TABLED DOCUMENT NO. 25 - 15(4) TABLED ON JUN 0 2 2005

N.W.T. LEGISLATIVE LIBRARY
3 1936 00072 8772

NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER

5018 - 47th Street
P.O. Box 262
Yellowknife, NT
X1A 2N2

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

ANNUAL REPORT 2003/2004

N.W.T.
LEGISLATIVE LIBRARY
JUN 0 3 2005
Yellowknife, N.W.T

In Yellowknife: 867-873-8631 ♦ Toll free: 888-521-7088 ♦ Fax: 867-920-2511 ♦ E-mail: AtippComm@theedge.ca

N.W.T. Legislative Library

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

5018 - 47th Street
P.O. Box 262
Yellowknife, NT
X1A 2N2

November 22, 2004

Legislative Assembly of the
Northwest Territories
P.O. Box 1320
Yellowknife, NT
X1A 2L9

Attention: Tim Mercer
Clerk of the Legislative Assembly

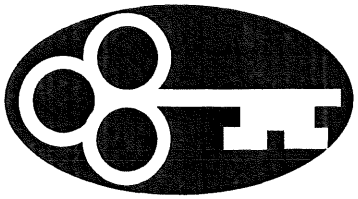
Dear Sir:

I have the honour to submit my annual report to the Legislative Assembly of the Northwest Territories for the period from April 1st, 2003 to March 31st, 2004.

Yours very truly

Elaine Keenan Bengts
Information and Privacy Commissioner
Northwest Territories

In Yellowknife: 403-669-0976 ♦ Toll free: 888-521-7088 ♦ Fax: 403-920-2511 ♦ E-mail: AttipComm@theedge.ca



1. COMMISSIONER'S MESSAGE

The first section of the Access to Information and Protection of Privacy Act states its purposes — to make public bodies more accountable to the public and to protect personal privacy. These are important goals for modern democratic government, but they are sometimes difficult to achieve in practice. No matter how well intentioned and no matter how deeply ingrained the goals are, openness is not always easy to achieve. The Office of the Information and Privacy Commissioner was created to provide independent guidance on access and privacy issues. The success of the legislation, however, is not dependent on the Information and Privacy Commissioner, but on the leadership of politicians and senior bureaucrats. If the leadership within government creates a corporate culture which respects the purposes of the Act, those ideals will be respected and encouraged throughout the organization. I am happy to say that, for the most part, the Government of the Northwest Territories does encourage and support the purposes of the Act. There are, of course, the exceptions, and some departments have more difficulty with openness than others, but it has been my experience that most government departments are anxious to adhere to the principles of the Act and do so successfully.

Every year, new and interesting issues arise in my work as the Information and Privacy Commissioner for the Northwest Territories. Fiscal 2003/2004 was no different. The number of new files was opened was up, but only very nominally, from last year. In all, sixteen new files were opened, only one

> The natural progress of things is for liberty to yield and government to gain ground. This is so because those who gain positions of power tend always to extend the bounds of it.
>
> **Thomas Jefferson**

more than in the previous year. Of those 16, ten were Requests for Review with respect to Access to Information issues. One privacy complaint was received. The Information and Privacy Commissioner was asked to provide her comments on one piece of legislation (amendments to the *Access to Information and Protection of Privacy Act)* and there was one request to speak at a conference being held in Yellowknife. In addition, the Information and Privacy Commissioner responded to two requests to comment on specific issues. One was with respect to a proposed National Identification Card initiative floated by the federal government. The second was with respect to the application of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). The remaining file was a general administrative file through which the Information and Privacy Commissioner responded to general inquires. As well, a number of national issues drew me into discussions with government employees and with my counterparts throughout the country.

Some of the national issues in which I joined discussions with my fellow Information and Privacy Commissioners included the federal government's exploration of a mandatory National ID Card, the effect of the Patriot Act in the United States on the privacy of Canadians (particularly insofar as it relates to the contracting out of government initiatives to private sector companies with American affiliation), the Federal/Provincial Territorial Health Privacy Framework and video surveillance issues.

Every citizen has the right to observe the operation of his or her government closely and personally. That right is the cornerstone of our great democracy. We can have no real freedom without openness in government.

Henry McMaster
Attorney General South Carolina.

I am pleased to report I have been able to maintain a very positive working relationship with most of ATIPP Co-Ordinators within the public service, particularly in those departments which receive a large number of information requests and with whom I am in fairly regular contact. I believe that the enforcement of the *Access to Information and Protection of Privacy Act* should, where possible, be involve open discussion and consultation and I have encouraged the ATIPP Co-Ordinators to call to discuss issues when they are unsure as to any particular matter or simply wish to discuss something which has arisen in their offices.

It appears that public bodies are now being provided with fairly regular opportunities to obtain training on the principles of the *Access to Information and Protection of Privacy Act.* What is not clear is whether all public bodies are taking advantage of those opportunities. Some public bodies, particularly some of the boards and agencies created by government but which have some level of independence, seem to have less knowledge of the legislation and either have not availed themselves of training opportunities or have not been made aware of those opportunities. It is important that some effort be made to ensure these boards and agencies are properly informed and trained and one of the recommendations I will be making in this report is that the government require at least the more senior members of boards and other agencies to receive ATIPP training and to refresh that training at least once every two years.

Striking a balance between the protection of privacy and the promotion of national security is one of the single most important issues facing our society today ,This is an issue to be addressed by all jurisdictions across Canada

Jennifer Stoddart
Information
Commissioner of Canada

We live in an age of technological miracles. The challenge we share is to use this incredible technology to serve us and our society without enslaving us.

Frank Work

Information and Privacy Commissioner of Alberta

2002/2003 Annual Report

Although the more visible role of the Information and Privacy Commissioner is as an independent referee on access to information issues, the Information and Privacy Commissioner also has a role as a watchdog with respect to personal privacy issues as well. I continue to be increasingly aware of and intrigued by the privacy aspects of the Information and Privacy Commissioner's role. The boundaries which surround personal privacy are ones that are constantly changing due to emerging technologies and the parameters of what is acceptable are shifting. Many things have contributed to the whirlwind of activity surrounding privacy issues. The fallout from September 11, 2001 continues to challenge governments to balance privacy rights with safety and security. Many initiatives which begin with good intentions either as government initiatives or as private sector initiatives have huge potential to burrow deeply into our privacy. As governments attempt to deal with these issues, we become increasingly aware of the potential for mistakes and misuse. For example, one of the issues being discussed on a national level is the implementation of a standard driver's license throughout the country. The standardization makes sense. The question, however, becomes what information should be included in the driver's license and in what form. It has been suggested that these standardized licenses might include the use of Radio Frequency Identification Devices (RFIDs) and/or biometric information. RFIDs are silicon chips about the size of a piece of rice with an antenna that can transmit data to a wireless receiver so that it can be read remotely with a receiver/ reader. These RFIDs can contain a large amount of personal

One of the key challenges for all governments in these turbulent times is the delicate balance of showing leadership on real issues of national important while avoiding invoking major policies or initiatives without due consideration of the long term impact of these changes.

Ann Cavoukian
Information and Privacy Commissioner of Ontario

Annual Report 2002

information, including names, addresses, dates of birth, medical information and perhaps other identifiers such as fingerprints or other biometric information. The desire of governments to make drivers licenses more uniform throughout the country is driven by security concerns and the need of law enforcement agencies to be able to verify identities. The privacy concerns, however, are numerous. For example, in a world where identity theft is the fastest growing criminal activity, once RFID's are fitted into a driver's license, anyone with a "reader" would be able to simply scan a crowd to obtain whatever information is contained on the individual's driver's licensee. There are very real concerns that this would be a gift to identity thieves who could simply "camp out" in a public place such as a mall or an airport and gather untold amounts of personal information simply by "reading" the information from RFID's embedded in electronic driver's licenses. The question then becomes whether embedding this kind of information in a driver's license will advance our personal security and protect us from terrorism and whether that protection will outweigh the increased invasion of our privacy . The addition of biometrics to driver's licenses will not create a sure fire means of identifying and catching terrorists or criminals. It is not the information in the identity document that matters, but how that information is collected and verified that really matters. All of the terrorists involved in the September 11th bombings had legitimate US identification documents. In Spain, where residents are required to hold a National ID card, that requirement did not prevent terrorists from bombing a commuter train during rush hour and killing hundreds. Although technology may well succeed in more accurately

identifying the law abiding public, whether or not these technologies will help in any way to protect us from further terrorist or criminal activities bears careful consideration.

Several Canadian provinces are also grappling with the wide reaching implications of the US Patriot Act, which was passed in response to 9/11. One of the provisions of the Patriot Act gives the American Government the right to demand of any American or American company that they provide a US government agency any and all personal information records they hold. If the company refuses to disclose the personal records, they face serious consequences. Even more disturbing is that these companies are prohibited from telling the individuals involved that their information has been disclosed. This issue came to the forefront in Canada when the British Columbia government decided to contract out the responsibility for maintaining the medical records of British Columbians to the Canadian branch of a wholly owned American company. The British Columbia Government Employee's Union raised an alarm, arguing that this put the personal medical records of Canadian citizens at risk for mandatory and clandestine disclosure to American officials. As a result of this concern, my counterpart in British Columbia is doing a major research project to determine how and when the Patriot Act will apply to American owned Canadian companies and what, if any steps, Canadian governments can take to minimize the risk. His conclusions will no doubt create a blueprint for all Canadian jurisdictions, including the Northwest Territories. Health records, in particular, are extremely sensitive and

To permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society....We must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy

Justice Gerald La Forest
Supreme Court of Canada

should demand the highest degree of protection. I do not know whether the Government of the Northwest Territories has any similar outsourcing issues, but I would suggest that a review of outsourcing contracts might be in order and privacy issues should be a primary concern in any future outsourcing contracts which the government might consider, particularly where the outsourcing would involve large amounts of personal information of individuals living and working in the Northwest Territories.

Ever evolving and improving technology makes possible today what was considered pure science fiction less than ten years ago. From microchips the size of a piece of rice which can carry more information than first generation personal computers did twenty years ago, to devices which can be implanted under the skin to monitor an individual's movements or provide medical histories, such as the ones recently approved by the American Federal Drug Administration; from cell phones capable of taking and transmitting digital pictures from almost anywhere, to GPS systems in vehicles which track you every where you go, technology continues to evolve. Most technology is aimed at making our lives easier. But for every positive use of such technology, more sinister uses can be, and often are, discovered. How much we will tolerate in terms of how our personal information is used? How much surveillance are we prepared to accept? Should the government or an employer be able to monitor our Internet use? Should foreign governments be able to demand our personal information in the name of their own security concerns and to keep and use

But privacy is not simply a frill or a selfish extravagance that can be tossed away the moment someone claims that it inhibits some other valuable social goal — regardless of whether the goal is security or public health or even individual life or death. Privacy is a cornerstone of individual freedom. It exists in a dynamic balance with our other social needs. The key to preserving privacy is careful analysis of any measure that purports to bring us some other social benefit, to ensure that the balance is maintained.

Robert Marleau
Interim Privacy Commissioner of Canada
Annual Report
2002-2003

For the system to function most effectively, the consumer must be informed of their rights and empowered to use them. Every corporation that collects personal information is required to publicly disclose the contact information for their privacy officer. You can ask that person what information that company is collecting on you. The information integrity gauntlet has been thrown down - now the power is in the hands of the consumer.

And the responsibility.

John Wunderlich and Carolyn L Burke
Globe and Mail

that information without our knowledge and consent for any number of purposes? Should businesses be able to buy and sell our personal information to willing buyers without our permission? Is a company's right to market their products greater than the right of individuals to be free of e-mail spam or tele-marketing calls? Technology can undoubtedly make our lives easier, but we must be aware of what we are giving up in exchange for that convenience. Keeping up with changes in technology can be a daunting task, but we must remain aware of these technologies in order to prevent and avoid their misuse.

In Canada, the federal government and three provinces (British Columbia, Alberta and Quebec) have all passed legislation to regulate the protection of personal privacy in the private sector. At least two other provinces have legislation that specifically deals with the protection of privacy in the health sector, private and public. Three other provinces are considering private sector privacy information. This is an issue that will become more and more important as technologies continue to expand. Although we in the North are somewhat sheltered from some of the worst abuses of these technologies, we won't be sheltered forever. Although we may have the luxury of time before these new technologies catch up with us in the North, they will arrive and we will have to be ready to deal with them. The Government of the Northwest Territories should be taking steps now to provide legislation which provides guidelines and direction to the private sector with respect to the use of personal

Is a passport any more "robust" than a driver's license as a confirmation of identity? The answer, unfortunately, is "not much".

There is a huge effort expended on designing and implementing a self-protecting identity token (driver's license, passport etc) and far too little effort on the validity of the actual identity, or on checking the legitimacy of the token. ....

It might also seem amusing that we regard the passport as the ultimate identity document, yet we're permitted to submit our application by mail.

What about biometrics, the catch-cry of the current decade? Biometrics is a very robust tool particularly in the case of fingerprint and iris recognition. Biometrics, however, won't identify anyone (despite the strident cries of the privacy police); it merely allows a strong link between a person and a previously established identity

David Heath
The Sydney Morning Herald
April 14, 2004

information and to do what can be done to protect the public from identity thieves and overreaching surveillance. Private sector legislation is necessary and I encourage the Government to begin the process of drafting and implementing legislation to deal with these issues.

The erosion of privacy, particularly since 9/11 has been pronounced. At first, a concerned public encouraged harsh security measures, even with their tendencies to erode privacy. As the public begins to reflect on those erosions of their right to privacy, however, they become less willing to accept those kinds of measures without some concrete assurances that they are necessary to protect them from terrorism. This has become a hot political issue throughout the world and will become hotter. Canada is no different. It is estimated that one in every 50 Canadians will be the victim of identity theft of some description over the next two years. Identity theft is the fastest growing criminal activity in the world, costing both individuals and businesses hundreds of millions of dollars. These are not "southern" issues. They are very real issues for the people of the Northwest Territories as well, and it is important that the government take what steps it can to deal with these issues. How do we ensure that companies do not improperly share their customer's personal information? What can we do to remind companies that they have to erase all data from their computers when disposing of old equipment? How do we impress upon the private sector that it is important to have appropriate security in place to ensure that only those who

need to know will have access to their client's information? It is hoped that the federal government's answer to private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) can start to address the problem. I believe, however, that leaving this role to Ottawa will leave Northerners exposed. Although the Federal Privacy Commissioner has jurisdiction to receive complaints from the Northwest Territories about privacy abuses in the Northwest Territories, her office is far removed and not in touch with the people. I will continue to encourage the government of the Northwest Territories to act as quickly as possible to address these issues.

I have a proposal before the Clerk of the Legislative Assembly for the creation of a web site for the Information and Privacy Commissioner's Office which will bring more visibility to the work which this office does. It is my hope that the funding approval to create this site will be given so that the page can be up and running before the end of the next fiscal year. This site will give the public more immediate contact with the Office of the Information and Privacy Commissioner. It will also help to more widely publish the recommendations I make to public bodies so that both the public and the government can have the guidance contained in those recommendations on a day to day basis. It will also provide information about how to make a request for information or a request for review and information and tips on steps that both individuals and businesses can do to protect their own and their customer's personal information. I realize that the Internet does not reach everyone, but the

However, at this point in our history, it is not clear how reducing the freedoms of all individuals in society will prevent further threats to public safety whether by terrorists on a political mission or for that matter, sex offenders acting on uncontrolled impulses.

But I can tell you that as we collect more information about more individuals we are increasing that possibility that people will be subjected to unnecessary scrutiny, that more people will be singled out, and that more people will be treated unfairly.

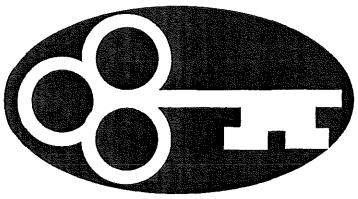
Jennifer Stoddart
Privacy Commissioner for Canada
Address to Standing Committee on Transport and Communications

March 18, 2004

Internet is becoming the research tool of choice and it is important to have that avenue open to the public and to make this office more accountable to the public as well.

"There is a widening and yawning gap between the surveillance that is actually happening and people's understanding for the capacity for surveillance. People just have no clue, and I'm describing intelligent people,"

Stephanie Perrin, President Digital Discretion Inc. Montreal.



II. INTRODUCTION

A. ACCESS TO INFORMATION

Background

The stated purpose of the *Access to Information and Protection of Privacy Act* as set out in section 1 of the Act, is to make public bodies more accountable to the public and to protect personal privacy. These can be difficult tasks. The Government, as a business, must be able to keep certain things to itself or it risks being taken advantage of in negotiating contracts and securing the best deal possible. 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 compete fairly in the business aspects of its mandate and to plan legislative initiatives. The general rule which has been applied to Access to Information legislation by the courts across the country is that openness is the rule and only narrow and specific exceptions to access should apply . Where those exceptions do apply, they must be applied in the manner that provides the greatest amount of public access and scrutiny. The legislation also recognizes that government agencies hold considerable amounts of personal, private information about individuals which needs to be protected from improper use or disclosure. There is sometimes a fine balancing to be done in dealing with requests for information to weigh which records should be disclosed to the public against which records should be subject to the Act's exemptions. 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

An attitude of service to access requesters is the frame of mind the Access Act requires public servants to take in answering access requests. Parliament has made it an express obligation to create records from electronic databases if it is reasonably possible to do so. it is not open to public servants to dictate to access requesters the format in which they will receive access to government records

Hon. John Reid
Information
Commissioner for
Canada
Annual Report 2003/2004

Distributed intelligence is everywhere, from the black boxes that record how we drive, to medical devices that log our tests for audit purposes. Increasingly, our movements are recorded in everything that we do, everything that we buy, everywhere that we go.
.....

A century from now, will people consider privacy and other liberties enjoyed by their grandparents to be a curiosity, a museum exhibit? Have we lost sight of the right to be left alone? Or will we choose to design a world safe from those who want to wield the power of prying electronic devices?

Ian Kerr
Globe and Mail
January 12, 2004

in the interpretation of the Act. Each request for information must be dealt with on its own terms and the facts surrounding the particular information in question may well dictate when and in what circumstances records are protected from disclosure.

In the Northwest Territories, the *Access to Information and Protection of Privacy Act* came into effect on December 31st, 1996, bringing it into line with almost all other jurisdictions in Canada. The Act gives the public the legislated means of gaining access to public records and information in the possession of the Government of the Northwest Territories and a number of other governmental boards and agencies, subject to the exceptions which are spelled out in the Act. The exceptions function to protect individual privacy rights, and 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 government departments) are subject to the provisions of the *Access to Information and Protection of Privacy Act.* Regulations came into force on December 31, 1996 in conjunction with the coming into force of the Act, naming 32 agencies as being subject to the Act. As far as I am aware, these regulations have not been reviewed or updated since that time. As eight years have passed, I would encourage the Government of the Northwest Territories to review the

Good records management is an essential pillar that supports the FOI process in Ontario. The public's statutory right to access government-held information cannot be fulfilled unless public servants properly document government programs and activities and maintain records in a well-organized manner.

A good records management system should enable a government institution to quickly locate and retrieve any requested records.

Excerpt from: Electronic Records and Document Management Systems: A New Tool for Enhancing the Public's Right to Access Government-Held Information?

Ontario Information and Privacy Commissioner's Office

July, 2003

regulations to ensure that they remain accurate and inclusive.

The Department of Justice now has on it's web site some information about the Act. Under the heading "Services" 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 names and contact numbers 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". That was, in fact, prepared in 1996, but to my knowledge has not been updated. This needs to be done as there have been a number of changes to the Act itself as well as to the contact names for each of the departments and the public bodies. Justice's web page contains most of the information required by section 70 to be included in the Directory, but the Act specifically requires that there be a written version as well so that those who do not have access to the Internet can also have something to refer to .

The Process

The Act provides that each public body subject to the Act is to appoint an ATIPP Co-ordinator to receive and process requests for information. Requests for information must be in

The over-arching purpose of access to information legislation...is to facilitate democracy. It does so in two 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 participate 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.

Supreme Court of Canada Dagg v. Minister of Finance [1997] 148 DLR (4th) 385

writing but do not require any particular form (although there are forms available to facilitate such requests). 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.

Once a request for information is received, the public body should identify all of the records which are responsive to the request and vet them with a view to disclosure. 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 of them discretionary. ATIPP Co-Ordinators are often called upon to use their discretion in determining whether or not to release the specific information requested and to interpret the Act in answering requests. The Public bodies must exercise their discretion to ensure a correct balance is struck between the applicant's general right of access to information and the possible exceptions to its disclosure under the Act.

In the case of personal information, if an individual finds information 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.

The ability to manage and effectively use information is a core skill that needs to be at the centre of any public sector education and training strategy.

Hon. John Reid
Information Commissioner of Canada
Annual Report 2002/2003

The Role of the Information and Privacy Commissioner

The legislation provides for the creation of an officer known as the Information and Privacy Commissioner. Her job is to provide an independent review of discretionary decisions made by the public bodies in the application of the Act. The Commissioner's office provides an avenue of non-binding appeal 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 credibility and 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 appointed on June 23, 2000 and her appointment will, therefore expire on June 23, 2005. The Act does provide for an Information and Privacy Commissioner to be re-appointed.

The powers given to the ATIPP Commissioner under the Act to resolve disputes are in the nature of those of an ombudsman. The Commissioner is mandated to conduct reviews of decisions of public bodies and to make recommendations to the "head" of the public body involved. In the case of a Department, the "head" is the minister. For other public bodies, the "head" is determined in accordance with the regulations. The Information and Privacy

Commissioner 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 of receipt of a recommendation. The head of the public body may chose to follow the recommendations made, reject them, or take some other steps 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.

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 Supreme Court of the Northwest Territories. Although there have been some appeals launched under the Act, there have not, to my knowledge, been any judicial decisions under the Act as of yet.

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.

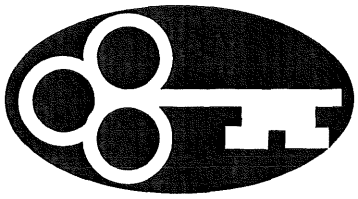
At times, being open and transparent may cause some discomfort for the government of the day – so be it. The need to allow for government decisions and actions to be publicly evaluated and openly assessed remains one of the keys to responsible government. We should have no less.

A successful access to information regime also opens the door to effective public participation in the democratic process. We often hear talk of the so-called "democratic deficit," reflected in such things as decreasing voter turnouts for general elections. Providing the public with access to the information required to assess government actions is a means to reduce this deficit.

Ann Cavoukian
Ontario Information and Privacy Commissioner

Annual Access and Privacy Conference

October 7, 2004



Society's willingness to accept diminished privacy for public safety purposes should not be misinterpreted. It doesn't mean people are any more willing than before to accept businesses misusing their personal information. Surveys have consistently shown high levels of consumer concern about privacy issues, which have thus far impeded the growth of electronic commerce. The need for business to respect customer privacy will not be diminished by this tragedy. Do not make the mistake of confusing one with the other.

Excerpt from: Public Safety is Paramount - But Balanced Against Privacy

Ann Cavoukian
Ontario Information and Privacy Commissioner

September 21, 2001

B. 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 government departments and public bodies. Part II of the Act outlines what have become generally accepted rules for protection of privacy internationally. They include:

- 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, and not from third party sources; and where it is collected from third parties, the individual should be informed of that fact and be given the opportunity to review it;

- Where personal information is collected, the agency collecting the information will advise the individual exactly the uses for which the information is being collected and will be utilized and, if it is to be used for other purposes, that the consent of the individual will be obtained;

- The personal information collected should be secured and the government agency 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 will be used only for the purpose it is collected; and

- Each individual is entitled to personal information about themselves held by any government agency and has the right to request that it be corrected if they feel it is inaccurate.

Prior to April 1, 2004, the Information and Privacy Commissioner was not given any specific authority under the Act to review complaints of breaches of privacy pursuant to the privacy provisions of the Act. The Information and Privacy Commissioner did, however, receive privacy complaints, make inquiries, attempt to resolve conflicts and made recommendations to public bodies with respect to privacy matters, albeit informally and with no specific mandate to do so. Prior to April 1, 2004, the only formal option available to someone who felt their privacy had been compromised was for that person to seek to have the person in the public body who breached the privacy protections of the Act prosecuted under section 59. As the Act is written, however, prosecution was clearly reserved for extreme cases, and there was no mechanism to review process or make change to avoid problems which might come to light.

Amendments to the Act introduced in 2003, however, and to take effect April 1st, 2004, will give the Information and Privacy Commissioner specific authority to review privacy complaints and make recommendations to the public body when privacy has been breached. This amendment is the result of recommendations made by the Information and

> The closer the information is to one's "biographical core" such as information about one's health, genetic characteristics, sexual orientation, employment, social or religious views, friendships and associations — the greater is the obligation on government to respect and protect the individual's privacy
>
> **David Loukedelis**
> **British Columbia**
> **Information and Privacy**
> **Commissioner**
> **"Privacy and the USA**
> **Patriot Act"**
> **October 2004**

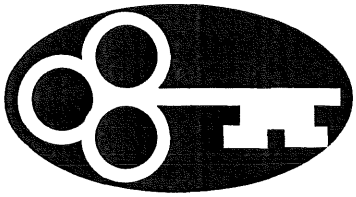
More broadly, excessive surveillance in the name of national security and public safety can threaten the freedoms on which every successful democracy depends. Awareness of widespread surveillance makes people nervous about speaking their minds, engaging in political activities, or doing anything that might arouse ill-founded or vague suspicion. Excessive surveillance herds people toward conformity and discourages the diversity of ideas and beliefs that are indispensable to the flourishing of our communities.

David Loukedelis
BC Information and Privacy Commissioner

Excerpt from : Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing

October 2004

Privacy Commissioner in previous annual reports and is a very positive step which will allow the Commissioner to review government practices and make recommendations as to how to improve process and practices which might, inadvertently or otherwise, lead to inappropriate disclosure of personal information. This has made the privacy provisions of the Act, which were weak and ineffectual, much more responsive and effective. The ever increasing amounts of information collected and retained by government, the amount of outsourcing which governments now do, and the evolution of technologies which allow easy data matching and sharing make it all the more important that this independent review process be in place and I commend the Government for taking this step.



Overall, most studies indicate that CCTV's (Closed Circuit Televisions) are not an effective means for reducing crime. CCTVs are effective at reducing incidents of burglary and property crime, but they are not effective against personal crime, violent crime or public disorder. A report released by NARCO (National Association for the Care and Resettlement of Offenders) states that CCTVs result in a 5% reduction in crime whereas better street lighting results in a 20% reduction in crime. These figures are fairly consistent throughout most CCTV studies

Literature Review on Issues of Privacy and Surveillance Affecting Social Behaviour

Stephen Greenhalgh, MA, MLIS
August, 2003

III. 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. This request must be made within 30 days of a decision by a public body in respect 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 involved and obtain an explanation from the public body. In most cases, the Commissioner will obtain a copy of the Applicant's original request for information and a copy of all 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 file. 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 an inquiry process. All of the parties involved, including the public body, are given the opportunity to make written submissions on the issues.

The Information and Privacy Commissioner's Office received ten (10) new requests for review in fiscal 2003/2004. This is up by two from the previous year in which eight such requests had been received.

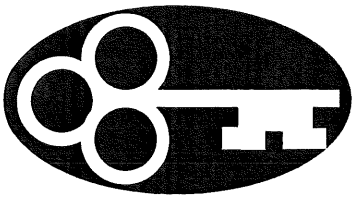
Eight review recommendation were made in fiscal 2003/2004, up two from 2002/2003.

Of the new requests received in 2003/2004, the following public bodies were involved:

Justice	3 requests
Financial Management Board	2 requests
Health and Social Services	1 request
Resources Wildlife & Economic Dev.	1 request
Transportation	1 request
Hay River Health and Social Services	1 request
NWT Housing Association	1 request

The right to remain anonymous (leaving no trace to one's identity) is something w have sought to maintain as a fundamental element in defending our private space. At best, we should only have to identify ourselves to government or business when knowledge of our identity is essential to concluding a particular transaction. It would not normally be essential when we are merely seeking information. Otherwise, we should be able to choose whether or not to reveal our identity. This is true as much in the electronic world as in the physical world.

John Woulds
Former UK Deputy Data Protection Commissioner as quoted in David H. Flaherty, "Defending the Right to Anonymity" , a paper delivered at "Frontiers of Privacy", Victoria, BC (Feb 13, 2003)



IV. REVIEW RECOMMENDATIONS

Review Recommendations #03-31

In this request, an Applicant sought from the Department of the Executive a list of the annual salaries of deputy ministers and presidents of corporations owned by the Territorial Government. The Applicant had been provided with a list showing the pay range for these employees but the Executive refused to disclose the actual salaries of any individual, relying on section 23 of the Act, which prohibits the disclosure of personal information where that disclosure would be an unreasonable invasion of an individual's personal privacy.

In making her recommendation, the Information and Privacy Commissioner agreed generally with the public body's refusal to disclose the information requested, noting that section 23(4) of the Act specifically provides that the disclosure of "salary ranges" is deemed not to constitute and unreasonable invasion of privacy, implying that the disclosure of specific salaries would be unreasonable. She recommended, however, that the Applicant should be provided with a salary range for each individual deputy minister and the president of each crown corporation, rather than a range within which all of them, collectively, were paid.

The Information and Privacy Commissioner's recommendations were accepted.

In drafting the personal information exemption provided by section 21 of the Act, the legislature weighed the competing interests of access and privacy and determined that, as a general rule, individual salary figures of public servants should be protected from disclosure, while salary ranges for positions held by these individuals should be accessible to the public.

Order 61
Ontario Information and Privacy Commissioner

As business processes become more complex and sophisticated, more and more personal information is being collected and used. As a result, the privacy of this personal information has become more vulnerable and is an increasingly critical concern for organization, the government and the public in general. With identity theft on the rise, and with fears of financial or medical records being accessed inappropriately, the number of challenges related to the protection of personal information is steadily increasing.

American Institute of Certified Public Accountants

Review Recommendation #03-32

This was a request for specific information about the severance benefits paid to two senior government employees upon their departure from government employment. In this case, the Applicant was asking to receive copies of the severance agreements entered into. Once again, the Department of the Executive took the position that the disclosure of this information would constitute an unreasonable invasion of the privacy of the individuals involved and declined the request.

The Information and Privacy Commissioner agreed that much of the information in the two contracts did, in fact, constitute personal information about the two individuals. After reviewing the specific provisions of section 23 of the Act, which provide guidance as to when the disclosure of personal information will and will not be considered to be an unreasonable invasion of a third party's privacy, the Information and Privacy Commissioner identified those parts of each contract which should be disclosed, and which parts should not be in light of the privacy provisions of the Act.

The Information and Privacy Commissioner's recommendations were accepted by the public body.

Review Recommendations 03-33

This Request for Review involved the Department of Justice. The Applicant in this case was requesting a copy of the file

Specifically, the record requested is the names only, without other personal information relating to the petitioners. In this case, however, the names do not appear alone but in the context of having signed a petition requesting a review of municipal practices. Disclosure of the names would reveal the fact that identifiable individuals signed the petition, which is other personal information about the petitioners.

Ontario Information and Privacy Commissioner's Office.
Order 171 (Appeal 890023) concerning the Ministry of Municipal Affairs

regarding his claim for compensation under the Criminal Injuries Compensation program administered by the Department. The Department had provided parts of the file to the Applicant but denied him access to that part of the file which had originated with the Royal Canadian Mounted Police on the grounds that "disclosure could reasonably be expected to impair relationships between the Government of the Northwest Territories and the Government of Canada. " and that the department was, therefore, exercising its discretion pursuant to section 16(1)(a) of the *Access to Information and Protection of Privacy Act* to deny access. This was based on the department's consultation with the RCMP who had provided a letter indicating that all material provided to the GNWT was provided in confidence and should not be disclosed. The Applicant indicated that he needed the information to appeal the decision to deny him compensation.

The Information and Privacy Commissioner reviewed the records in question and observed that at least some of the records in question were publicly available in any event, and that section 3(2) of the *Access to Information and Protection of Privacy Act* specifically provided that the Act was not intended to in any way limit access to government information or records normally available to the public. She indicated, therefore, that any of the documents in the Department of Justice file which also appeared on the criminal court file should be provided to the Applicant. She also concluded, however, that for those records which were not already in the public domain, the Department of Justice

It is not for me to say whether or not the public body exercised its discretion well. It is, however, for me to consider whether it is clear that discretion was, in fact, exercised or whether access to the documents in question was denied simply because the information fit into a discretionary exemption. I cannot, in this case, say that the public body did not exercise its discretion. They have obviously considered the possibility of releasing the information and went so far as to request consent from the RCMP.

Elaine Keenan Bengts
Information and Privacy Commissioner
Review Recommendation #03-33

had followed all the necessary steps under the Act and had clearly exercised their discretion to deny access to the RCMP portion of the file. She did suggest, however, that more could have been done to assist the Applicant in this case, if only by the department providing more detailed information to the RCMP when requesting their consent to the disclosure of the information.

The Commissioner's recommendations in this matter were accepted.

Review Recommendation #03- 34

This Request for Review came from a member of the press in respect of a Request for Information made to the Department of Transportation. The Applicant had requested a number of records and received most of those. The only records in issue were records which would indicate the names of sitting Members of the Legislative Assembly who had accounts owing to the department which were in arrears and the amounts owing. The department denied access to this information, citing section 24(1)(c) of the Act, on the basis that the information in question was provided to them in confidence by third parties and the disclosure of the information could result in the loss of revenue, corporate reputation and goodwill as commonly understood in the private sector.

The Department, on review, provided a number of additional arguments as to why the information in question should not

In this case, the Applicant has made a request for records relating to a very specific matter, being the amounts of money owed to the Department by sitting Members of the Legislative Assembly. It is not for the Department to determine what, or what is not, sufficient to meet the Applicant's stated objective. Rather, it is for the Department to provide the Applicant with the records responsive to the request, regardless of whether or not the Department considers those records to have any connection to the Applicant's stated objective.

Elaine Keenan Bengts
Information and Privacy Commissioner
Review Recommendation 03-34

be disclosed. Firstly, they suggested that the information already provided to the Applicant was sufficient for his stated purposes which was to allow him to "gauge the territorial government's effectiveness in collecting on accounts owed it". They took the position that the information which had been provided was "far beyond what is required to meet [the Applicant's] stated objectives." The Information and Privacy Commissioner noted that although the Applicant's stated motive may assist the department in responding to a request for information, it could not limit the information provided and it was not for the department to determine what was sufficient for the Applicant's purposes or objectives.

The department also relied on section 24(1) of the Act, saying that the information requested constituted financial information of a third party (the MLA's) which had been obtained in confidence. The Information and Privacy Commissioner pointed out that a statement of amounts owing to the government by an individual was not "obtained" or "supplied" to the government and could not, therefore, be protected from disclosure under section 24(1).

The next argument made by the department was that sections 79 and 80 of the *Legislative Assembly and Executive Council Act* provides that the department is not required to disclose records that may or may not include information about a sitting MLA's financial dealings with the government. The Information and Privacy Commissioner, however, pointed out that this legislation merely requires a sitting MLA to disclose his or her assets and corporate

interests to the Conflicts of Interest Commissioner and does not preclude the disclosure of that Information on a Request for Information under the *Access to Information and Protection of Privacy Act*. Furthermore, she pointed out, section 4 of the ATIPP Act provides that its provisions prevail if there is a conflict between it and another Act.

The Information and Privacy Commissioner noted that the information being requested appeared to be personal information about individual MLA's in their capacities as private citizens and that, although the public body had not referred her to section 23 of the Act dealing with the unreasonable invasion of privacy, this is the section which would appear to apply. Based on section 23, she indicated that the information being requested was, very likely, the personal information of the individual MLA's involved and that the disclosure of the exact amount owing might well be an unreasonable invasion of the privacy of those individuals. However, in light of their public positions, she felt that it would be appropriate for the public body to consult with the MLA's involved to determine whether they might consent to the disclosure of the information in question. If they did not agree to the disclosure of the specified amounts, the Information and Privacy Commissioner suggested that the name of each MLA be provided, along with an indication of the "range" of the debt owed (for example, MLA #1 owed between $1000 and $2,500 to the public body).

In responding to the recommendations, the head of the public body indicated that it had reviewed the relevant records in

The protections for commercially sensitive information contained in section 20 of the Act are both broad and mandatory. However, there is also a heavy onus on government institutions not to refuse disclosure under these sections based on mere assertions of commercial confidentiality or competitive harm from disclosure. Rather, there must be evidence of harm, at the level of probability, and concrete evidence that the information in question is of a confidential nature.

Hon. John Reid
Information
Commissioner of Canada
2003/2004 Annual Report

Clearly, there is no obligation for any public body to find and disclose information which is in the control of another public body. I do believe, however, that section 12 puts the onus on the public body to forward a request for information to another department where the information would be more easily available in the other department. It is sometimes difficult, especially for someone unfamiliar with the workings of government, to know where the most likely source of the information might be. In this case, FMB apparently did take steps to determine that the Applicant had also filed the same request with the Department of Finance and that, I think, meets the requirements of subsection 12(1).

Elaine Keenan Bengts
Information and Privacy Commissioner
Review Recommendation #03-35

detail and had determined that, at the time of the Applicant's request, there were no records that indicated that there were any monies owing to the Department personally by any sitting MLA. The response went on to point out, however, that the head of the public body did not agree with the analysis of the Information and Privacy Commissioner and, if there had been any responsive documents, would not have accepted the recommendations made with respect to the disclosure of the names of individuals.

Review Recommendation #03-35

This review involved very similar information to the information involved in Recommendation #03-34. In this case, however, the request was made to the Financial Management Board (FMC) for the names of sitting MLA's for whom there were outstanding accounts or overdue receivables exceeding 90 days owing to the Government of the Northwest Territories. FMC provided the Applicant with a list that referred to MLA #1 and MLA #2, indicating the exact amounts owing and how long they were past due. Both amounts were less than $1000 and in one case, the amount was only $25.00. The information provided to the Applicant also indicated that the larger account had been paid between the date of the initial Request for Information and the date of the response. The Applicant was not satisfied, indicating that he wanted the names of MLA #1 and MLA #2.

In this case, the Information and Privacy Commissioner agreed with the public body that, barring their consent, it

Would the release of the names of MLA's who owe money to the Financial Management Board be an unreasonable invasion of their personal privacy? Part of the answer to that will depend on the circumstances in which the debts arose. If they arose in the context of the MLA's work as an MLA, I would suggest that it would be hard to argue that the disclosure of the information would be an unreasonable invasion of his or her personal privacy. If, however, the debt arose simply from personal dealings that we all have with governments on a day to day basis (for example, annual tax levies for property), the answer is not so clear.

Elaine Keenan Bengts
Information and Privacy Commissioner

Review Recommendation #03-35

would be an unreasonable invasion of the privacy of the two MLA's involved to disclose their names, providing that the debts due had nothing to do with their roles as MLA's. If the debts were incurred by the MLA's as a result of their public role as MLA's, the commissioner indicate that they cannot have any expectation of privacy. However, if the debts were incurred by the MLA's in their private capacities as residents of the Northwest Territories, they were entitled to the same right of privacy as other citizens. The Information and Privacy Commissioner did, however, suggest that in light of the fact that the individuals involved were public figures, it would be appropriate for the department to contact the MLA's to see whether they were prepared to consent to the disclosure of the information in question, particularly in light of the relatively small amounts involved and the fact that the larger of the two had since been repaid.

The Information and Privacy Commissioner's recommendations were accepted in that the head of the public body chose not to disclose the names of the MLA's that had debts owing to the government. No comment, however, was made on whether or not the third parties had been consulted as to whether or not they would provide their consent.

Review Recommendation #03-36

The Applicant in this case made a request to the NWT Business Credit Corporation (BCC) for copies of all records pertaining to a certain collection litigation involving the BCC

In all of these circumstances, and particularly in light of the fact that the individuals in question are elected officials, it is my opinion that it would have been appropriate in this case to ask those two individuals if they had any objection to the disclosure of the information in question. I suspect that they would consent. By simply refusing to disclose the information, the public body plants the seed of suggestion that some impropriety exists and I would think that most elected officials would like to avoid that conclusion

Elaine Keenan Bengts
Information and Privacy Commissioner

Review Recommendation 03-35

as plaintiff against an individual who was, at the time of the Request for Information, a sitting member of the Legislative Assembly. In its initial response to the Applicant, BCC took the position that it could not disclose the information requested based on section 15 of the *Business Credit Corporation Act.* When the matter came up for review, BCC changed its approach and argued that the information requested was personal information, the disclosure of which would constitute an unreasonable invasion of a third party's privacy. They further suggested that the information was "confidential" and that there were "valid policy reasons" supporting the non-disclosure of the requested information, although those policy reasons were not outlined.

In this case, the Information and Privacy Commissioner found it difficult to make recommendations as the public body did not provide her with copies of the responsive documents so that she could independently assess the nature of the information involved.

The Information and Privacy Commissioner made the observation that the public body did not go far enough to assist the Applicant. At the very least, BCC should have provided the Applicant with details of the litigation in question and given him guidance as to how he could examine the court file himself.

The Recommendation made was that the Applicant be provided with copies of all court documents in the possession of the public body which were filed in the court in connection

with the litigation in question, as those would be available to him as public documents in any event. She also directed BCC to provide her with copies of the responsive documents so that she could review them and finalize her recommendations with respect to the balance of the responsive records.

The Commissioner's recommendations were accepted.

Review Recommendation # 04-37

This was another request to the Financial Management Board for a copy of a severance contract between the Government of the Northwest Territories and a former senior employee of a public body.

FMB took the position that the entire document was exempt from disclosure pursuant to section 23(1) of the Act, as it was the personal information of the former employee and its disclosure would be an unreasonable invasion of that person's personal privacy.

The Applicant argued that the contract may well contain the personal information of the former employee, but that it was not exempt from disclosure because it was information which fell under section 23(4) of the Act, which sets out a list of circumstances in which the disclosure of personal information will be deemed not to constitute an unreasonable invasion of privacy. The Applicant suggested that the information in the contract represented a "discretionary benefit of a financial

In my opinion, the term "discretionary benefits" include all benefits, financial and otherwise, that are not required to be paid for work done but which, at some point, are within the discretion of the employer to include or not in a pay package or a termination agreement. They include such things as medical benefits, housing assistance, removal assistance and performance pay.

Elaine Keenan Bengts
Information and Privacy Commissioner

Review Recommendation 04-37

nature" because the compensation package was a negotiated amount, subject to the discretion of the public body. The Applicant also relied on a case from the Ontario Information and Privacy Commissioner where it was, in similar circumstances, held that the information in a retirement contract could not be said to describe an individual's finances, income, assets, net worth, financial history or financial activity but showed , instead, a one time payment to be conferred immediately or over a defined period of time arising directly from the acceptance of the former employee of a negotiated retirement package.

The Information and Privacy Commissioner agreed that some of the information in the severance contract did, in fact, constitute the personal information of the individual involved. She reviewed the terms of the contract and applied both the Act and case law from other jurisdictions and recommended that the contract should be disclosed but that certain specifics in the agreement be severed so as to protect the personal information of the former employee.

The head of the public body decided not to disclose any part of the termination agreement, thereby rejecting the Commissioner's recommendations.

This decision has been appealed to the Supreme Court of the Northwest Territories.

Clearly, any time that the government expends public money, the public should have the opportunity to evaluate, for itself, whether it was money well spent. The more controversial the expenditure, the more important it is to the credibility of government that the public be able to scrutinize the government's actions as minutely as possible.

Elaine Keenan Bengts
Information and Privacy Commissioner

Review Recommendation 04-37

The critical test is whether the opinion or comments refer primarily to individuals themselves or the manner in which they carry out their duties or directed to the position and the nature of those duties. In other words, is the information, comments or opinions about an individual rather than the position in which they are employed.

Dagg v. Canada (Department of Finance) (1997) 148 D.L.R. (4th) 385

Recommendation #04-38

In this review, the person requesting the review was a Third Party whose name and other personal information was contained in records which another individual had requested from the Department of the Executive. The individual who had originally requested the information was a member of the press who was doing research on a story and who had requested copies of all records relating to any complaints which might have been launched against a certain individual (the Third Party) under the Workplace Conflict Resolution Policy. Eventually, the complaint was transferred to be dealt with by another agency, outside of the government. The only records which the public body had, therefore, were copies of correspondence up to the point that the complaint was forwarded. The public body took the position that most of the records should be disclosed. They severed the name of the Complainant and other references in the records that might have identified the complainant, but they did not intend to sever the name of the person against whom the complaint was made or any other references to her. It was their position that an accusation cannot, by itself, qualify as personal information because it was an accusation only, untried and untested. As such, they said, it did not fall under any of the headings listed under the definition of "personal information" contained in the Act.

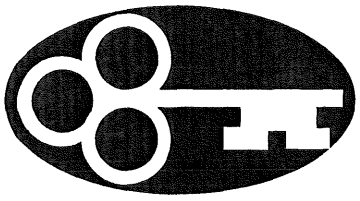
The Information and Privacy Commissioner considered whether or not the information in the complaints was about the person or about the person's position or job functions.

She concluded that the information in question was about the individual and really did not relate to her position or job functions and that it was, therefore, her personal information. Furthermore, much of the information was nothing more than "opinion" expressed by the Complainant about the Third Party. By definition, opinion belongs to the person about whom the opinion is expressed. She concluded that much of the information requested was protected from disclosure as being the personal information of the Third Party, the disclosure of which would be an unreasonable invasion of the Third Party's privacy. Her recommendation was that only very limited parts of the information responsive to the request for information should be disclosed.

The Recommendation was accepted.

No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.

Article 12
1948 Universal Declaration of Human Rights



In a democracy, the people are vested with ultimate decision-making authority, which they delegate to elected representatives and other public servants. Except in very limited and specific circumstances, public officials should conduct their business in open, not in secret, and ensure that the people to whom they are accountable - the public - are given proper notice of all meetings.

Making Municipal Government More Accountable - The Need for an Open Meetings Law in Ontario
Office of the Ontario Information and Privacy Commissioner
Oct 2003

VIII. RECOMMENDATIONS

I was pleased to see that some of the recommendations which I have made in previous years have now been acted upon. The Information and Privacy Commissioner will now have formal authority to review a privacy complaint, and that is a significant and positive step. The issue of what happens if the head of the public body does not respond to a Review Recommendation within 30 days has also been resolved, albeit in a way which I believe is counter to the general spirit intended by the Act. Be that as it may, the issue is resolved and those using the Act now know what happens when the head of the public body does not respond to a recommendation as required by the Act.

Other recommendations which have been made in previous Annual Reports remain unaddressed. My recommendations, therefore, will continue to seek that these matters be addressed.

A. I recommend that the Government of the Northwest Territories direct the preparation and publication of an updated "Access and Privacy Directory" as required by section 70 of the Act . Once published, the Directory should be made available, either at no cost or for a nominal fee, to the public. Further, the Directory should be available for review by the public at government offices throughout the Territories. The Directory should also be made available on line on the Government's web page in such a manner as to be easily found and accessed, perhaps by a direct link

from the Legislative Assembly's web site.

B. The regulations naming the public bodies subject to the act should be reviewed annually to ensure that they remains up to date and reflect changes that are made in the way government does business. For example, the Legislative Assembly may wish to consider whether the new Human Rights Commission should be made subject to the Act.

C. I have found in the last year or so that most (though not all) departments have people who are familiar with the requirements of the Access to Information and Protection of Privacy Act. However, the various boards and agencies appointed by the Government seem to be less familiar and are having some problems dealing with both initial requests for information and with reviews. I recommend that when appointing members of boards, government contractually require at least the more senior members of boards and other agencies to receive ATIPP training and to refresh that training at least once every two years.

D. Further to the last recommendation, with respect to publicly appointed boards, some confusion has become apparent over the course of the last year as to what constitutes a record "in the possession of" the public body. Board members who are not otherwise employees of the government of the Northwest Territories do not appear to be aware that the records they receive and the

Change must come from the ranks of the most senior public servants and from the political level itself. The best guarantee of that change is greater access by the public, the media, non-government organizations, and others to information that enables them to scrutinize the workings of government and hold public servants and politicians accountable.

Hon. John Reid
Information Commissioner of Canada
Annual Report
2002/2003

notes they take while doing board business are subject to access requests (as well as to the privacy provisions of the act). When they leave the Boards, they often take their files and their notes with them. These are, however, public records and should be open to the public on a request for access to information. I would recommend, therefore, that the Act be amended to clarify that members of Boards are to be considered to be public employees for the purposes of the Act and that all Board members be given instruction as to the collection, use and disclosure of information and records which come into their possession in their role as board members. Although the logistics might be difficult, I would also recommend that a protocol should be developed with respect to how boards and individual board members are required to deal with records created, obtained or received in the course of their work on those boards to limit as much as possible the improper disclosure of personal records as well as to ensure that all board records are available for an access request in the normal course. This protocol might, for example, include a requirement that all board members return all printed materials to the Board's recording secretary or executive director at the end of meetings, along with at least a copy of any notes taken during the meeting. It may be that this protocol would have to be "tweaked" to meet the procedural realities of individual boards, but there should be, at the very least, a clear set of guidelines developed and applied to all boards and agencies that are subject to the act.

Ten centuries ago, at the previous millennium, a Viking lord commanded the rising tide to retreat. No deluded fool, King Canute aimed in this way to teach flatterers a lesson -- that even sovereign rulers cannot halt inexorable change.

A thousand years later, we face tides of technology-driven transformation that seem bound only to accelerate. Waves of innovation may liberate human civilization, or disrupt it, more than anything since glass lenses and movable type. Critical decisions during the next few years -- about research, investment, law and lifestyle -- may determine what kind of civilization our children inherit. Especially problematic are many information-related technologies that loom on the near horizon -- technologies that may foster tyranny, or else empower citizenship in a true global village.

David Brin
Aug. 3, 2004

However, many of the disclosures [of publicly available records] were practices developed at a time when the predominance of paper records provided a practical protection for personal information. It was just too difficult for any but the most determined to locate and copy personal information, which was held in many different locations. The value of "practical obscurity" has been eroded by computerization, and so disclosure now takes place in an entirely new context. This new context, in my view, necessitates a review of government practices in the sale of personal information.

Excerpt from: Balancing Access and Privacy: How Publicly Available Personal Information in Handled in Ontario, Canada

Ann Cavoukian Information and Privacy Commissioner for Ontario

October, 2000

E. As noted in previous Annual Reports and in my report to the Standing Committee I have long been a proponent of including municipalities as "public bodies" under the Act. The alternative is to develop stand alone legislation to apply to municipalities to govern both access to information and protection of privacy. Not only is it important that municipal authorities be accountable to the public, it is also clear that municipalities, particularly tax based municipalities, gather and maintain significant information about individuals in their day to day dealing with the business of running communities. I am receiving an increasing number of inquiries from municipalities themselves and from the public about what rules govern municipalities when it comes to both access issues and privacy issues. Because municipalities do not fall under either the *Access to Information and Protection of Privacy Act*, or the federal *Personal Information Protection and Electronic Documents Act,* these entities are really in a limbo which gives them no guidance. I would again encourage the government to consider legislation to include municipalities under an access to information and protection of privacy regime of some kind.

F. On the same theme, I continue to be concerned about the outsourcing of various government functions, particularly in those sensitive areas which include the collection, retention and use of financial and/or medical information of individual residents of the

The public's demand for greater accountability is getting stronger and "trust me" is just not good enough; either for shareholders who demand accountability from their corporate directors, or for citizens who expect good governance at all levels.

For government, transparency is a key requirement to achieve accountability.

Integrity will always be an issue unless we have rules for transparency that are clearly understood and consistently adhered to.

Dr. Ann Cavoukian and Tom Mitchinson
Oct. 14, 2003.

Northwest Territories. The health sector is particularly troublesome, in that this kind of information is highly sensitive and there is a fair amount of outsourcing of various aspects, of , for instance, medical care. Those who undertake medi-vac services, those who manage the telehealth system, dentists, and many other service providers in the private sector gather information by reason of their contracts with the Government of the Northwest Territories. In fact, there are a large number of private entities which administer or undertake public functions on contract with the Government of the Northwest Territories. I have previously recommended that there be clear provisions included in all contracts for such services to compel those organizations to comply with the *Access to Information and Protection of Privacy Act* and to comply with requests made by the public body to provide any records responsive to access requests received. There must be some assurance that those private companies have the responsibility to allow the public access to relevant records in accordance with the Act and to adhere to the privacy provisions of the Act. Access and privacy clauses should be standard fare in outsourcing contracts.

G. I continue to feel that the Northwest Territories should be taking steps to create "made in the north" legislation to deal with the protection of personal information in the private sector, rather than leaving this field to the federal government and the federal

Privacy Commissioner's office. This is a particular concern in the health sector. Health care is not only a public sector service. There are many private sector businesses which receive and hold very sensitive personal information. Most private businesses in the health sector are careful and responsible in the use they make of the information they gather and one might hope that they would continue to be so. However, to rely exclusively on volunteer adherence to a privacy policy by the private sector in today's world is, I would suggest, short sighted and overly optimistic. Furthermore, legislated guidelines can provide consistency in approach and practice. Even if the government does not want to tackle generalized private sector legislation, I would strongly recommend that it does consider health sector legislation.

H. I repeat my assertion that this government should consider generalized privacy legislation over private sector businesses. As noted at the beginning of this report, technological advancements, easy access to databases, the free wheeling and 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 information and guidelines and, in some cases, the rule of law, to regulate the use they make of personal information. The public needs legislation it can rely on to help them avoid the escalating costs of

Governments make skeptics of Information Commissioners Time after time, regime after regime, scandal after scandal, government leaders raise expectations by promising to be more accountable and transparent. Just as routinely, governments maintain their deep addiction to secrecy, spin, foot-dragging and decision making by nods and winks. When it comes to honouring the public's "right to know", governments have found it profoundly challenging to "walk the walk".

John Reid
Information Commissioner of Canada
Annual Report 2003/2004

identity theft. Although the *Personal Information Protection and Electronic Documents Act* applies to the private sector throughout Canada effective January 1st, 2004, it is legislation administered by the Privacy Commissioner in Ottawa and is quite limited in its ability to deal with some of the smaller, more localized issues as she will have to concentrate on the larger issues of national import. Privacy is becoming more and more prominent, both within business and as a political issue. Private sector privacy legislation will, in very short order, become absolutely necessary for the Northwest Territories to be able to continue to do business with the world. I believe that the Government of the Northwest Territories should be pro-active in addressing these issues, rather than waiting until businesses and individuals in the north have suffered losses as a result of the absence of legislation. I believe that legitimate and ethical business would welcome such guidance and I would encourage the Government of the Northwest Territories to make private sector privacy legislation a priority.

I. The Government of the Northwest Territories is involved in a devolution process to give the aboriginal peoples of the Northwest Territories more say in those issues that most concern them. I would encourage the government to include in those discussions the inclusion of both access to information and protection of privacy protocols. The aboriginal peoples of the

"Freedom of information is a fundamental human right, crucial in its own right and also as a cornerstone of democracy, participation and good governance. Recognition of this key right is essential to empowering all members of society, including Parliamentarians, to strengthening parliamentary democracy, to reversing practices of government by the few and to improving the relationship between Parliament and the media."

Recommendations for Transparent Governance

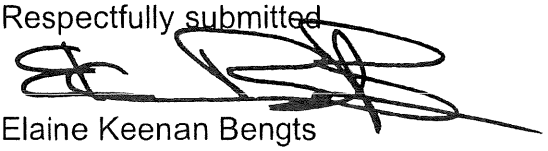
The Commonwealth Parliamentary Association

Northwest Territories have the right to an open government, no matter what form that government takes and it is important for that open government that the people have access to records. Equally important is the right of individuals to control the use of their personal information. There are likely to be cultural differences on many issues particularly when it comes to privacy issues. All peoples, however, have an expectation of a certain level of privacy when it comes to their personal circumstances. These issues should be considered, debated, and incorporated in devolution discussions.

> They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.
>
> **Benjamin Franklin**

When I last appeared before the Standing Committee with respect to my last Annual Report, I emphasized the need for a "corporate culture" which respects the goals of the Act. My strongest recommendation would be to continue to foster this corporate culture. It is sometimes difficult to do. The balance between openness and the protection of personal privacy is difficult to maintain and the line is sometimes difficult to discern. However, as long as the leadership at both the political and the bureaucratic levels remain committed to the principles of the Act, its long term objectives will be achieved.

Respectfully submitted



Elaine Keenan Bengts
Northwest Territories
Information and Privacy Commissioner