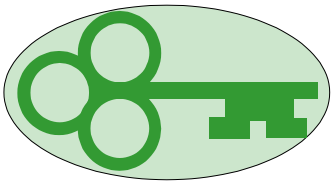


Office of the Information and Privacy Commissioner

Annual Report 2006/2007

Elaine Keenan Bengts
P.O. Box 262
Yellowknife, NT
X1A 2N2

October 10th, 2007

NUNAVUT
INFORMATION
AND
PRIVACY
COMMISSIONER

5018 – 47th Street
P.O. Box 262
YELLOWKNIFE, NT
X1A 2N2

October 16, 2007

Legislative Assembly of Nunavut
P.O. Bag 1200
Iqaluit, NU
X0A 0H0

Attention: Hon. Peter Kilabuk
Speaker of the Legislative Assembly

Dear Sir:

I have the honour to submit to the Legislative Assembly my Annual Report as the Information and Privacy Commissioner of Nunavut for the period of April 1st, 2006 to March 31st, 2007.

Yours truly,

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner

In Yellowknife: 867-873-8631 ♦ Toll free: 888-521-7088 ♦ Fax: 867-920-2511 ♦ E-mail: privacy_comm@internorth.com

INDEX

I. COMMISSIONER'S MESSAGE

> 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.
>
> The Offices of the Information and Privacy Commissioners: The Merger and Related Issues
>
> Report of the Special Advisor to the Minister of Justice
>
> Gérard V. La Forest
>
> November, 2005

It has been ten years since I entered the world of access and privacy when I was appointed as the first Information and Privacy Commissioner of the Northwest Territories prior to division. The world was a different place ten years ago. The pace of technological advance is mind boggling. Terrorism close to home has changed the way many people think and react to the world around them. With these changes come changes in public opinion and values. Things that would have been unthinkable ten years ago as unacceptable invasions of our privacy have become commonplace and even accepted. Closed Circuit Televisions (CCTV's) which monitor our movements are now everywhere. Some airports now use scanning machines which, quite literally, see right through clothing. Radio Frequency Identity Devices (RFID's) are being used to monitor everything from how much garbage is disposed of by each household in Britain, to tracking the movements of children in schools. DNA databases are proliferating and governments and police forces are finding ways to expand the use of these databases. Secret "No Fly" lists with few, if any, rights of appeal and no oversight now exist in most parts of the western world. In short, Governments everywhere are struggling with how to maintain both privacy and security, and how to balance those with the basic right of every citizen in a democratic society to hold their governments to account by having access to government records and their own personal information. With this backdrop, it is my growing conviction that access and privacy laws have growing significance and importance to democracy, regardless of how large

or small the population in that democratic entity might be. At the Territorial level, we may not be dealing with the issues that will impact on global attitudes and perceptions. But we have to keep our eye on the big picture and do what we can to protect democracy in our little corner of the world.

In the case of General Motors Acceptance v. Saskatchewan Government Insurance, [1993] S.J. No. 601 at [11], the Saskatchewan Court of Appeal described that province's Freedom of Information and Protection of Privacy Act as follows:

> The Act's broad provisions for disclosure, coupled with specific exemptions, prescribe the "balance" struck between an individual's right to privacy and the basic policy of opening agency records and action to public scrutiny

Fears of terrorism must not become a convenient excuse for the destruction of the protection of privacy.

Jennifer Stoddart

Information and Privacy Commissioner of Canada

The finding of that balance is not always easy. If I have learned anything in the last ten years, it is that the *Access to Information and Protection of Privacy Act* is not as easy to apply as it might appear at first blush. The Act is a complex one that requires close attention to its stated objects for assistance in interpreting some of the provisions contained in the Act. I still find myself thinking and rethinking the nuances of the exemption provisions. In the end, however, I always come back to the statement of purpose set out in Section 1 of the Act:

> 1. The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by

> (a) giving the public a right of access to records held by public bodies;
>
> (b) giving individuals a right of access to, and a right to request correction of, personal information about themselves held by public bodies;
>
> (c) specifying limited exceptions to the rights of access;
>
> (d) preventing the unauthorized collection, use or disclosure of personal information by public bodies; and
>
> (e) providing for an independent review of decisions made under this Act.

By applying these principals, I find that the interpretation becomes much easier and really more of an exercise of common sense than an intellectual exercise.

> The question is whether the Government is entitled to demand, record, sift, sort, match and share our private information and biometric identifiers without making a solid case for why this is necessary, how it will work, and why less invasive approaches won't do
>
> Dr. Leslie Cannold
>
> Fellow, Philosophy Department, University of Melbourne

In my annual reports and in my appearances before the Standing Committee on Government Operations and Accountability, I have developed a consistent theme. That theme is that the purposes and intent of the *Access to Information and Protection of Privacy Act* are most likely to be realized if those at the top of the political and managerial teams actively support the Act and encourage close adherence to its principals. This theme has been echoed by my fellow Access and Privacy Commissioners around the country. Gary Dickson, Information and Privacy Commissioner for Saskatchewan, in his 2006/2007 Annual Report made the following observation:

> The critical missing piece is an explicit message from the Premier, Chief Executive Officers (CEOs) of govern-

> ment institutions (outside of Executive Government), and local authorities that statutory compliance with FOIP, LA FOIP and HIPA must be a priority. Although the courts in Saskatchewan and Canada have spoken frequently about the special 'quasi-constitutional' nature of these laws, that alone tends not to mobilize public bodies.

In her 2003 Annual Report, Dr. Ann Cavoukian, Information and Privacy Commissioner for Ontario said:

> It is now time for the Premier to take this principle of openness a step further by issuing an open letter to all ministers and deputy ministers emphasizing the government's direction that a culture of openness and transparency within government must underlie decision-making under our access laws.

In my view, the routine disclosure of the details of government expenditure is critical if there is to be any level of transparency and accountability for the use of taxpayer's money.

Ann Cavoukian

Information and Privacy Commissioner of Ontario

It is important that all elected members of the Legislative Assembly, and particularly those holding Ministerial office, are knowledgeable about Act and what it requires of the government in terms of both access to information and the protection of the private personal information of its citizens. That knowledge should, in turn, be filtered down through the ranks, from Deputy Ministers down. It is important that all members embrace the principals of the Act in their leadership roles. As always, I encourage the Executive Committee and all Members of the Legislative Assembly to publicly and clearly endorse the goals of the Access to Information and Protection of Privacy Act and to provide leadership in the implementation of principals of openness. This includes making compliance with these principals a priority for all government employees.

I was recently privileged to have the opportunity to listen to a key-note address given by Maja Daruwala, Executive Director of the Commonwealth Human Rights Initiative. Ms. Daruwala is from New Delhi, India. India is, of course, a constitutional democracy. It is, however, a country that struggles, at times, with democratic princi-pals. Ms. Daruwala told the story of Boru, a small and poor village of about 2,500 people in rural India. The only access the people of Boru have to health services is in a neighbouring community, eight kilometers away and accessible to most only by foot, a difficult journey even for people who are not ill. The government health worker was supposed to come to that community three times a week to provide immunization and supplements and take care of tuberculosis patients, children and pregnant women. But, the peo-ple of the area were lucky if she actually came three times a month. So, after walking for hours to get medical assistance, the people of Boru were like as not to find that the government health worker who was supposed to be there to provide them with medical assistance had not come and their long walk was for naught. One day a member of the village decided to use the Right to Information (RTI) Act. He applied to the local doctor who doubled as its Public Information Officer (PIO) and asked for information about the medical assistance provided to patients, the facilities available for pregnant women, health workers and their duties at Boru. To the delight of all in the village, after this request was made, there was a turn for the better. The health worker began to attend the health center in accordance with her schedule and the health of the peo-ple in the village improved as a result. In the words of Ms. Daru-wala, “The visits made an immediate impact on general health.”

It is not entirely absurd to imagine that supermarkets' loyalty card data might one day be used by the Govern-ment to identify people who ignored advice to eat health-ily, or who drank too much, so that they could be given a lower priority for treatment by the NHS

Dilemmas of Privacy and Surveillance—Challenges of Technological Changes

Royal Academy of Engineer-ing

But, according to Ms. Daruwala, the request had other, more profound, effects as well. The doctor himself called on the villager who had made the request and wanted to know why he had asked for the information. The villager told him that it was important for the people to know their rights and know how to exercise those rights. Only then, he told the doctor, would be real change in society. The doctor assured the villager that he would ensure the health worker's regular visits to the village and invited the villager and others to talk to him if there were any other problems. In Ms. Daruwala's words:

> The doctor's visit indicated the subtle shift in power that having information and using the law makes in unequal relationships between bureaucrats and people in whose service they are supposed to be… The villagers had a huge success and it was one more step to accountability.

This story reinforced for me the importance of being able to hold our governments to account for their actions. It helped to remind me how incredibly important it is for us to protect our democracy and make sure that it remains strong so that we can all share in its benefits. It also emphasized the importance of Access to Information legislation and the role it plays in maintaining that democracy.

So what do I mean by "privacy pollution"? It's an idea I see as having some similarity to air pollution: where small blots of contamination build to form blankets of smog. In themselves, they are relatively minor – specks of soot or puffs of smoke – but in combination the effect can be overpowering. Like environmental contaminants, privacy breaches run from serious even criminal, across to minor annoyance…

The overall effect is that these tiny but insidious measures combine together to shape our behaviour. Together, they contribute to a climate where private space, thoughts and choices are encroached upon and subtly eroded. We must strive to find some way not only of limiting the impact that this has on each of us, but also to find spaces in which we can be free.

Marie Shroff

Privacy Commissioner of New Zealand

II. AN OVERVIEW OF THE ACT

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)

Sound information management is critical to accountable government for obvious reasons. Simply put, the effectiveness of the public's right of access to information is determined by the quality of a government's information management. If governments are to be held accountable and the public are to have meaningful rights of access to government information, information must be accurately and securely preserved to ensure there is a record of what has been done.

David Loukidelis

Information and Privacy Commissioner of British Columbia

ACCESS TO INFORMATION

The underlying premise of the access to information provisions in the *Access to Information and Protection of Privacy Act* is that open and accountable government is good government. That having been said, there is a need for some confidentiality in government as well, in order to allow governments to develop policy directions and

to ensure its ability to negotiate the best deals possible for outside services. The Act recognizes that the government operates 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 the business of government. Superior courts throughout the country, up to and including the Supreme Court of Canada, have laid out the rule that this act and its counterparts throughout the country should be interpreted in a manner so as to provide for the most access possible and that exemptions to disclosure are to be interpreted narrowly. Where exemptions apply, the courts have held, they should be applied in the manner which provides the greatest amount of public access and scrutiny.

> The notion that people who hold public responsibility must be accountable for what they do is not simply a legal fact. It is a social and cultural norm. It is fundamental to our concept of democratic government. People would demand it even if there was no law. This doesn't mean that you cannot make a decision that is not controversial. It means that you have to explain your decisions, account for them. If people disagree, well, that's politics.
>
> Frank Work
>
> Information and Privacy Commissioner of Alberta

The spirit of openness suggested by the Act is clear. However, it is not always quite so easy to apply the law to individual records. Simple common sense is an important and valuable resource in the interpretation 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. Most importantly, each request for information must be dealt with on its own terms.

The *Access to Information and Protection of Privacy Act* came into effect prior to division on December 31st, 1996. When Nunavut was formed, the Act became part of the law of Nunavut. It applies to and binds all Territorial Government ministries and a number of other governmental boards and agencies. All "records" in the possession or control of a public body are available to the public through an access to information request, unless the record is subject to a specific exemption from disclosure as provided for in the Act. The exceptions to the open disclosure rule function to protect individual privacy rights,

allow elected representatives to research and develop policy and the government to run the "business" of government. 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 ministries) are subject to the provisions of the Access to Information and Protection of Privacy Act. Currently there are 10 ministries and 14 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.

> We're waking up in a surveillance society. And when you start to see how many well-intentioned, apparently beneficial schemes are in place to monitor people's activities and movements, I think that does raise concerns. It can stigmatize people. I have worries about technology being used to identify classes of people who present some sort of risk to society.
>
> And I think there are real anxieties about that.
>
> Richard Thomas
>
> UK Information Commissioner

Information about the Act can be found on the Government of Nunavut's web site. From the main page of this site, there is a direct link to the office of the Manager of Access to Information and Privacy and from here 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-Ordinators 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 Information and Privacy Commissioner's web site, which will include copies of all recommendations made, is under construction and should be available to the public very shortly.

The Process

Every government agency subject to the *Access to Information and Protection of Privacy Act* is required to appoint a person within the organization to be responsible for dealing with Requests for Informa-

tion made under the Act. This person, the "ATIPP Co-Ordinator", receives and processes requests received from the public for information. Requests for information must be in writing. 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. An e-mail request may require, in addition, written correspondence signed by the Applicant, depending on the requirements of the public body. Requests are submitted, along with the $25.00 fee, to the appropriate public body. There is no application fee if an individual is requesting his or her own personal information , although there may be a fee for copying records in certain circumstances. .

When a request for information is received, the public body has a duty to identify all of the records which are responsive to the request and respond to the request within 30 days. Once all of the responsive documents are identified, they are reviewed to determine if there are any records or parts of records which should not be disclosed for some reason. 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. Public Bodies are prohibited from disclosing certain kinds of records. In some instances, the Public Body has discretion to decide to either disclose the records or not. These discretionary exemptions require the public body to consider whether or not to disclose the information, keeping in mind the purposes of the Act and the weight of court authority which requires public bodies to err on the side of disclosure.

Every person has the right to ask for information about themselves. If an individual finds information on a government record which they

There has been an erosion of the principles of data protection over the past 10 years, Data storage has become so cheap, there is no incentive to be selective about what we keep and what we discard. It is easier to keep almost everything and that has had a cumulative effect. There is an approaching crisis in data protection.

Caspar Bowden

Chief Privacy Adviser, Microsoft.

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.

The Role of the Information and Privacy Commissioner

The legislation provides for an independent oversight officer known as the Information and Privacy Commissioner. The Commissioner's job is review decisions made by Public Bodies where the public is not satisfied with the response they receive from a public body in response to a request for Information. The Information and Privacy Commissioner conducts an independent review of the decisions made by public bodies, and provides non-binding recommendations to the public body.

The Information and Privacy Commissioner is appointed by the Legislative Assembly for a five year renewable term. 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. The current Information and Privacy Commissioner was reappointed for a five year term in October, 2004 and will serve until October, 2009 .

The Information and Privacy Commissioner 's role is that of an ombudsman which means that she has the obligation to provide recommendations to public bodies but no power to make orders or require the public body to act on the recommendations made. The Commissioner's recommendations are made to the "head" of the public body involved in the Request for Information. In the case of a ministry, the "head" is the minister. For other public bodies, the "head" is determined in accordance with the regulations. Public bodies must consider the recommendations made, but have no obligations to accept

If you are outraged over the sponsorship affair, you must be in favour of open government and access to information. Things like this do not happen when people expect their actions to be public and therefore to be held accountable for them. If you know you have to explain yourself, if the energy spent concealing what was done was expended in explaining to the public why something is being done, everyone is better off. The public may still disagree with policy decisions, which of course they will, but they cannot be angry about lies and deception.

Frank Work

Information and Privacy Commissioner of Alberta

or implement them. Once the recommendations are made, it lies to the pubic body to respond to the recommendations made within thirty days. The public body may choose to follow the recommendations made by the Information and Privacy Commissioner, reject them, or take some other steps he or she feels is advisable based on the information in 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 still have public trust. But, trust is not a renewable resource -- once it is lost it may not be regained.
>
> Mary Lysyk,
>
> Policy Adviser, Health Canada

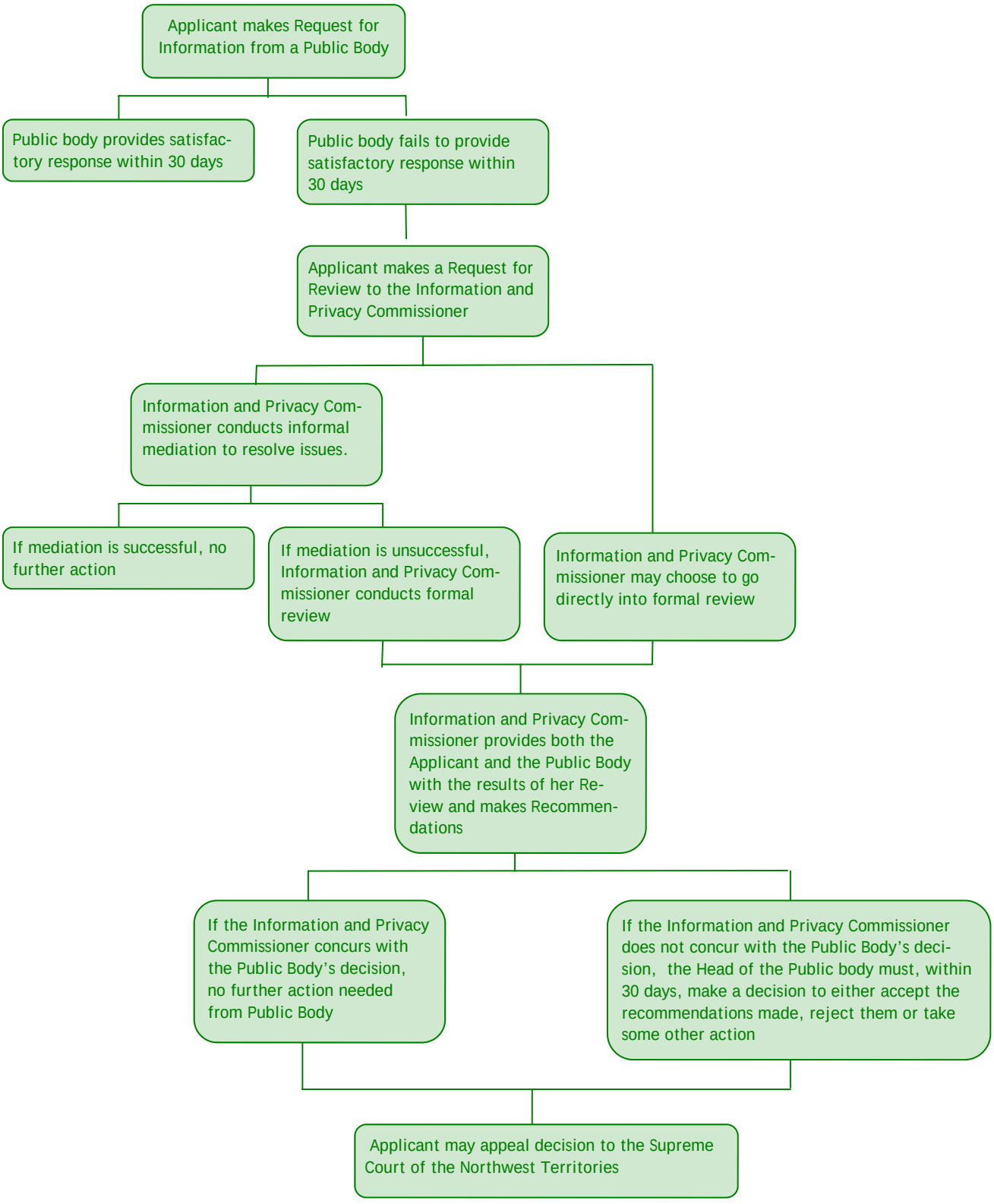
In the event that the person seeking information does not agree with the decision made by the head of the public body, that party has the right to appeal that decision to the Nunavut Court of Justice. To date the Commissioner is unaware of any decisions made on appeal to the court from the decision of the head of a public body after recommendations of the Information and Privacy Commissioner.

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.

PROTECTION OF PRIVACY

The *Access to Information and Protection of Privacy Act* also provides rules with respect to the collection, use and disclosure of personal information by Territorial government agencies. Part II of the Act outlines the basic rules for protection of privacy, which have been recognized and adopted internationally as the standard minimal privacy

THE REQUEST PROCESS



protection standards which governments should be held to. They are:

- No personal information is to be collected unless authorized by statute or consented to by the individual
- Personal information should, where possible, be collected from the individual about whom the information relates, and not from a third party
- Where information is collected from third parties, the person who is the subject of the information should be informed of the fact and be given the opportunity to review it
- Where personal information is collected, the agency collecting it must advise the individual of the use to which the information will be put and if the public body wishes to use it for other purposes, the consent of the individual must be obtained first.
- The personal information collected must be kept safe and secure and the public body must ensure that it is available only to those who require the information to provide the service or conduct the business for which the information was collected.
- Personal information collected by a government agency must be used only for the purpose it is collected; and
- Each individual is entitled to know what personal information about themselves is held by any public body and have the right to see that information and request that it be corrected if they feel that it is inaccurate.

The Information and Privacy Commissioner is given no official power or jurisdiction in the Act to investigate privacy complaints or to make recommendations where breaches are found to have happened.

> People have many different reasons for wanting to control information about themselves, motives ranging from freedom from defamation to commercial gain. When freedom from scrutiny, embarrassment, judgment and even ridicule are at stake, as well as protection from pressure to conform, prejudice, emotional distress, and the losses in self-esteem, opportunities or finances arising from these harms, we are more inclined to view the claim to control information as a privacy claim.
>
> Judith Wagner DeCew
>
> In Pursuit of Privacy, (Cornell University, 1997) pp. 62-80.

Regardless of the lack of official jurisdiction to undertake such reviews, however, the Information and Privacy Commissioner has routinely accepted such complaints, investigated them and made recommendations based on her findings. In such cases, however, the public body has no obligation to take any steps to respond to or implement any of the recommendations made.

> Our view of those things which make up privacy changes as we change, as our society changes. Some of these changes occur slowly as social mores change. Twenty years ago politicians governed, administrators implemented programs and the public largely accepted it. Now we speak of transparency, accountability, stakeholders, and consultation. Other changes come with technology. ...Some of these changes are lightning fast. Consider how quickly the balance between privacy and physical security shifted after the attack on the World Trade Center.
>
> Frank Work
>
> Information and Privacy Commissioner of Alberta

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 that decision. This includes decisions about the disclosure of records, corrections to personal information, time extensions and fees. The purpose of this process is to ensure 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 within 30 days of receiving a decision from a public body under the Act. 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 involved and obtain an explanation from the public body. In most cases, the Commissioner will receive a copy of the responsive documents from the public body involved and will review the records in dispute. In some cases, it may be necessary for the Information and Privacy

Commissioner to attend the government office to physically examine the public body's files. Generally, an attempt will first be made by the Commissioner's Office to mediate a solution satisfactory to all of the parties. 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 a more in depth review. All of the parties involved, including the public body, are given the opportunity to make written submissions on the issues.

In the 2006/2007 fiscal year, the Information and Privacy Commissioner's Office opened six files.

Requests for Review (Access Issues)	2
Requests for Review (Privacy Issues)	1
Other	3

The Requests for Review involved the Department of Health and Social Services, the Department of Education, and the Department of Community and Government Services.

The Information and Privacy Commissioner issued two recommendations in 2006/2007.

The Information and Privacy Commissioner attended two meetings of her counterparts from across the country during the year. In addition, she was invited to speak at a conference in Edmonton.

Records management is also bedevilled by the expanding reliance on electronic records and databases. The sheer volume, and variety, of electronic records makes it difficult to catalogue, organize and preserve them in a way that keeps them accessible. And this isn't to mention the difficulty in deciding which of many versions of an electronic record is the authentic original. These problems are exacerbated in the electronic realm as hardware, software and storage media become obsolete over time, often leaving behind records that can no longer be read, making once-valuable information worthless.

David Loukidelis

Information and Privacy Commissioner of British Columbia

III. REVIEW RECOMMENDATIONS

Review Recommendation 06-024

It is not the public body's job to "protect" public records or people within the public body.

Elaine Keenan Bengts

Review Recommendation 06-024

This review came about when an applicant requested certain information about himself in connection with incidents which arose during his employment with the Government of Nunavut. The request was addressed to various public bodies, including the Legislative Assembly, the Department of Economic Development and Transportation and the Department of Community and Government Services. The public body provided the Applicant with a number of records, some of which had sections which had been severed. The Applicant was not satisfied with the response received and felt that there should be more documents responsive to his request. The only issue was whether the public body had properly applied section 23 of the Act in refusing to disclose certain parts of certain documents. Section 23 provides that the public body must refuse to disclose documents if that disclosure would be an unreasonable invasion of a third party's privacy. The Information and Privacy Commissioner reviewed all of the records identified as being responsive to the Applicant's request and, for the most part, recommended disclosure. She commented that it appeared in this case that the public body had taken the very narrowest reading of the Applicant's request possible and that this was likely the reason that the Applicant was unhappy with the response received. She suggested that where there was any doubt, the public body should attempt to clarify the request with the Applicant rather than make assumptions. She also indicated frustration with the public body's failure to provide her with a full and thorough explanation about why certain records had not been disclosed and pointed out that it was not sufficient in the context of a review by her office to sim-

ply refer to a section of the Act, without providing any explanation. She indicated that it was incumbent on the public body to establish that the exemptions apply, not the Information and Privacy Commissioner's to guess the circumstances.

The recommendations were accepted.

Individual civil servants should, as well, be responsible for information management tasks within their own employment duties, with relevant requirements being made a condition of employment and of employee appraisal. Information management should form part of executive level compensation assessment and information management performance should be an institutional performance standard and subject to regular appraisal.

David Loukidelis

Information and Privacy Commissioner of British Columbia

Recommendation 06—025

In this matter, the Applicant had requested all letters, memo's, faxes and emails to/from/with the Applicant's name or job description during a stated time period. The request was addressed to Minister Aglukkaq personally. The public body was unable to find any records responsive to the Applicant's request for information. However, a similar request had been provided to the Department of Health and Social Services and the Applicant had received responding materials. Some of those materials indicated that Minister Aglukkaq had been involved in e-mail discussions respecting the Applicant and the Applicant felt that these records should have been discovered in the Minister's records. For this reason, she asked that the Information and Privacy Commissioner review the matter.

The Information and Privacy Commissioner, after considering all of the materials provided, was satisfied that the public body had done a complete and thorough search of the Minister's records and that they were genuinely unable to find any responsive records, including records of e-mail that should have been there. She did, however, point out some of the problems of doing business by means of e-mail. She noted that e-mail has a "feel" about it that is less formal, both in terms of the language used in such correspondence and in terms of

record management. It is easy to hit the “delete” button, sending e-mail correspondence into the ether, never to be seen again. She also pointed out that e-mail sent from a private computer may not be stored in the system in the same way as e-mail from government computers would be archived. She recommended that the Government of Nunavut take immediate steps to create a clear policy with respect to the use of e-mail in connection with government business, including a provision that provides that substantive communication on sensitive issues should not be conducted by e-mail.

Our democracy is all the more vibrant for the legally enforceable right we Canadians have to go behind the "stories" governments choose to tell us, to obtain source documents, and to explore the stories which all governments store in dark corners.

Robert Marleau

Information Commissioner for Canada

IV. RECOMMENDATIONS

As in previous years, many of my recommendations are repeated or ongoing. Some of the recommendations are longer term issues and will take some time to address in a thorough and complete way. Some, however, could be addressed fairly quickly and without a significant amount of work.

One hundred million -- that's a pretty big number. It's roughly three times the population of Canada, about a third of the U.S. population, and roughly equal to the population of Mexico.

It's also the number of notifications that have gone out to individuals in the United States informing them that their personal information has been lost or stolen by companies. Upwards of 100 million "records" have been disclosed to date and reported upon pursuant to state disclosure notification laws, according to the Privacy Rights Clearinghouse.

TechNewsWorld, January 4, 2007

A. Privacy Investigations

I believe that each of the Annual Reports I have made to the Legislative Assembly have contained a recommendation that more is needed in the *Access to Information and Protection of Privacy Act* to give teeth to the provisions of the Act which protect the personal privacy of the people of Nunavut. Although the Act provides rules and regulations with respect to the collection, use and disclosure of personal information, it does not have any enforcement mechanism to ensure that the legislation is honoured. I strongly believe that amendments are required to address this huge gap in the legislation so as to give individuals an easy way to seek redress where their information has been inappropriately collected, used or disclosed contrary to the Act. Currently, the Information and Privacy Commissioner's power of review is limited to the review of access to information issues. 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. 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.

B. Municipalities

Another recommendation which I have made in each of my Annual Reports since becoming the Information and Privacy Commissioner of Nunavut is 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. In response to my previous reports, the Government of Nunavut has 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. 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 therefore maintain my recommendation that steps be taken to ensure that municipalities are governed by a set of rules

The number of electronic communications channels has exploded in the past few years, but email remains a top focus for organizations when it comes to data protection and security challenges. With a staggering 70 percent of corporate data residing in email, this channel will continue to pose the biggest threat as a means for the improper disclosure of confidential data. However, additional outbound data streams - including HTTP (i.e., blogs, web-based email, message boards), instant messaging and FTP - have entered the mix and can also be conduits for violations of internal communications policies, confidential information exposure or sources of regulatory risk.

SC Magazine, February 21, 2007

and regulations to ensure open access to records and to address important privacy issues within municipalities. It might take the form of something less formal than legislation. It may be as simply done as to include municipalities as "public bodies" in the Regulations under the *Access to Information and Protection of Privacy Act*. But I do believe that municipal governments, as governments, should be subject to consistent guidelines and that there should be some means of independent oversight so as to provide consistent access to information and privacy rules for municipalities within Nunavut.

Thanks to the falling costs of telecommunication and the enhanced processing and memory capabilities of computers, the volume of personal data being generated by this always-on economy is growing exponentially. One needs only to think of the enormous amounts of information shared during online searches or social networking Web site visits. More organizations have access to more information about more people than ever before.

Jennifer Stoddart

Privacy Commissioner for Canada

C. 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 their members 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 once again recommend that the Act be amended to clarify that individuals appointed to public bodies are specifically subject to the Act by virtue of their appointments. 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.

> In my view, the routine disclosure of the details of government expenditure is critical if there is to be any level of transparency and accountability for the use of taxpayer's money."
>
> Ann Cavoukian
>
> Information and Privacy Commissioner of Ontario

D. Openness of Contract Details

An issue that seems to arise fairly often in Nunavut has been the concern about how government contracts are awarded and how government funds are spent. The public wants to know who is getting government contracts and what they are being paid. While there does seem to be some progress over the years in ensuring openness about contracts and how they are awarded, there is still room for improvement. This is not an issue that is unique to Nunavut. It is an issue throughout the country and more and more, governments are starting to be far more open about the contracts they enter into. As has been pointed out by Dr. Anne Cavoukian, the Ontario Information and Privacy Commissioner in her last 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.

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 requirements 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.

The risks that arise from excessive surveillance affect both individuals and society as a whole. As well as risks such as identity mistakes and security breaches there can be unnecessary intrusion into people's lives and loss of personal autonomy.

There is also a concern that too much surveillance will create a climate of fear and suspicion. It is essential that before new surveillance technologies are introduced full consideration is given to the impact on individuals and that safeguards are in place to minimize intrusion,

Richard Thomas
Information Commissioner
Great Britain

E. 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 and internet access 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. 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 businesses 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 inter-provincial 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.

Despite the clear guidance provided by my office, some government ministries still refuse to disclose government contracts for the provision of goods and services. The routine disclosure of the details of government expenditure is critical if there is to be any level of transparency and accountability for the use of taxpayers' money.

Ann Cavoukian

Information and Privacy Commissioner of Ontario

F. Electronic Records

Although the Government of Nunavut has a policy on acceptable e-mail and internet usage, I cannot find any policies on the use of other electronic media. It is unclear how well the existing policy on internet and e-mail usage is advertised or enforced and it is far from comprehensive. For example, the policy does not address the use of

personal computers in undertaking government business. A government employee might, for instance, use a personal home computer to send e-mail relating to government business from their own home computer while working from home. There does not appear to be any policy that applies to those records in terms of their retention or inclusion in the public record. There should be a clear policy that requires a copy of such e-mails to be sent to the employee's work e-mail address so that it can be dealt with appropriately in terms of records management procedures.

Also of concern is the security of electronic records, particularly as those might be contained in mobile devices. Are there any policies with respect to the use of mobile devices, including laptop computers and mass storage devices. Is there a policy on the kinds of data that can be taken out of the office for any purpose. Are there rules and regulations about the encryption of sensitive data on such devices so that if they are lost or misplaced, no one else will be able to access the data? If there are such policies, how well are they known and how well are they enforced?

It is important that written government policies regarding electronic medium keep up with changing technologies so as to ensure that government records are available and accessible when requested and to ensure that there are no inadvertent or accidental disclosures of personal information because of lack of attention to security measures. To the extent that these policies already exist, they should be reviewed at least annually to ensure that they keep pace with the changes in technology. To the extent that they do not yet exist, there should be a concerted effort to create these policies and ensure that they are widely disseminated and strongly enforced.

> … public policy cannot second guess the kinds of personal information about which a given population or group will be concerned at a given time. Public policy and law can only establish the rules, principles and procedures by which any individually identifiable personal information should be treated, and by which the worst effects of new technologies can be countered. Information privacy policy is based inevitably, therefore, on procedural, rather than substantive, tenets.
>
> Bennett and Raab
>
> The Governance of Privacy (Burlington, Ashgate Publishing, 2003) page 16.

V. CONCLUSION

Although there are now considerably more tools and resources available to government institutions, and there is now a much larger group of identified leaders in these organizations, the access and privacy regime in Nunavut is not yet fully working the way envisaged by the legislation.

To paraphrase the words of my fellow Commissioner from Saskatchewan, Gary Dickson, one critical missing piece is an explicit message from the Premier, and Chief Executive Officers (CEOs) of government institutions that statutory compliance with ATIPP must be a priority. . I know that those who have been given the mandate within their organizations to oversee access to information and privacy issues as the ATIPP Co-Ordinators work hard to ensure that they meet their responsibilities under the Act. I am not so sure that those in more senior positions always support the work that these Co-Ordinators are asked to do.

More needs to be done to provide significant incentives for public bodies to achieve excellence in meeting these statutory responsibilities. Those factors that might, if addressed by remedial action, provide powerful motivation to strive for such excellence include:

• A schedule should be established to ensure a review of the Act so that amendments can be made to reflect lessons learned in this and other jurisdictions . This office has made many suggestions for amendments and changes to the Act but any changes have been small and piecemeal. It may be time that a more thorough review be done to see if there are ways to improve the system and meet the ideals for which the act was established..

• There has, to my knowledge, been no mandated orientation sessions for senior government officials and CEOs to acquaint them with

> Totalitarian regimes have, after all, always collected information on their citizens. Hitler pioneered the use of ID cards as a means of repression. The Belgians left Rwanda with a bloody legacy by implementing an ID card system which divided the population into Hutu and Tutsi.
>
> When the 1994 genocide began, these cards proved a device for horrific ethnic cleansing, with one million people dying in 100 days. The Stasi secret police in Soviet East Germany kept millions of files in order to keep track of everyone in the country.
>
> Of course these examples are the extremes - but basic liberties such as privacy and free speech have been hard-won over centuries and history shows that we should not allow them to be brushed aside.
>
> Mike Elgan
>
> June 22, 2007
> (Computerworld)

the goals and objectives of the Act . This would go a long way to reinforce on a corporate level the importance of the Act and it's application

- Public bodies are free to offer no reason for disregarding the recommendations made by the Information and Privacy Commissioner (although some public bodies do provide explanations). Perhaps there should be a requirement for public bodies to provide an explanation when they choose to disregard recommendations made by the Information and Privacy Commissioner.
- There are no provisions requiring that Privacy Impact Assessments be undertaken at any point when considering new initiatives or programs. Most jurisdictions in Canada require that such assessments be done prior to implementation of new programs so as to ensure that there is minimal impact on privacy

Perhaps the greatest perversity about the explosion of surveillance is that experts say it doesn't necessarily do any good. While crime has gone down in some areas, studies show that it's seldom due to the presence of CCTV cameras. In fact, there is evidence that cameras can provoke more criminal behaviour.

If people start to feel they are constantly under surveillance, the feeling of being watched starts to create the behaviour that the surveillance was there to prevent,

Kirstie Ball, Open University Business School.

In closing, I would just say that I firmly believe that those within the Government of Nunavut who have been given the mandate to be responsible, within their organizations, for access to information, have been doing their best to deal with the matters which come before them.. There is, however, always room to improve the way things are done. Furthermore, I do believe that the privacy aspects of the Act are less well understood and not always well addressed within government either on a policy level or on a day to day basis. It may be that it is time to review the Act and the manner in which this service is provided and to consider changes to address some of the problems which have come to light with the application of the Act over the last number of years.

Respectfully submitted

Elaine Keenan Bengts

Information and Privacy Commissioner