%. But in a post-9/11 survey conducted in November, 2001, Privacy Fundamentalists increased from 25% to 34% of the population; Privacy Pragmatists were at 58%; the Privacy Unconcerned dropped to 8% – the lowest figure ever. Clearly, business cannot take privacy for granted. Today's educated consumers have indicated that they are unwilling to part with their personal information if they do not have the necessary confidence and trust that a business will treat their information with respect. Businesses must take privacy seriously – good privacy is good business, but perhaps more significantly, bad privacy is really bad for business.

The theme of this conference is transparency, a theme that is indeed most topical. The last few months have witnessed accounting scandals, too numerous to mention. Public reaction to these situations has been, unexpectedly, one of anger and to some degree, a sense of “well, we knew it along.” Enron, WorldCom, Adelphia – apparently any company that has put its name on a sports stadium in the last number of years (excluding Air Canada, I hope) seems to have gone under due to accounting “irregularities.” Even Arthur Andersen, a highly regarded accounting and audit firm, apparently assisted in the creation of accounting statements that, to be charitable, lacked transparency.

Governments, accounting standards boards, and securities commissions have been tripping over themselves trying to impose new, tough regulations and higher standards of oversight to prevent such business practices from continuing. Some might argue that much of what has gone on was always illegal, but that our system of oversight perpetuated and permitted it to occur. Who knows whether CEOs will have to sign-off on their corporate accounts or whether auditing firms will have to be rotated every five years? The important point is that there has been a lapse of more than just accounting oversight, but of an ethical understanding of the importance of transparency.

When Adam Smith spoke of the “Invisible Hand” that guided the marketplace, he spoke about a world in which there was an assumption of equal access to information about business, in order for people to make fair decisions. Transparency is why there are laws against insider trading, why there are numerous corporate disclosure laws about both routine transactions and material changes to operations, and why companies have to file an extremely detailed prospectus prior to an initial public offering – all so that the players in the market can make informed business decisions.

Transparency also lies at the heart of open government. The recent federal Access to Information Review Task Force report noted the importance of transparency as a key element of public trust and confidence in government. My office has advanced the concept of transparency through a number of works promoting Routine Disclosure and Active Dissemination (RD/AD) – most recently in a paper entitled, *Opening the Window to Government: How e-RD/AD Promotes Transparency, Accountability and Good Governance*. I’m sure you will agree that transparency is one of the very foundations of our democratic system.

In the context of privacy, transparency or openness is one among eight (or 10 in Canada) Fair Information Practices, which are internationally recognized guidelines for data protection. These practices form the basis of the Canadian Standards Association’s *Model Code*, incorporated into Canada’s federal private sector privacy law and in Ontario’s pending privacy legislation.

I would like to pass along my initial thoughts on the pending health and private sector privacy legislation (obviously I’ll have more to say once the legislation has been introduced) since some of you may be curious about our views on developments to date. As the Information and Privacy Commissioner of Ontario, I have been calling for this legislation for many years, and my office is very excited that the introduction of such legislation appears to be on the horizon.

Before highlighting what the bill is likely to contain, and how my office is preparing for our new responsibilities, I would like to publicly acknowledge the dedicated work of the staff at the Ministry of Consumer and Business Services and the Ministry of Health and Long-Term Care. I am confident that the extensive consultation process and the detailed discussions that the government has had with stakeholders and staff from my office will result in a comprehensive, coherent and truly privacy-protective bill being introduced in the legislature this fall. I would also like to applaud Minister Hudak for his dedication to moving the bill forward, and his predecessor, Minister Sterling, for his important contributions to the development of this legislation.

Developing this type of legislation is not easy work – it is complicated and difficult. As you can imagine, there are numerous stakeholders to be consulted, and a multitude of issues to be considered. The staff of both ministries have worked diligently preparing this bill. I am eagerly awaiting the introduction of the bill, which I intend to fully support.

Based on the draft legislation that was released earlier this year, and discussions that we have had with staff of the two lead ministries, I would like to provide you with a brief overview of what this legislation is likely to look like.

In general, the legislation will cover all provincial organizations that are not subject to the provincial or municipal *Freedom of Information and Protection of Privacy Acts*. Unlike PIPEDA, the federal private sector privacy law, this will include non-commercial entities such as universities and not-for-profit organizations. Privacy protection will also be extended to the employees of organizations that are subject to the law.

Special protections would also be established for personal health information. This is obviously of utmost importance, since health information is probably the most sensitive of all personal information.

The bill will set out clear rules for how businesses and organizations handle personal information. These rules will be based on Fair Information Practices, principles that are set out in the *CSA Model Code for the Protection of Personal Information*. These include such important principles as accountability, the need for consent, limiting use, disclosure and retention, security, individual access and the right to challenge compliance.

An important aspect will be the need for organizations to be transparent in their information management practices. The law will entitle individuals to be given enough information to know how their personal information is being collected, used and disclosed and to know what rights they have in relation to this information.

An organization will need to designate a contact person to be responsible for receiving public inquires and complaints. Further, the organization will be required to make publicly available a written statement describing its information practices and telling people how they can obtain access to their information and make a complaint to the IPC.

In addition to the right of access to personal information, individuals will be able to request that mistakes be corrected.

Effective oversight and enforcement are critical to any meaningful privacy scheme and are key components of fair information practices. Under the legislation, my office will be the oversight body. We will have the power to investigate privacy complaints against organizations and to review information practices of businesses and organizations if there is a reason to believe that those organizations or businesses are contravening the *Act*. But this will be a last resort – we intend to lead with consultation and mediation – working with businesses to help them understand the issues and get it right.

An important aspect of our anticipated new mandate will be conducting public education programs and providing information concerning the *Act* and the Commissioner’s roles and activities.

We intend to take this responsibility very seriously. In fact, we have already started the work of preparing for our new responsibilities. Over the spring and summer, my staff has met with many private and health sector organizations; groups as diverse as the Retail Council of Canada, Ontario Federation of Labour, Canadian Marketing Association, Insurance Bureau of Canada and the Ontario Hospital Association, to name a few. These meetings started the process of relationship building, helping us to understand the needs and concerns of organizations that will be subject to the legislation and, hopefully, reassuring businesses and health providers that we will act responsibly in undertaking our new mandate.

If there are two messages that I want to get out to business they are these: First: don’t view compliance with this legislation as a burden, view it as something that will build customer trust in the way you do business, and therefore, something that is good for your business, not an impediment. Second: as the oversight body, our focus will **not** be on finding fault and meting out punishment, but rather on assisting organizations in meeting their responsibilities in a manner that respects their business needs while protecting the legitimate privacy concerns of the individuals’ whose personal information is held by those organizations.

We will also work hard to educate the public and the organizations that will be subject to the legislation, and work to assist those organizations in meeting their new responsibilities. Education is key.

As a first step, we recently posted a detailed Frequently Asked Questions document on our Web site. The FAQ provides as much guidance as possible on what the new legislation will say. It also provides valuable links to privacy resources. We will update the document when necessary, such as when the legislation is actually introduced. We also intend to develop a range of educational material, for both organizations and the public, to explain the legislation and our role as the oversight body.

In summing up my comments on the new legislation, one fact must remain crystal clear. Preparing for this new legislation, and implementing it, will occupy a great deal of my office's energy and resources over the next few years. However, I want to assure everyone that we will not allow this work to distract us from continuing to stress the importance of our access to information regime, especially its role in underpinning open and responsible government.

We will continue to press government to improve the FOI process, including response times; work to increase the routine dissemination of information, and oppose attempts to remove existing institutions from coverage by provincial and municipal access to information laws.

We have a big challenge ahead of us, but I'm very excited about the future and look forward to both the challenges and opportunities that face us in the days and months ahead.

There is one final item I want to mention today, before I wrap up my remarks. In the spirit of transparency and full disclosure, I'd like to tell you that tonight I am launching a new book that I have just written, with Tyler Hamilton, a highly regarded technology journalist. The book is called, *The Privacy Payoff: How Successful Businesses Build Customer Trust*. I wrote this book because businesses kept telling me that while they were beginning to warm to the privacy message, they did not know how to begin to address it – "Where do I start? What do I do?" I couldn't point them to one text – which is what they wanted, so Tyler and I decided to write one! If anyone is interested, it should be available in local libraries by the end of the month and the table of contents and a sample chapter can be accessed from my Web site: www.privacypayoff.com.

Let me end, as always, with a sincere thank you to my staff, who have been working harder than ever – if that's possible – in preparation for the new bill, and to the staff who work diligently, day-to-day, in the IPC's tribunal and mediation services. I am so fortunate to be working with such a dedicated team of professionals.

I would like to thank **you** for your kind attention this morning. I know that you have a great conference ahead of you, and that you'll be hearing from many speakers on a wide range of interesting topics. You have my best wishes for a wonderful two days ahead of you.

Thank you.