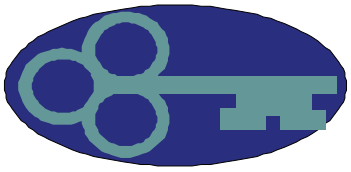


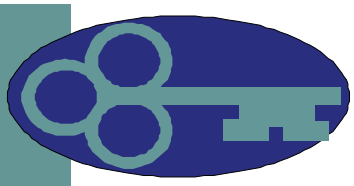
INFORMATION AND PRIVACY COMMISSIONER OF NUNAVUT

ANNUAL REPORT
2005/2006

ANNUAL REPORT 2005/2006

TABLE OF CONTENTS

1.	Commissioner's Comments	2
2.	An Overview of the Act	10
	Background and Purposes of the Act	10
	The Process	13
	The Role of the Information and Privacy Commissioner	15
	Protection of Privacy	17
	Requests for Review	20
3.	Review Recommendations	23
	Review Recommendation 05-018	23
	Review Recommendation 05-019	25
	Review Recommendation 05-020	27
	Review Recommendation 05-021	31
	Review Recommendation 05-022	33
	Review Recommendation 06-023	36
4.	Recommendations	37
	A. Privacy Investigations	37
	B. Boards and Tribunals	38
	C. Educating Boards and Tribunals	39
	D. Municipalities	40
	E. Contracting Out Information Management	41
	F. Openness of Contract Details	42
	G. Private Sector Privacy Legislation	44
	H. Review of Privacy Commissioner's Compensation	45



1. COMMISSIONER'S MESSAGE

It has certainly been an interesting year to work in the information and privacy arena. The longer I continue to do this work, the more I appreciate the importance of the principals embodied in access and privacy legislation across the country. Every year I appreciate more how important open and accountable government is to our way of life. Every year, I worry more about how the expanding use of our personal information is changing our way of life and how we view democracy.

> Any man who would exchange liberty for security deserves neither.
>
> Benjamin Franklin

In 1997, in the case of *Dagg v. Canada (Minister of Finance)* [1997], 2 S.C.R. 403, Mr. Justice La Forest of the Supreme Court of Canada made what has proven to be the most enduring and oft repeated statement about the purpose of access to information legislation

> The overarching purpose of access to information legislation … is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process and secondly, that politicians and bureaucrats remain accountable to the citizenry ...
>
> Parliament and the public cannot hope to call the government to account without an adequate knowledge of what is going on; nor can they hope to par-

ticipate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view. Access laws operate on the premise that politically relevant information should be distributed as widely as possible …

Rights to state-held information are designed to improve the workings of government; to make it more effective, responsive and accountable. Consequently, while the ATIA recognizes a broad right of access ... it is important to have regard to the overarching purposes of the Act in determining whether an exemption to that general right should be granted.

"... there are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations."

~ James Madison

On the other side of the coin are the new technologies which are constantly expanding the ability to collect, combine, store, manipulate, exchange and disseminate information. The use of these technologies undoubtedly promises efficiencies and the possibility of positive change. Human nature, being what it is, is always looking for easier, more efficient ways of doing things and governments are always keen to embrace technology for these same reasons. When they are used without full consideration of the consequences, however, new technologies can have significant negative impact. The state of the world and its politics have accelerated the development and use of such technologies. Technology has been hailed as **the** solution to the threat of terrorism and has been used as a panacea by governments to convince citizens that they are more secure, often without any evidence that that is the case.

> Once you accept that the government has the right to know where you are at all times, to demand that you tell its agents when you move home or to render up your private musings at its behest, then you have changed the nature of the individual's relationship to the state in a way that is totally alien to this country's historic, though ill-defined, covenant between the rulers and the ruled.
>
> Philip Johnston
>
> Telegraph (UK), September 18, 2006

One need only look as far as the seat of democracy, Great Britain, to see how government use of technology can change lives. In England, there are so many closed circuit cameras that every person in England is caught on camera no less than 300 times each day. The movement of vehicles is monitored with the use of roadside devices which read license plates equipped with radio frequency ID chips which hold identifying information about the vehicle and its owner and can follow the progress of a vehicle as it travels from place to place. Starting in 2010, the government plans to implement a universal identity card, including biometric identifiers, which will require every person in the country to have an identity card which will be required to access government programs, including health and welfare programs. The British government maintains the largest DNA database per capita in the world and it is their intention to collect DNA samples for every man, woman and child in the country These are but a few of the many government initiatives in England over the last number of years. . Individually, these government initiatives are reason for concern. Collectively, they are alarming. The surveillance society that George Orwell predicted in his “futuristic” novel, 1984 has clearly arrived. The question is, are we willing to let it invade our lives and change the relationship between the individual and the state?

As my counterpart in Alberta has pointed out, we need to learn from the lessons that history has to offer us. His words from his 2004/2005 Annual Report bear repeating:

So what are the lessons from Normannenstrasse?

- The right of access to information is precious. No government should ever oppose it or impede it on the basis that it is too expensive, too time consuming or only the “trouble-makers” use it
- Accountable governments are better governments
- The right to privacy is precious. There must be limits on what the State is allowed to know about us, even in the name of “security”. Every State has its ideology (yes, even ours) and, if it has the means, a State will tend to “defend itself” against its perceived enemies from within or without
- It is never, ever, a question of “what have you got to hide?” It is always a question of “why do you need to know?”
- Well intentioned people can do bad things.
- History may not judge us as we would judge ourselves.

All totalitarian dystopias, in life and in art, seem to be obsessed with identifying people. The obligatory scene in which a stern, uniformed man demands "your papers, please" has evolved into the automatic scanning of various body parts, but the purpose is always the same: to abolish the right to be anonymous.

By Stan Cox

October 3, 2006

The Canadian government is not immune to these sorts of initiatives. It is, for example, expected to introduce a "lawful access" bill in the next few months which will expand the ways in which governments and law enforcement agencies can collect information without warrant. Over the course of a very few years, it has become increasingly acceptable for governments to gather and

use information in ways which would not have been considered appropriate only a few years ago. This is not unique to federal governments. Provincial and even municipal governments are actively beginning to encroach into this kind of legislation as well. British Columbia's Information and Privacy Commissioner has recently found it necessary to comment on this trend in a report released by his office on August 30th, entitled "Local Governments and the Growth of Surveillance" where he says:

> In recent years, however, it has become more and more common for British Columbia's local governments to enact bylaws requiring businesses to collect their customers' personal information and provide it to local police agencies or licensing inspectors. We have seen in recent years an expansion of the types of businesses that are required to collect customers' personal information, the purposes for such requirements and the types of personal information which must be collected and handed over to police. New information technologies that enable quick and efficient distribution of personal information to police agencies, and its storage, have added a significant dimension to the trend.

He also warns against creating surveillance bylaws which circumvent the normal court process :

> ....this Office strongly believes that municipalities should not be in the business of passing surveillance bylaws. They clearly have privacy implica-

Whenever there's real-time monitoring, we raise alarm bells about the potential invasion of people's privacy. [These] cameras can peer over your shoulder and look at what you're reading. If somebody was doing that in real life, you'd challenge them, but video surveillance takes away our ability to defend our privacy in a way that's quite insidious because it's a faceless technology that doesn't allow us to react.

Murrary Mollard, Executive Director, B.C. Civil Liberties Association.

tions of varying degrees, depending on the nature of the personal information being collected, for ordinary members of the public who are going about their lawful business. Among other things, the bylaws we reviewed contain no measures to ensure that personal information is used properly and is protected against unauthorized use or disclosure. Against the clear privacy impact of such bylaws, it is doubtful that such bylaws are really effective, and there are certainly tools that may more effectively achieve the community safety objectives that the bylaws purport to address. This Office is therefore firmly of the view that municipalities should not pass bylaws compelling citizens to give up their privacy in a wholesale and indiscriminate manner. Consistent with long-standing law and practice in Canada, it should be left to the courts to issue warrants or orders to businesses to turn over customer information on a case-by-case basis where justified.

Terrorism isn't about identity; it's about motivation.

Lembit Opik

Northern Ireland spokesman

Many projects which governments take on have implications for the personal privacy of the general public. Perhaps no single project, however, has more potential to affect the privacy of individual citizens than the national strategy to move toward electronic health records. I understand that there is a federal initiative to create electronic health records throughout the country. I also understand from my discussions with a number of people within Nunavut that electronic health records are being considered but are currently hindered by the lack of internet access. I have no doubt, however, that plans are being made so that when the technology is more readily available, the Government will be

able to avail itself of the efficiencies offered by electronic health records. I would invite the government to focus on the privacy and security of such systems as a preliminary requirement to any such system. As noted by Mary Lysk, a policy advisor for Health Canada in discussing electronic health records "We still have public trust, but trust is not a renewable resource -- once it is lost it may not be regained."

> Since the attacks of September 11 2001, we have seen an erosion of liberty in most established democracies. If he's still alive, Osama bin Laden must be laughing into his beard. For this is exactly what al-Qaeda-type terrorists want: that democracies should overreact, reveal their "true" oppressive face, and therefore win more recruits to the suicide bombers' cause. We should not play his game. In the always difficult trade-off between liberty and security, we are erring too much on the side of security. Worse still: we are becoming less safe as a result.
>
> Timothy Garton Ash, The Guardian, November 17, 2005

In closing, I would once again repeat one of my consistent themes in my annual reports over the last few years and that is that there is a need to encourage a "corporate culture" consistent with the goals of the *Access to Information and Protection of Privacy Act*. I have, in each of my last three Annual Reports, said that this culture must be embraced from the top in order to become ingrained. So long as the Information and Privacy Commissioner's mandate is to give direction and make recommendations only, the purposes of the Act will only be met if there is a commitment on the part of the government as a whole and support from the highest levels of management to the concept of openness. Without this commitment from the top, the ombudsman role of the Information and Privacy Commissioner has limited impact. It is my observation that, for the most part, both the political and bureaucratic leadership within Nunavut has a healthy respect of access and privacy legislation and has taken that leadership role. I am encouraged by the input from and discussions I have had with public bodies in Nunavut that

they are doing a good job in promoting respect for both the letter and the spirit of the law. I therefore encourage the Premier and each of the Ministers to continue to publicly and clearly endorse the goals of the Access to Information and Protection of Privacy Act and to continue to provide leadership in the implementation of principals of openness.

FOI is also part of the constitutional settlement. It's a reminder that Governments serve the people, and not the other way around. It's a reminder that what Government does in our name, on our behalf, and with our money, is a matter of public interest.

Richard Thomas, UK Information Commissioner

It has been, and continues to be, a great privilege to serve the public in the areas of access to information and privacy protection. I would like to thank the legislative assembly for providing me with the opportunity to undertake this important work.

2. AN OVERVIEW

Background and Purposes of the Act

As a general principle, the public has a right to scrutinize the government's financial arrangements with consultants. Otherwise, the principles of transparency and accountability are meaningless.

Brian Beamish

Assistant Information and Privacy Commissioner of Ontario

The "overarching purpose of access to information legislation […] is to facilitate democracy." The legislation does this by insuring that citizens are properly informed so as to be able to participate meaningfully in the democratic process and by insuring that politicians and bureaucrats remain accountable to citizens.

(Dawson J., A.G. Canada v. Information Commissioner of Canada; 2004 FC 431, [22])

The essence of liberty in a democratic society is the right of individuals to autonomy – to be free from state interference. The right to privacy has several components, including the right (with only limited and clearly justified exceptions) to control access to and the use of information about individuals. Although privacy is essential to individual autonomy, it is not just an individual right. A sphere of privacy enables us to fulfill our roles as community members and is ultimately essential to the health of our democracy.

Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing; B.C. OIPC, Oct. 2004, p. 13)

The *Access to Information and Protection of Privacy Act* of Nunavut embodies these purposes in its preamble and in its first section. It is difficult to argue with the underlying philosophy of this legislation that open government makes for good government. Modern government, however, is also a business and the reality of doing business is that some matters must be guarded. The Act recognizes that the government does operate in a business world and tries to balance the right of the public to know with the ability of the government to maintain confidentiality where necessary to allow it to do business. Superior courts throughout the country, up to and including the Supreme Court of Canada, have laid out the rule that access to information legislation should be interpreted in a manner so as to provide for the most access possible and that exceptions to full disclosure should be narrowly interpreted and applied. Where exemptions do apply, the courts have held, they should be applied in the manner which provides the greatest amount of public access and scrutiny.

> Once a government is committed to the principle of silencing the voice of opposition, it has only one way to go, and that is down the path of increasingly repressive measures, until it becomes a source of terror to all its citizens and creates a country where everyone lives in fear.
>
> --Harry S. Truman

The Act also recognizes that government agencies hold considerable amounts of confidential personal information about individuals which must be protected from improper use or disclosure.

The spirit of openness suggested by the Act is clear. However, it is not always easy to apply the law to individual records. Simple common sense is an important and valuable resource in the in-

terpretation of the Act. There is often a fine balancing to be done in applying the Act and interpreting the provisions *vis a vis* specific records and whether or not the exemptions apply. Each request for information must be dealt with on its own terms.

> We shouldn't be so quick to assume that the only thing the watchers care about is criminal acts. Once the government gathers information about you (for example, what you read, who your friends are, what organizations you join), it then has the capacity to use that information in ways that have nothing to do with terrorists.
>
> Geoffrey R. Stone, the Harry Kalven Jr. Distinguished Professor of Law at the University of Chicago

In Nunavut, the *Access to Information and Protection of Privacy Act* was imported from the Northwest Territories on division day. The Act applies and binds all Territorial Government ministries and a number of other governmental boards and agencies. The Act also gives individuals the right to see and make corrections to information about themselves in the possession of a government body.

The regulations identify which government agencies (other than government departments) are subject to the provisions of the *Access to Information and Protection of Privacy Act.* Currently there are 10 ministries and 16 other agencies which fall under the Act. The list of public bodies subject to the Act is amended from time to time to include new agencies as they are created by the government to meet the needs of the people of the Territories.

The Legislative Assembly has on its web site some information about the Act. Through this medium the public can find out how to make a request for information, how to request a correction to personal information and how to ask the Information and Privacy

Commissioner for a Review of a public body's decision in connection with a request for information. It also provides a list of the contact information for the ATIPP Co-Ordinator for each of the public bodies subject to the Act so that individuals requesting information can know who they should direct their inquiries to. The Act also requires that the Government create and maintain an "Access to Information Directory". This Directory has recently been updated and is available on line and in booklet form.

What's going to be taking place over the next 10 years in the privacy space will have profound implications for how we relate to each other socially, economically and politically. We shouldn't be too quick to turn personal data over to market forces.

Jerry Kang, Professor of Law, UCLA

More information about the Act, including answers to a number of frequently asked questions and copies of the Act and its regulations are also available on the recently launched web site of the Information and Privacy Commissioner at http://www.info-privacy.nu.ca, which will also, in time, include copies of the Information and Privacy Commissioner's recommendations and Annual Reports as well as other informative items about access and privacy issues.

The Process

The Act provides that each public body subject to the Act is to appoint an Access to Information and Protection of Privacy (ATIPP) Co-ordinator to receive and process requests for information. Any person may make a request for information and there is no requirement that any person provide an explanation

for why they are making the request. Requests may be made by "proxy" in that an agent may request information on behalf of an individual who does not want to be identified. Although forms are available, requests for information do not need to be in any particular form. The only requirement is that the request be in writing, which would include an e-mail request. Requests are submitted, along with the $25.00 fee, to the appropriate public body. There is no fee if an individual is requesting his or her own personal information.

The right of citizens to access records in the possession or under the control of public bodies is a quasi-constitutional right of the "highest importance in the functioning of a modern democratic state".

Saskatchewan OIPC Report on The Youth Drug Detoxification and Stabilization Act, March 22, 2006

Once a request for information is received, the public body must first identify all of the records which are responsive to the request for information. Once all of the responsive documents have been identified, the public body must review them and determine whether there are any exemptions to disclosure might apply. In vetting the records, the public body must endeavor to provide the applicant with as much of the requested information as possible, while at the same time respecting the limited exceptions to disclosure specified in the Act. Some of the exemptions from disclosure are mandatory and some are discretionary. The discretionary exemptions require the public body to consider whether or not to disclose the information, keeping in mind the general philosophy of disclosure. Public bodies must exercise their discretion in favour of disclosure unless there is good reason not to do so.

Every person has the right to ask for information about themselves. If an individual finds information about themselves on a government record which they feel is misleading or incorrect, a request in writing may be made to correct the error. Even if the public body does not agree to change the information, a notation must be made on the file that the individual has requested a correction.

When Parliament explicitly sets forth the purpose of an enactment, it is intended to assist the court in the interpretation of the Act. The purpose of the Act is to provide greater access to government records. To achieve the purpose of the Act, one must choose the interpretation that least infringes on the public's right of access.

Canada (Information Commissioner) v. Canada (Immigration & Refugee Board) (1998), 140 F.T.R. 140 (Fed. T.D.) at 150,

The Role of the Information and Privacy Commissioner

When an Applicant is unhappy with the response received from the public body, he has the right to seek a second opinion. The legislation provides for an independent review in the person of the Information and Privacy Commissioner. The Commissioner's office provides an avenue of independent non-binding re-consideration for those who feel that the public body has not properly applied the provisions of the Act.

The Information and Privacy Commissioner is appointed by the Legislative Assembly but is otherwise independent of the government. The independence of the office is essential for it to maintain its ability to provide an impartial review of the government's compliance with the Act. Under the Act, a Commissioner is appointed for a five (5) year term. The current Information and Privacy Commissioner was reappointed to her second full term of office in October, 2004 and will serve until October, 2009.

Under the *Access to Information and Protection of Privacy Act* the Information and Privacy Commissioner is mandated to conduct reviews of decisions made by public bodies with respect to the disclosure of public records and to make recommendations to the "head" of the public body involved. In the case of a Ministry, the "head" is the minister. For other public bodies, the "head" is determined in accordance with the regulations. The Information and Privacy Commissioner's role is advisory only, much like that of an ombudsman. She has no power to compel compliance with her recommendations. The final determination on any matter which is raised under the Act is made by the head of the public body who must respond to recommendations made by the Information and Privacy Commissioner within thirty (30) days after receiving the recommendation. The head of the public body may choose to follow recommendations made by the Information and Privacy Commissioner, reject them, or take some other steps he or she feels is advisable based on the recommendation. The decision must be in writing and must be provided to both the person who requested the review and to the Information and Privacy Commissioner.

> We must stand on guard against state access to the databanks of the corporate world. Fears of terrorist attacks or impending pandemics provide superficially attractive justifications for intrusive powers, but the real need for these powers is often not apparent.
>
> Jennifer Stoddart, Privacy Commissioner of Canada

People who have requested information, and who have gone through the review process and are still not satisfied with the response received, have the right to appeal the decision of the public body to the Nunavut Court of Justice. The Information and Privacy Commissioner's Office is not aware of any appeals that have been brought to the court in Nunavut since division day.

In addition to the duties outlined above, the Information and Privacy Commissioner has the obligation to promote the principles of the Act through public education. She is also mandated to provide the government with comments and suggestions with respect to legislative and other government initiatives which affect access to information or the distribution of private personal information in the possession of a government agency.

But as more and more information is passed from one database to another it is important to get the basics right. Trust and confidence will be lost if information is inaccurate or out of date, if there are mistakes of identification, if information is not kept securely or if reasonable expectations of privacy are not met. There must be clarity of purpose - not just sharing because technology allows it. And people must be told how their information is being shared and given choices wherever possible.

Richard Thomas

England's Information Commissioner

PROTECTION OF PRIVACY

The *Access to Information and Protection of Privacy Act* provides rules with respect to the collection, use and disclosure of personal information by government departments and public bodies. Part II of the Act codifies a the Canadian Standards Association's *Model Code for the Protection of Personal Information*, which was recognized as a national standard in 1996. This code sets out ten principals for the protection of privacy:

1. Accountability: an organization is responsible for personal information under its control and that there must be one person within the organization who is designated as the person accountable for the organization's compliance with the privacy rules of the organization.

2. Identifying Purposes: when personal information is collected, the purposes for which it is being collected should be identified at or before the time the information is collected.

3. Consent: there should be a requirement that the individual provides informed consent for the collection, use or disclosure of personal information, except when inappropriate.

The right of citizens to access government-held information is essential in order to hold elected and appointed officials accountable to the people they serve. This is particularly true for details of government expenditures and the public's right to scrutinize how tax dollars are being spent. When government organizations use the services of individuals or companies in the private sector, the public should not lose its right to access this information.

Dr. Anne Cavoukian

Ontario Information and Privacy Commissioner

4. Limiting Collection: the collection of personal information is to be limited to that which is necessary for the purposes identified by the organization and, furthermore, information is to be collected by fair and lawful means.

5. Limiting Use, Disclosure, and Retention: personal information should not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. Further, personal information should be retained only as long as necessary for fulfillment of those purposes.

6. Accuracy: personal information should be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

7. Safeguards: personal information in the possession of an organization must be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness: an organization must be prepared to make readily available to individuals specific information about its policies and practices relating to the management of personal information.

9. Individual Access: on request, an individual should be informed of the existence, use and disclosure of his or her personal information and be given access to that information. Further, an individual should be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Challenging Compliance: that an individual should be able to address a challenge concerning compliance with the above principles to the designated individual or individuals for the organization's compliance.

I think given my mandate as an information and privacy commissioner, what I'm trying to push is that the surveillance society should be a last resort. I think if we raise our children in a climate of fear - and they are not stupid, they know what cameras are - I don't think you'll raise the kind of citizens you ultimately want.

Frank Work

Alberta Information and Privacy Commissioner

Currently, the *Access to Information and Protection of Privacy Act* does not provide for any means of challenging a public body where there is a concern that an individual's personal information has been inappropriately collected, used or disclosed, contrary to the rules codified in the Act. There is no enforcement mechanism to ensure that the rules are followed. Although the Information and Privacy Commissioner has accepted and reviewed complaints of breaches of privacy, there is no legislated mandate for her to do so. Nor is there any obligation imposed

by the Act for public bodies to co-operate in a privacy review, or any obligation for the public body to take any steps in response to recommendations which may be made by the Information and Privacy Commissioner with respect to a breach of privacy.

This culture shift should be based on the principles that information should be available to the public, and that necessary exemptions from the right of access should be limited and specific. Exemptions should not simply be claimed because they are technically available in the Act; they should only be claimed if they genuinely apply to the information at issue."

Ann Cavoukian

Order (MO-1947)

REQUESTS FOR REVIEW

Under section 28 of the *Access to Information and Protection of Privacy Act,* a person who has requested information from a public body, or a third party who may be affected by the disclosure of information by a public body, may apply to the Information and Privacy Commissioner for a review of the public body's refusal. This includes decisions about the disclosure of records, corrections to personal information, time extensions and fees. The purpose of this process is to provide an impartial avenue for review and independent oversight of discretionary and other decisions made under the Act.

A Request for Review must be made in writing to the Information and Privacy Commissioner's Office. This request must be made within 30 days after the public body provides its response to a request for information. There is no fee for a Request for Review.

When the Information and Privacy Commissioner receives a Request for Review, she will take steps to determine what records

...are all these new powers necessary? Obtaining personal information without a warrant or establishing new tracking capabilities will obviously make life easier for law enforcement authorities. The price for these new powers should not be underestimated though as lawful access will lead to reduced privacy and increased consumer costs. Given the high price, it should fall to law enforcement to make the case that their existing powers are inadequate. They have thus far failed to do so, neglecting to point to a single case where current Canadian law ultimately resulted in a botched investigation or failed prosecution.

Michael Geist

Canada Research Chair in Internet and E-commerce Law at the University of Ottawa, Faculty of Law

are involved and obtain an explanation from the public body explaining their reasoning with respect to why certain records may not have been disclosed. In most cases, the Commissioner will request and receive a copy of the responsive documents from the public body involved and will review the records in dispute. Sometimes, when there is an allegation that the public body may not have fully responded to the request and is, for some reason, "hiding" records, it may be necessary for the Information and Privacy Commissioner to attend the government office to physically examine the public body's files. Generally, the Information and Privacy Commissioner will attempt to mediate a resolution to the dispute before undertaking the full review process. In several cases, this has been sufficient to satisfy the parties. If, however, a mediated resolution does not appear to be possible, the matter moves into an investigation process. All of the parties involved, including the public body, are given the opportunity to make written submissions on the issues.

In the 2005/2006 fiscal year, the Information and Privacy Commissioner's Office received seven (7) new requests for review. In addition, there was one privacy complaint and four requests that the Information and Privacy Commissioner provide comment on government initiatives or with respect to how the act might affect the business of government.

...the inevitable combining of private and public sector databases will increasingly fuel state law enforcement and national security activities, including through sophisticated data mining techniques that will undoubtedly be secret and entirely or largely non-reviewable.

David Loukidelis

Information and Privacy Commissioner

Six review recommendations were made during the 2005/2006 fiscal year, including two dealing at least in part with privacy complaints. One Request for Review was withdrawn before recommendations were made. The Information and Privacy Commissioner provided detailed comments with respect to three of the four requests for comment and exchanged correspondence with the public body in the fourth instance, but without providing formal comments.

Of the new requests for review received in 2005/2006, the following public bodies were involved:

Department of Education	2 requests
Health and Social Services	2 requests
Nunavut Business Development Corp	1 request
Economic Development and Transportation	1 request
Department of the Environment	1 request

3. REVIEW RECOMMENDATIONS

Review Recommendation #05-18

It is imperative that businesses understand that implementing responsible information practices will not only help to combat identity theft but also build consumer confidence, develop a leadership position, reduce the cost of crisis management, and ultimately protect the corporate brand. Failing to do so will leave companies, and consumers, wide open to identity theft and other risks. I urge businesses in Ontario to be proactive – to develop a "culture of privacy" by establishing accountability, identifying vulnerabilities, developing processes, training staff, and evaluating their data protection practices on a regular basis because privacy is good for business.

Dr. Ann Cavoukian

Ontario Information and Privacy Commissioner

2005 Annual Report

This review involved a member of the press who was seeking to obtain a copy of a report prepared by a private consultant at the request of the Department of Health and Social Services with a view to analysing the efficiency of the health delivery system at the Baffin Regional Hospital.

The public body took the position that the report was an instrument of internal management, enabling hospital management to improve hospital functions and efficiency and qualified as "advice and recommendations" and was, therefore, subject to a discretionary exemption from disclosure pursuant to section 14 of the Act. They were concerned about the impact that releasing the document might have on the Department's ability to ascertain candid input and engage in the type of consultative processes that often form the key components of "these types of reports".

The Applicant, on the other hand, argued that "the department's need to access information on how to improve their system does not trump the public's right to know what is being done on their

behalf". He considered the matter to be an accountability issue and suggested that the Government of Nunavut owed the public nothing less than "full accountability and transparency".

> ... there are indications of a trend developing whereby personal information collected for national security purposes may be used more and more for ordinary law enforcement purposes. Such a trend blurs the traditional division between the state's role in protecting the public from domestic and foreign national security threats and its role in enforcing ordinary criminal and regulatory laws, a blurring of roles that could have significant implications for privacy.
>
> David Loukidelis
>
> British Columbia Information and Privacy Commissioner, Annual Report 2005

The Information and Privacy Commissioner reviewed the report and concluded that although there were parts of it which were clearly intended to be analysis and recommendations, much of what was in the report was merely a recitation of facts. She felt that the factual parts of the report could not be classified as "advice or recommendations" and that those parts of the report should be disclosed. She further concluded, however, that other parts of the report were properly classified as "advice or recommendations" and were, therefore, eligible to be withheld pursuant to section 14 if the public body, in the exercise of its discretion, chose not to disclose that information. She indicated, however, that there was no clear indication that the public body had exercised its discretion before deciding not to disclose those parts of the record.

The recommendation was to disclose those parts of the reports which did not fall under section 14. For those parts of the report which did fall under section 14, the Information and Privacy Commissioner recommended that the public body should clearly exercise its discretion and consider whether or not to disclose the record, providing the Applicant with a full analysis of the reasoning used in exercising that discretion.

The recommendations were accepted and most of the report was disclosed. Where the public body chose not to disclose sections of the report, they provided the Applicant with a detailed explanation of how it exercised its discretion.

.

The principle of open government is a linchpin of democracy because it allows citizens to scrutinize the activities of elected officials and public servants to ensure that they are acting in the public interest. One pillar that supports open government in Ontario is the province's freedom of information laws that give people the right to access government-held information.

Dr. Anne Cavoukian

Ontario Information and Privacy Commissioner

Making Municipal Governments More Accountable—The Need for an Open Meetings Law in Ontario

Review Recommendation #05-019

This Request for Review involved an employee who was seeking information in relation to a disciplinary matter in which he found himself involved. He was seeking to obtain copies of all correspondence between certain individuals within the public body in which the disciplinary matter was discussed.

Although the Applicant had received a response, some information in the records had been severed and he felt that the edited items should not have been blacked out. In addition, he was convinced that there were other records which were responsive to his request, but which the public body had deliberately failed to provide.

The public body, took the position that, although there were other documents which mentioned the Applicant and were created in connection with the disciplinary issue in question, there were no other documents which were responsive to his

request because any other documents that otherwise fit the description of the information the applicant was seeking were created outside the dates for which the Applicant had asked for records. Further, they advised that if the record did not fit the exact description of the kind of record requested (for example, there were minutes of meetings and other notes which, the department said, were not "correspondence" and were not, therefore provided) and if the correspondence was sent or received from someone not specifically named in the Applicant's request, the record was also not provided.

The Information and Privacy Commissioner found that the public body had complied with the narrow technicalities of the Act. She also concluded, however, that in a situation such as this there should be some onus on the public body to communicate with the applicant to determine exact what it is that the person is looking for so as to avoid multiple requests for information as well as the appearance that something is being "hidden". In this case, she pointed out that the public body clearly had doubts about the scope of the request being made to the point that they sought legal advice as to what they "had to" disclose. She thought that in such circumstances, clarification should have been sought from the Applicant instead of seeking legal advice as to how to narrow the response provided to the Applicant. People who apply for access to records are not all going to be able to articulate their requests clearly. The legislation

No fault can be found with a public body for applying the exceptions to disclosure: it is their right, their duty. The Information and Privacy Commissioner exists to make the determination of whether they did so properly. ……But what can be faulted is behaviour calculated to thwart, frustrate or stonewall the functioning of the law. Not just because it is the law, although that is certainly reason enough, but because it was introduced as, and remains a pillar of, government accountability.

Frank Work

Alberta Information and Privacy Commissioner, Remarks to the Access and Privacy 2005 Confer-

recognizes this and puts a positive onus on the public body to work with Applicants to ensure they get all of the information they are seeking. Failure to do this not only makes it look like the public body has something its trying to hide, but it creates more work when the Applicant comes back to get the information he missed the first time around.

The recommendations made by the Information and Privacy Commissioner were accepted.

Review Recommendation #05-020

The Applicant in this case was also a government employee. He complained that the Department of Culture, Language, Elders, and Youth (CLEY) had not responded fully to his request for review. At the same time, he complained that his personal information had been improperly disclosed to third parties without his consent and in a fashion which was calculated to embarrass him with his employer.

In this case, CLEY took exception to the way in which the Applicant had handled a certain situation as a private citizen. In fact, they alleged that the Applicant's actions were contrary to law. The Applicant was an employee of the government, but in another department. A series of correspondence went back

This is a crucial time in our democracy and for our democratic institutions, the Access to Information Act being one of those institutions. It has become easier and easier, each and every month since September 11, 2001, to justify more and more secrecy in the name of security, as well as to justify more and more intrusion into personal privacy.

Hon. John Reid

Information Commissioner of Canada

THE ACCESS ACT – MOVING FORWARD – A COMMISSIONER'S PERSPECTIVE"

[2005-9-8]

Countless individuals reported that senior officials, both political and administrative, find various ways to deny providing information to the public."

Justice John H. Gomery, Restoring Accountability: 2nd Report of the Commission of Inquiry in the Sponsorship Program and Advertising Activities, 2006
Cf. pp. 43-44

and forth between CLEY and the Applicant. Copies of this correspondence appeared to have been fairly widely distributed by CLEY in the form of "carbon copies" to the Deputy Minister in the Applicant's department, to the Applicant's own supervisor, and to a senior executive with a non-governmental corporation with which CLEY had an ongoing relationship. This correspondence contained allegations about inappropriate and allegedly illegal conduct on the part of the Applicant. The Applicant adamantly and unconditionally denied the truth of the allegations and described them as "malicious, slanderous and defamatory".

In dealing with the allegations made, the Applicant requested that CLEY provide him with certain information, most of which was provided. One of the items which he requested, however, was documentary proof that certain individuals within CLEY had the legal authority to take certain steps which they had proported or threatened to take to take against the Applicant. No such documentation was provided.

The public body relied on a section of the Nunavut Act which set out a number of rules about the issue at hand in the Request for Review. There was nothing in the material which the department provided which answered the Applicant's request. The public body admitted that they simply "surmised" that the sections of the Nunavut Act which created certain obligations on

"There is undoubtedly a need for certain kinds of government information to remain confidential. This need is reflected in the many exemptions to access set out in the *Access to Information Act.* The Act itself proclaims, however, that as a general rule 'government information should be available to the public', and the 'necessary exceptions to the right of access should be limited and specific'. If this legal principle is to have its full effect, however, the bureaucracy must experience a profound cultural shift."

[La Forrest Report, p. 46

the general population of Nunavut gave the Minister the "legal authority" to police the Act and that the two individuals in question, being responsible to the Minister, thereby had concurrent authority to do so.

The Information and Privacy Commissioner concluded that it would seem logical to assume that there must be some record which would confirm who had responsibility to enforce the rules in question. She agreed with the Applicant that this part of his request for information had not been complied with. She recommended that the matter be considered again and, if there were in fact no documentation specifying who had the authority to enforce certain parts of the Nunavut Act, the Applicant should at least be advise what steps were taken to find the requested information.

The same applicant also complained that the correspondence in which CLEY accused him of wrongdoing had been deliberately distributed widely and in a way calculated to negatively affect his employement and his relationship with an outside agency. The Information and Privacy Commissioner found that much of the information in the letter in question was the Applicant's personal information. She reviewed section 48 which outlines the circumstances in which personal information can be disclosed without the Applicant's consent and concluded that none of those circumstances applied in this case. She concluded, therefore,

that there was, in fact, an improper disclosure of the Applicant's information.

The Information and Privacy Commissioner futher cautioned the public body about sending documents containing personal information by means of fax transmission when they do not know that the receiving fax is private.

Sometimes protecting privacy looks like trying to stem a flood with a snow shovel: you push the water away from in front of you but it rushes past you everywhere else.

Frank Work

Alberta Information and Privacy Commissioner, Remarks to the Access and Privacy 2005 Conference , June, 2006

The Information and Privacy Commissioner concluded that in sending copies of the letter containing allegations against the Applicant to his Deputy Minister, to his immediate supervisor and to the third party non-governmental organization, the public body had wrongfully breached his privacy. She recommended that steps be taken to correct that error as far as is possible by writing a letter to each of these recipients acknowledging that the letter should not have been copied to these parties and that the contents of the letter should remain confidential. She further recommended that the Applicant should receive a full and complete apology for the improper disclosure of his information and that a copy of the apology should be placed on his personnel file if the Applicant requested it.

The head of the public body acknowledged the recommendations made with respect to the privacy issues and indicated that they would be taking steps to address the

Applicant's concerns in a fair and timely way, and that a letter would be sent to the Applicant acknowledging the breach of his privacy.

The privacy challenges posed today in contemporary government are compounded by increased globalization and heightened concerns over national security, combined with higher public expectations that the federal government will respect the fundamental privacy rights of the public it serves. The challenges are not unique to the federal government – or to the Canadian federation. These issues cut across many jurisdictions and even defy the very notions of national boundaries and the exercise of sovereignty.

Office of the Privacy Commissioner of Canada

Government Accountability for Personal Information—Reforming the Privacy Act

Review Recommendation #05-021

The Applicant in this case, a member of the press, requested a copy of a report which had been prepared for the Department of Education called "Aaqqigiarniq, Time to Move Forward". A copy of the report was provided, but sections of it were omitted or otherwise severed.

The department indicated that they considered those portions of the report which were not disclosed to be recommendations or advice and that they were, therefore, exempt from disclosure pursuant to section 14 of the Act. They argued that the portions of the report which were excluded involved the results of interviews with individual staff of Nunavut Arctic College and to disclose them "could have deleterious effects on individual staff of Nunavut Arctic College, relations between the College, Departments of the Government of Nunavut , and third parties, and could compromise the college's competitive position". They also stated that the revelation of the excluded sections "could compromise the strategic planning by the College and the Department of Education". No explanation or reasoning was provided with respect these predictions.

Before Canadians go online to do business with the government, they want assurance that government systems are secure and that their personal information will be properly protected. As more and more government services are offered online, individuals and businesses need to have confidence that the information they share will be well protected.

Sheila Fraser

Auditor General for Canada

The Applicant took the position that it appeared that the report was a fact finding report that made recommendations that were not directed at any specific course of action which would ultimately be accepted or rejected by its recipient and that the survey of staff and students was simply an element of the fact-finding report, and not a consultation the met the requirements of section 14(1).

The Information and Privacy Commissioner reviewed the report and made specific recommendations with respect to each of the sections of the report which had been excluded. In some instances, the Commissioner conceded that the deleted information was "advice or recommendations" which were subject to a discretionary exemption. In other instances, the Commissioner did not agree with the public body's assessment and recommended that those portions be disclosed. Where the Commissioner found that a discretionary exemption applied, she recommended that the public body provide an explanation for the way in which the discretion was exercised so as to clearly show that discretion had, in fact, been exercised.

The recommendations made were accepted and most of the report was provided to the Applicant with only very few sections being excluded.

Review Recommendation #05-022

This was a review requested by a former employee of the Department of Health and Social Services. He had requested documents in which he was discussed by certain other individuals from three different departments. Between them, the public body had identified more than 1700 records which were responsive to the request for information. There were a number of records to which access was denied, and a number of records which were disclosed only partially.

The public bodies argued that most of the records which were not disclosed were withheld pursuant to the discretionary exemption allowed in section 14 of the Act (advice or recommendations). It was their position that certain "audits" which they had withheld involved analyses of Government of Nunavut (GN) operations and advice with respect to how those GN operations should proceed in the future and it was, therefore, considered "prudent" not to disclose them because they identified gaps in accounting and reporting in the GN. E-mail records and notes from interviews used to prepare the audits and leading up to them were not disclosed, again because the public body felt that the disclosure would reveal gaps in the accounting and reporting of the GN. The public bodies also relied on section 14 to refuse access to information relating to the competition which had lead to the Applicant being hired .

Simply publishing a privacy policy does not make a business privacy compliant. Organizations must ensure that all employees are aware of and adhere to privacy policies. When there are breaches, these must be brought to the immediate attention of the organization's privacy officials,

Jennifer Stoddart

Privacy Commission of Canada

Report into CIBC's misuse of customer records

They claimed that the disclosure of this information would reveal administrative information such as salary ranges and salary negotiations relevant to future GN hiring and employment decisions.

Canadians are increasingly aware of their privacy rights and expect a reasonable and balanced approach to a national strategy to combat terrorism with greater accountability, transparency and oversight. The absence of serious evidence of the effectiveness of the extraordinary broad powers under the Anti-terrorism Act need to be questioned so security threats do not end up abolishing the very freedoms and democracy we claim to be defending"

-- Jennifer Stoddart,

Privacy Commissioner of Canada

May 9, 2005

The Applicant took the position that all of the information requested was his personal information. He suggested that the fact that the public body had simply refused to disclose all records subject to a discretionary exemption indicated that no discretion had, in fact, been exercised. He suggested, as well, that not every record which had been denied under section 14 consisted entirely of advice or recommendations. He also suggested that the public body failed to apply section 14(2), in particular, s. 14(2)(f) which says that the discretionary exemption did not apply where the record was an instruction or guideline issued to officers or employees of a public body.

The Information and Privacy Commissioner examined every record and commented on each individually. The most prevelant comment by the Commissioner was that when a discretionary exemption is relied upon to refuse disclosure, the public body has an obligation to advise the Applicant the factors that went into the exercise of the discretion. When a discretion is given, she suggested it was not sufficient just to apply that discretion so as to deny disclosure. The discretion must be actively exercised and, to show that that is the case, the public

body should provide the Applicant with an indication of the factors that went into the exercise.

Most of the recommendations made by the Information and Privacy Commissioner were accepted. However, despite the repeated suggestion that where the discretion is exercised it should be seen to be exercised, no explanations were given where the minister chose to exercise his discretion to deny access.

Most of us are seduced by the convenience of technology, and often live a life connected by mobiles, email and the internet. But it is only a matter of time, some say, before "function creep" takes us to places we thought we would never go. Where the possible becomes the inevitable, where governments, business and industry will do it just because they can.

Ruth Pollard

Sydney Morning Herald (NSW, Australia), June 13, 2005

Review Recommendation 06-23

This review arose out of a request made to the Department of Health and Social Services by a former government employee. This was the second request by the same individual for similar information. Although all of the responsive documents had been provided to the Applicant in connection with an earlier request, they were provided a second time.

The Applicant had two complaints about the response he had recieved. Firstly, he indicated that there were records missing from the response. He initially indicated that he had proof that other documents existed and would provide them in support of his allegation. That documentation was, however, never recieved and the Information and Privacy Commissioner

concluded that there was nothing to suggest that there were any further responsive documents.

The second of the Applicant's complaints was that he did not receive transcripts of telephone calls which he said had been transcribed. In its initial response, the public body indicated that they had misunderstood the request as the Applicant had requested transcripts of telephone calls "between" certain individuals. They indicated that the only things that had been transcribed were telephone messages left on answering machines. When the Applicant clarified his request through his submissions to this office, the transcripts were provided. The Information and Privacy Commissioner came to the conclusion that the failure to disclose the transcripts initially was an honest error and not done with the intention of avoiding disclosure.

No further action was recommended and the recommendations were accepted.

The more another individual or body can know about you, the more power and leverage they have over you. If we look at human history, we see that you cannot rely on the powerful people, whether they're elected or not, to do the right thing. Privacy is just essential to freedom."

Darrell Evans, Executive Director, British Columbia Freedom of Information and Privacy Association.

4. RECOMMENDATIONS

A. Privacy Investigations

> In times of crisis, privacy is going to lose, and that is not OK. Privacy and security are not mutable forces that can rise and fall depending on our level of crisis. They are immutable.
>
> Nuala O'Connor Kelly
>
> Chief Privacy Officer, Homeland Security Department

I have recommended in past Annual Reports that steps be taken to amend the *Access to Information and Protection of Privacy Act* so as to include a means for individuals to redress the inappropriate collection, use and disclosure of their personal information. Although the Act sets out detailed rules governing collection, use and disclosure, there do not appear to be any consequences for breaches of these sections, and no way for an individual to seek redress if their information is wrongfully used. There is, quite simply, no enforcement mechanism. The review provisions in the Act apply only on access matters. Although I have, as Information and Privacy Commissioner, accepted privacy complaints and have investigated those complaints and provided recommendations, there is no statutory obligation for any public body to co-operate with such an investigation and, perhaps more importantly, there is nothing to require the public body to address any recommendations made. Rules respecting the protection of privacy are fairly hollow if there is no review mechanism and no recourse for failure to comply with the rules. In the Northwest Territories, this gap in the legislation has been addressed by amending the Act to add provisions which specifically give the Information and Privacy Commissioner the authorization and power to review privacy complaints

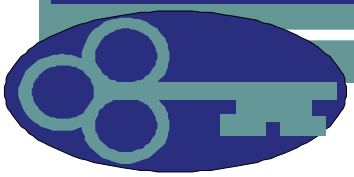
and to provide recommendations. Public bodies are now required to respond to privacy recommendations made within 90 days. This seems to be a fairly obvious oversight in the original legislation and it is my recommendation that the necessary amendments be made to the Act to allow the public a means to address privacy breaches by public bodies.

The reason for the creation of legal obligations to maintain and not to destroy government records, in addition to similar rules in the access to information regime, is that the rationale for mandatory record-keeping does more than facilitate public access to information: it ensures good government and accountability, a requirement consistent with the theme of the Commission's overall recommendations.

[Gomery Report #2 at pp. 180-181]

B. Boards and Tribunals

Governments delegate many functions to boards and tribunals which are populated by individuals who are not government employees. These boards and tribunals are subject to the *Access to Information and Protection of Privacy Act*, but because the members of these organizations are not government employees, there is some concern that their records are not being adequately protected, both in terms of retaining the records in accordance with acceptable records management standards and in terms of protecting personal information which might be contained in such records. What is the role of individuals appointed to government boards and tribunals? What are their obligations in terms of the records they produce? What, if any, policies are in place to ensure adequate records management and appropriate protection of personal privacy? Do they keep their own records and their own filing systems, outside of the government management system? These are all questions which need to be addressed in one way or another. I would,



therefore recommend that the Act be amended to clarify that individuals appointed to public bodies are specifically subject to the Act by virtue of their appointment by a government agent. This would create for appointees the same responsibilities which government employees have with respect to the collection, use and disclosure of personal information. It would also clarify that records in the hands of such appointees and the papers they create as members of such boards and agencies are subject to access to information requests. It is further recommended that steps be taken to create policies for all boards and agencies to establish the necessary protocols for proper handling of records produced by them. These would include policies for proper security of records, and appropriate retention and destruction rules as well as policies which direct what happens to records of an individual sitting on a board his or her term ends or they quit.

> The mere fact that someone has communicated with an HIV support group, an abortion clinic, an alcoholism recovery website or support group, a gay website or support group, conveys sensitive personal information, if only the fact that the individual has at least an interest in any one of these issues. In fact, simply knowing that someone has an interest in a topic, without knowing exactly what that interest is, can be more harmful than having access to the content so as to know what the actual interest is. Many things can be inferred by the simple fact that someone happened to have visited a certain website, or sent a certain email.
>
> Frank Work, Alberta Information and Privacy Commissioner
>
> Excerpt from a letter to The Honourable Irwin Cotler PC, MP Minister of Justice and Attorney General of Canada, April, 2005

C. Educating Boards and Tribunals

On the same theme, I would continue to encourage the Government of Nunavut to do an inventory of all boards, tribunals and agencies to which it appoints members and to ensure that these organizations are both aware of and knowledgeable about the rules regarding access to information and the collection, use, disclosure and retention of personal information. In the best case scenario, all persons appointed to such bodies should be required to undertake basic ATIPP training. As a minimum, the

leadership of such bodies (Executive Directors and Board chairs) should be required to receive basic training in the principals of access and privacy issues and be required to update that training periodically. Although the problem has not yet arisen in Nunavut, there have been several instances in the Northwest Territories where arms length boards and agencies have had access requests made of them and they have not had the knowledge to deal with them properly.

One of the fundamental contrasts between free democratic societies and totalitarian systems is that the totalitarian government relies on secrecy for the regime but high surveillance and disclosure for all other groups, whereas in the civic culture of liberal democracy, the position is approximately the reverse

Professor Geoffrey de Q Walker, Dean of Law at Queensland University.

D. Municipalities

Since my first Annual Report, I have maintained that municipalities should be subject to access and privacy legislation. Not only is it important that municipal authorities be accountable to the public through access to information rules, it is also important that municipalities should have rules regarding how they gather, use and disclose personal information about individuals. Municipalities gather and maintain significant information about individuals in their day to day dealing with the business of running communities. Every jurisdiction in Canada, except for Nunavut, the Northwest Territories, Yukon, New Brunswick, and Prince Edward Island have legislation which addresses access and privacy at the municipal level. It has been suggested that municipalities are covered by the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) so that no specific legislation is needed to address the issues at the municipal level.

> We are a society that is in love with the techno fix. Crime? Put up cameras. Drugs? Bring in drug testing. The technology is so easy to apply. Put up some surveillance cameras. Watch the kids in the halls. See who comes and goes. If there is an incident, there is tape. Drug and alcohol test all students. Have students carry ID with RFID chips that can be tracked. Or track them via their cell phones. There are arguments in favour of this: safer schools, more effective enforcement of rules. But in our rush for the techno fix, we are not very discerning in terms of cause and effect.
>
> Frank Work, Information and Privacy Commissioner of Alberta
>
> Privacy Rights in Schools: A Perspective from Alberta's Privacy Commissioner
>
> September, 2006

With respect, I disagree. PIPEDA applies to "commercial activities" only and much of what municipalities do would not be considered "commercial activity". Furthermore, PIPEDA does not apply to protect the information of municipal employees. Finally, PIPEDA addresses only privacy issues. It does not address the right of citizens to have access to public records of municipalities. I would again encourage the Legislative Assembly either amend the *Access to Information and Protection of Privacy Act* to include municipalities as "public bodies" or to create separate legislation which deals with access and privacy matters at the municipal level so as to provide consistent access and privacy rules to municipalities within Nunavut and appropriate protection of the personal information of its citizens.

E. Contracting Out of Information Management

In the last eighteen months, an issue which has become significant in many jurisdictions in Canada is the contracting out of what have traditionally been government activities. In many jurisdictions, for instance, motor vehicle registries have been privatized. I would once again encourage the Government of Nunavut to take a close look at its contractual relationships with outside service providers and outsourcing, particularly in those sensitive areas which include the collection, retention and use of financial and/or medical information of individual residents of Nunavut. I have previously recommended that there be clear

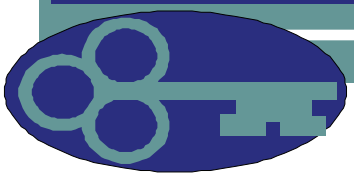
provisions included in all contracts for such services to compel contractors to comply with the *Access to Information and Protection of Privacy Act* and making them subject to access requests and responsible for the privacy of individuals whose personal information they acquire as a result of the contractual relationship. This has become a major concern for many of my provincial counterparts. This is a particularly sensitive issue when it relates to health information management work.

> The right of citizens to access government-held information is essential in order to hold elected and appointed officials accountable to the people they serve. This is particularly true for details of government expenditures and the public's right to scrutinize how tax dollars are being spent. When government organizations use the services of individuals or companies in the private sector, the public should not lose its right to access this information.
>
> Dr. Ann Cavoukian
>
> Ontario Information and Privacy Commissioner
>
> 2005 Annual Report

F. Openness of Contract Details

One of the most predominant political issues which I have observed in Nunavut since its inception has been the concern about how government contracts are awarded and how public funds are spent. The public wants to know who is getting government contracts and what they are being paid. As has been pointed out by Dr. Anne Cavoukian, the Ontario Information and Privacy Commissioner in her most recent annual report:

> The right of citizens to access government-held information is essential in order to hold elected and appointed officials accountable to the people they serve. This is particularly true for details of government expenditures and the right of the public to scrutinize how tax money is being spent. When



government organizations use individuals or companies in the private sector to help develop, produce or provide government programs or services, the public should not lose its right to access this information. Any government office planning on hiring a consultant, contractor, etc., should make it clear to that future agent that the *default position* is that the financial and all other pertinent information related to the contract will be made available to the public, except in rare cases where there are very unusual reasons not to do so.

> There was, of course, no way of knowing whether you were being watched at any given moment. How often, or on what system the Thought Police plugged in on any individual wire was guesswork. . . . But at any rate they would plug in your wire whenever they wanted to. You had to live-did live, from habit that became instinct-in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinized.
>
> George Orwell
>
> "1984"

I would echo these comments and encourage public bodies to make it clear that private companies contracting with the government should do so knowing that the accountability of government may well require that details of the contract will be shared with the public unless either the government or the company can provide cogent evidence that the disclosure of those details would be reasonably expected to harm the financial interests of either the government or the business. This should be established as a formal government policy. The policy should include a listing of the sorts of circumstances which may restrict disclosure but make it clear that the onus will be on the contractor to prove the facts necessary to justify a refusal to disclose.

G. Private Sector Privacy Legislation

It will come as no surprise that I continue to support the creation of "made in the north" legislation to deal with the protection of personal information in the private sector. As I noted in my opening comments, technological advancements, easy access to databases, the unrestricted ability of companies to buy and sell personal information, and the increasing reliance of both businesses and the public on computers means that our personal information is at greater risk than ever. Businesses need guidelines and, in some cases, the rule of law, to regulate the use they make of personal information. In order to attract businesses to the north, the public needs to know that their personal information is safe and secure and will not be used except for the purpose it is provided. The people of Nunavut need to be able to do business with local businesses knowing that there are rules of law which limit what those businesses can do with their personal information. Although there is federal legislation which purports to govern business in the private sector, it is of limited practical effectiveness because it is administered by the federal Privacy Commissioner's office in Ottawa. It is to be noted as well that PIPEDA does not protect the privacy of employees in the private sector unless the employee is working in a federally regulated business such as banking, airlines, telecommunications or interprovincial transportation. Yet employers have records relating to some of their employee's most sensitive personal information including income, health and family relationships. It is important that this issue be addressed, particularly as more national and international corporations set up business in the north.

> One of the worries we have, is the rather casual use of biometric data. If children get used to thinking biometric data can be used for trivial purposes - and a school library is a rather trivial purpose - how do they learn to be careful where they put their fingerprints and iris scans? The more you use biometric data and the more casually you use it, the more scope there is to exploit it.
>
> Terri Dowty, Director of Action for the Rights of Children

H. Review of Privacy Commissioner's Compensation

I would respectfully request that there be a review of the Information and Privacy Commissioner's compensation package. The work involves a level of expertise which in other jurisdictions is compensated at a Deputy Minister's level. The contract to provide the services of the Information and Privacy Commissioner provides for compensation at an hourly rate which is currently set at a relatively low level, in fact less than a lawyer undertaking legal aid files would be paid. That hourly rate has not changed since I first undertook the position seven years ago. In the circumstances, I respectfully request that the hourly rate be reviewed with a view to implementing a reasonable increase.

All of which is respectfully submitted.

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner

There are risks of going too far down the route of what is often called a surveillance society, that is the fundamental rationale of data protection law. There are risks of having unacceptable volumes and details of personal information, especially with major, heavily concentrated databases. There are practical risks of inaccuracy, loss of accountability where information is shared, risks of lack of security.

Richard Thomas,

UK Information Commissioner
28 Nov 2005