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 2004/2005

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

NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER

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

September 11, 2005

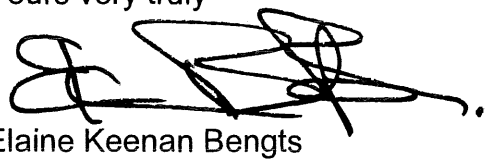
Legislative Assembly of the
Northwest Territories
P.O. Box 1320
Yellowknife, NT
X1A 2L9

Attention: Tim Mercer
Clerk of the Legislative Assembly

Dear Sir:

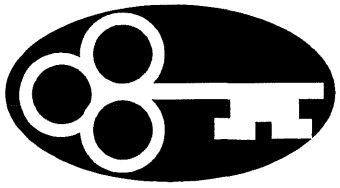
I have the honour to submit my annual report to the Legislative Assembly of the Northwest Territories for the period from April 1st, 2004 to March 31st, 2005.

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

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

Benjamin Franklin

Openness and accountability. Democracy demands both. The challenge is to balance those concepts with the realities of doing business in the wired world and with security concerns which have focussed so much attention from legislators since 9/11. Governments at all levels have taken steps and implemented legislation that would have been considered absolutely unacceptable before terrorists brought unpredictability and fear to America. Most of those steps were taken without benefit of public debate or even contemplation of the possible peripheral consequences of the legislation to our democracy. The United States Patriot Act was one such piece of legislation. This Act allows the FBI and other American Government agencies unprecedented access to the private lives of Americans and non-Americans alike . Our Federal Government passed its own security legislation in the wake of September 11, 2001 which increased the federal government's ability to gather information about Canadians. With the passage of time, one would have hoped that sober second thought and experience may have led to revisions to some of the more unpalatable aspects of the legislation. After all, many of the powers granted in these Acts create more of a "feeling" of security than real security. Instead of reconsidering the necessity of such draconian measures, however, governments have instead created expanded security programs. At the time of the writing of this report, for example, the Canadian government has just announced plans which would allow

police to demand that Internet service providers hand over a wide range of information on the surfing habits of individuals, including online pseudonyms, and whether someone's computer is infected with a computer virus. Not only are governments continuing to introduce new laws, there has been a steady expansion of how information gathered is used. The uses now go well beyond the extraordinary (the prevention of terrorism) and venture widely into the ordinary (general law enforcement). Information ostensibly gathered as a precaution against terrorism is now being used for far wider purposes. In his 2003/2004 Annual Report, my counterpart in Alberta, Frank Work, eloquently made the point by comparing today's world with the world of the German Ministry of State Security (the "Stasi") which had 91,015 career personnel and 174,200 unofficial members performing surveillance of a total population of 16.4 million East Germans. Mr. Work asked himself what the difference was between the Stasi and Canadian society in the post 9/11 world and concluded that the difference is that Canada is a democracy, with a Charter of Rights that acknowledges and protects the rights of individuals and minorities to speak out, protest, dissent and be different. In addition, as Canadians we all have the legislated right to have access to the information which our governments collect and produce so that governments and politicians can be held accountable.

In the end, Mr. Work makes the following observations:

> So what are the lessons from Normannenstrasse?

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

Jennifer Stoddart, Privacy Commissioner of Canada

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

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

- The right of access to information is precious. No government should ever oppose it or impede it on the basis that it is too expensive, too time consuming or only the "trouble-makers" use it.

- Accountable governments are better governments.

- The right to privacy is precious. There must be limits on what the State is allowed to know about us, even in the name of "security". Every State has its ideology (yes, even ours) and, if it has the means, a State will tend to "defend itself" against its perceived enemies from within or without.

- It is never, ever, a question of "what have you got to hide?" It is always a question of "why do you need to know?"

- Well intentioned people can do bad things.

- History may not judge us as we would judge ourselves.

I could say it no better myself.

Access to information continues to be a challenge, particularly for some government agencies. In the last year, some of the challenges came as a result of inexperience in dealing with the Act, rather than any reluctance to adhere to the concepts outlined in it. For others, there continues to be what I would suggest is a visceral reluctance to disclose information. The Financial Management Board Secretariat continues to show reluctance to allow disclosure, at least in the first instance, when responding to requests for information. That agency's willingness to follow my recommendations, however, has improved in that most of the recommendations made in the 2004/2005 fiscal year were accepted and implemented.

A handful of voices - mine included - have long insisted that sacrificing privacy for security represents a Faustian bargain that will have decidedly undesirable repercussions over the long term. Unfortunately, the weight of history strongly confirms what thinkers from Machiavelli, to Benjamin Franklin have told us for centuries: faced with a choice between liberty and security, the majority will choose security.

Bob Barr
U.S. House of Representatives
1995-2003

This year, however, the Department of Resources, Wildlife and Economic Development (which has now been divided into two separate departments....The Department of Environment and Natural Resources and the Department of Industry, Tourism and Investment) was the department which most frustrated me in connection with their handling of one particular request for information. The applicant was seeking information about loans made by the NWT Business Credit Corporation. The information was denied and the applicant asked my office to review the refusal. I requested the department's input on the question and they themselves relied on section 24(1)(f) of the Act to justify their refusal to disclose. That section provides that:

> Subject to subsection (2), the head of a public body shall refuse to disclose to an applicant:
>
> f) a statement of financial assistance provided to a third party by a prescribed board

Recommendations were made based on the submissions of the public body and the Applicant. However, when considering the recommendations made by this office, the department belatedly decided that section 24(1)(f) did not apply because the Business Credit Corporation was not a "prescribed board". Quite apart from the fact that I disagree entirely with that conclusion, if a public body decides to disallow access to information, the onus **by legislation** is on them to show that the information falls within one of the exemptions from disclosure under the Act. Having failed to meet that onus on review, it is, in my opinion, somewhat disingenuous for them to try to avoid disclosure by saying,

after the fact, that the section they relied on to deny disclosure did not actually apply to the records in question. One of the features of the ombudsman format of the *Access to Information and Protection of Privacy Act.* is that the Commissioner's recommendations are not binding. This is both a strength and a weakness. It is a strength in that it allows the Information and Privacy Commissioner to make suggestions and provide direction knowing that governments have some room to work within those recommendations. This will often lead to more innovative resolutions to disputes. One of the weaknesses of such a system is that, public bodies are not bound by or accountable for their submissions when dealing with the Information and Privacy Commissioner If the Commissioner had "order" powers, there would be potentially serious consequences for not being thorough when making submissions in respct to a Request for Review. Because the Information and Privacy Commissioner can only make non-binding recommendations, however, there are no consequences of submissions that are incomplete or not well thought out. Although the Act specifically provides that there is an onus on the public body to do certain things, including the justification of exemptions, that onus is of little import when the department can step back afterwards and say "oops, we didn't rely on the right section of the act and we're therefore rejecting your recommendations". If public bodies were to take this approach consistently, the Act would lose all effectiveness and the Information and Privacy Commissioner all credibility. This kind of response simply cannot be allowed to hijack the system. In my recommendations at the end of this report I have, therefore, suggested that the Act be

The basic purpose of the Freedom of Information and Privacy Act of Saskatchewan "reflects a general philosophy of full disclosure unless information is exempted under clearly delineated statutory language. There are specific exemptions from disclosure set forth in the Act, but these limited exceptions do not obscure the basic policy that disclosure, not secrecy is the dominant objective of the Act".

Saskatchewan Court of Appeal

amended so as to require public bodies to refer to all relevant sections of the Act when making submissions to the Information and Privacy Commissioner and to be bound by those submissions. I have also recommended that section 24(1)(f) be amended to clarify what is intended by the phrase "prescribed corporation or board" so as to avoid this particular problem again.

I have also been asked to deal with a number of privacy issues this year. In most cases, the public body involved worked with me to address the concerns of the complainant. In one instance, however, I was more than a little disappointed in the approach taken by the public body to the complaint and the investigation process. My concerns were exacerbated by the fact that the public body involved was one which provides health care services. I mentioned this case in last year's address to the Standing Committee but it does, in my mind, merit further comment. The facts of the case are set out in some detail later in this report. However, in dealing with this case, I was very surprised that the management team responsible for the privacy breach simply could not understand the concerns of the complainant or of this office. Even after the final recommendations were made, I was left with the impression that I had failed to impress upon them that there were serious problems with the way in which the matter had been handled and that the actions taken were contrary to the Act. The recommendations were accepted only in part and as far as I know, no changes have been made to the policies or administrative process to avoid further inappropriate sharing of information.

The rights and freedoms we have come to expect can be easily eroded in the fight against terror. We should be calling for meaningful and timely reform to the public safety and anti-terrorism acts to comply with clear privacy rights.

Concerns about terrorism have driven public policy. We need to keep our senses about us and assess the real threats, not the exaggerated fear of attacks.

David Loukidelis
BC Information and Privacy Commissioner

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

One of the trends that I have seen in the Northwest Territories (as in the rest of the world) is the proliferation of video surveillance technology as a crime prevention tool. Several times this year I read news reports about video surveillance equipment being place on schools and other public buildings within the Northwest Territories to battle vandalism. Unfortunately, the evidence is that cameras rarely prevent crime and are often less than helpful in solving crime because the pictures are grainy and indistinct. With the recent bombings in London, governments have become even more enthusiastic about video surveillance as a crime prevention tool. However, the evidence is that video surveillance does not prevent crime. It merely moves it to another place. A recent report prepared for the United Kingdom Home Office that assessed the very extensive use of video surveillance in London and other communities has come to what will be for many a surprising conclusion;

> "The truth is that [video surveillance system] is a powerful tool that society is only just beginning to understand. It looks simple to use, but it is not. It has many components, and they can impact in different ways. It is more than just a technical solution; it requires human intervention to work to maximum efficiency and the problems it helps deal with are complex. There needs to be greater recognition that reducing and preventing crime is not easy and that ill-conceived solutions are unlikely to work no matter what the investment."

At one point in the report, the authors state:

> "Assessed on the evidence presented in this report [the video surveillance system] cannot be deemed a success. It has cost a lot of money and it has not produced the anticipated benefits."

I would simply caution public bodies about jumping on the video surveillance bandwagon before studying both the benefits and the costs of such systems.

Some of the national issues in which I joined discussions with my fellow Information and Privacy Commissioners included an exploration of 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.

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, 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. It is clear, however, that

In my opinion, privacy laws are only part of the answer to privacy protection. As with any law, they cannot provide an absolute guarantee. What is essential is that governments understand and respect the immense level of trust citizens place in government when they relinquish any detail of their personal information. They are disclosing details about their relationships, their finances and their health, after which point they have no control over what happens to the information. This lack of control is even more pronounced in an era of digitized information.

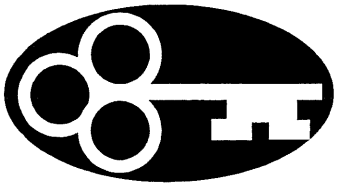
A Special Report
to the Legislative Assembly of Ontario
on the Disclosure of Personal Information
at the Ministry of Health
February 20, 1997
Submitted by Tom Wright
Information and Privacy Commissioner/Ontario

some of the secondary public bodies (boards, housing authorities, health authorities and the like) have very little knowledge of the Act. I have specifically recommended in the context of a request for review that as a minimum, the senior members of such bodies be required to receive mandatory ATIPP training as a condition of their appointment . I would like to see a government wide policy in this regard, rather than a piecemeal policy department by department. It is important that some effort be made to ensure these boards and agencies are properly informed and trained.

I would like to take this opportunity to thank the Legislative Assembly for confirming my re-appointment as Information and Privacy Commissioner for another five year term. I am honoured to be able to serve the people of the Northwest Territories in this capacity and will continue to give my best efforts to addressing the objectives of the Act.

Since 9/11, governments on both sides of the border have taken advantage of the suspect assumption that less privacy means more safety to justify legislation that tramples values synonymous with the freedom they claim to be defending.

JAMES TRAVERS
The Toronto Star (Ontario), August 11, 2005



II. INTRODUCTION

A. ACCESS TO INFORMATION

Background

Purposes 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

These purposes appear fairly straight forward and susinct. However, government is a business like any other and must be able to maintain confidentiality in certain aspects of its work. The Act recognizes that the government does operate in a business world and tries to balance the right of the public

The struggle for information is, first and last, a struggle for accountability

Jeremy Pope, "Access to Information: Whose Right and Whose Information" In Global Corruption Report 2003 at p. 8

Vigilance, by users, the media, academics, the judiciary, information commissioners and members of Parliament, must be maintained against the very real pressures from governments to take back from citizens, the power to control what, and when, information will be disclosed.

Hon. John Reid
Information Commissioner of Canada
2004/2005 Annual Report

to know with the ability of the government to maintain confidentiality where necessary to allow it to do business. 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 confidential personal information about individuals which must be protected from improper use or disclosure.

There is often a difficult balancing to be done in dealing with requests for information in determining which records should be disclosed to the public and 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 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

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

and a number of other governmental boards and agencies. There are exceptions which 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 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. Although some changes have been made over the years, the regulations again need to be updated to reflect recent changes in some of the departments. The regulations continue to show 32 boards and agencies in addition to government departments which are subject to the Act.

The Department of Justice has on its 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 contact information for the ATIPP Co-Ordinator for each of the public bodies subject to the Act so that individuals requesting information can know who they should direct their inquiries to.

The 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

The Act also requires that the Government create and maintain an "Access to Information Directory". The first Directory was prepared in 1996 when the Act came into effect. It has, in the last year, been updated and posted to the internet at the Department of Justice's web page. The Act specifically requires, however, 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 writing. Although forms are available, requests for information do not need to be in any particular form and need not be submitted on the form. 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 disclose the specific information requested and to interpret the Act in answering requests. Public Bodies must often 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.

"Let me encourage everyone to strike the word 'balance' from their vocabulary when talking about privacy and national security. In times of crisis, privacy is going to lose, and that is not OK. Privacy and security are not mutable forces that can rise and fall depending on our level of crisis. They are immutable."

Nuala O'Connor Kelly
Homeland Security Department's
Chief Privacy Officer,

The Role of the Information and Privacy Commissioner

The legislation provides for the creation of an officer known as the Information and Privacy Commissioner. The Commissioner's job is to provide an independent review of discretionary decisions made by Public Bodies in the application of the Act. The Commissioner's office provides an avenue of independent non-binding re-consideration for those who feel that the public body has not properly applied the provisions of the Act. The Information and Privacy Commissioner is appointed by the Legislative Assembly but is otherwise independent of the government. The independence of the office is essential for it to maintain its credibility and ability to provide an impartial review of the government's compliance with the Act. Under the Act, a

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

Commissioner is appointed for a five (5) year term. The current Information and Privacy Commissioner was re-appointed to a third term in June, 2005 and will serve until June, 2010.

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 choose 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

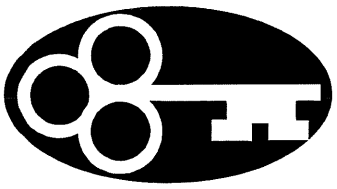
have been some appeals launched under the Act, there have not, to my knowledge, been any judicial decisions under the Act as of yet.

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.

Hundreds of organizations that are recipients of large transfer payments from the government are not subject to the provincial or municipal Freedom of Information and Protection of Privacy Acts, which means they are not subject to public scrutiny. Openness and transparency of all publicly funded bodies is essential - they should be publicly accountable.

Ann Cavoukian
Ontario Information and Privacy Commissioner

Annual Report 2004



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.

First, many people fear they are losing control over what happens to their personal information and worry that their privacy rights are being displaced by economic and national security priorities.

David Loukidelis
BC Information and Privacy Commissioner
2004/2005 Annual Report

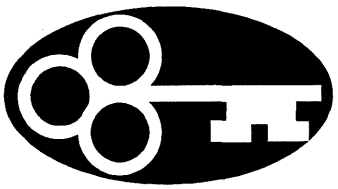
- Personal information collected by a government agency will be used only for the purpose it is collected; and

- 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.

In April of 2004, the Information and Privacy Commissioner was given specific authority under the Act to review complaints of privacy breaches under the Act. This new amendment to the Act provides a real and substantive avenue to file complaints about inappropriate uses of personal information . This is a very positive improvement in the Act which gives teeth to the privacy provisions. Clearly an improper use of personal information cannot subsequently be taken back. Privacy, once breached, is not recoverable. However, these new provisions in the Act do allow for an independent investigation of how the breach occurred and for recommendations to be made which might serve to prevent the same kind of breach again. These amendments are the result of recommendations made by the Information and Privacy Commissioner in previous annual reports.

Second, many people believe that information technology developments are fuelling the appetites of governments for larger data banks and for the mining of personal information for national security and other purposes. They fear that new laws since September 11, have encouraged or compelled the private sector to share personal information with government authorities for national security or law enforcement purposes. They also fear diminished accountability and transparency of the actions of law enforcement agencies in this regard.

David Loukidelis
BC Information and Privacy Commissioner
2004/2005 Annual Report



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

David Loukidelis
BC Information and Privacy Commissioner
2004/2005 Annual Report

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 twenty-four (24) new written inquiries and requests for review in fiscal 2004/2005. This is more than double the number of request received in the previous year. Of these, two were resolved through an informal mediation process and the Applicants withdrew their requests. In one case, the Applicant failed to respond to correspondence from the Information and Privacy Commissioner and the Commissioner, therefore, closed the file without a recommendation being made. Two inquiries were requests which were outside the jurisdiction of the Information and Privacy Commissioner and were not, therefore, pursued further. In one instance, a private organization requested some input on their proposed privacy policy and the Information and Privacy Commissioner provided comments. Of the inquiries received, three of the requests dealt with privacy issues and the balance were about access to information issues. In one of the inquiries, the issue was whether or not the Applicant should be required to pay costs associated with his request for information.

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

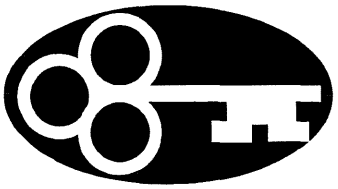
A profoundly important aspect of the post-9/11 changes is the blurring of lines between collection and use of personal information for law enforcement purposes under criminal and other penal laws and use for national security purposes. A defining characteristic of police states is the blurring of distinctions between law enforcement and national security functions, the danger being that the rule of law eventually gives way to arbitrary decision-making by law enforcement authorities and the rights of ordinary citizens lose meaning.

David Loukidelis
BC Information and Privacy Commissioner

Ten Review Recommendation reports were issued which is two more than were issued in 2003/2004.

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

Financial Management Board	5 requests
Justice	4 requests
Liquor Licensing Board	4 requests
Various Health Authorities	3 requests
Resources Wildlife & Economic Dev.	2 requests
Education, Culture and Employment	1 request
Executive	1 request
Legal Services Board of the NWT	1 request
Business Credit Corporation	1 request



IV. REVIEW RECOMMENDATIONS

Review Recommendations #04-39

This was an application by a member of the press to review a response received from the Financial Management Board to the Applicant's request for "the review of allegations against the [Grolier Hall Residential School] Healing Circle, conducted by the Audit Bureau in 2001." The public body denied access to the requested record because the record consisted of confidential financial, commercial and labour relations information of the Healing Circle and others, and it contained personal information of third parties, the disclosure of which would be an unreasonable invasion of the personal privacy of the third parties. The report in question was prepared by the Audit Bureau in response to complaints about misspending and mismanagement by the Healing Circle, a non-profit organization contracted by the Government of the Northwest Territories to provide certain social services.

The Information and Privacy Commissioner agreed with the public body that the Healing Circle was a Third Party as that term is defined in the Act. However, she did not agree with the public body with respect to its claim that the information contained in the report as a whole constituted "financial, commercial and labour relations information" of the third party. To the extent that such information appeared in the report, the Information and Privacy Commissioner suggested that it could be easily severed.

Simply put, the report sets out the findings of an investigation done in response to a complaint and comes to conclusions as to whether or not the complaints were well founded. No recommendations at all are made...only statements of facts and findings. In the circumstances, therefore, I can see nothing within the record which might qualify for a discretionary exemption as "advice, recommendations, or analysis" of a policy making action.

Elaine Keenan Bengts
Review Recommendation 04-039

I therefore believe that a "consultation" occurs when the views of one or more officers or employees is sought as to the appropriateness of particular proposals or suggested actions. A "deliberation" is a discussion or consideration, by the persons described in the section, of the reasons for and against an action. Here again, I think that the views must either be sought or be part of responsibility of the person from whom they are sought and the views must be sought for the purpose of doing something, such as taking an action, making a decision or a choice.

Robert Clark
Former Information and Privacy Commissioner of Alberta
Order 1996-006

She also felt that any personal information of individual third parties contained in the report could be effectively severed so as to protect their identities.

The Public Body also relied on section 14 of the Act which allows a governmental agency to refuse disclosure in its discretion where the disclosure would be likely to reveal advice, proposals, recommendations, analyses or policy options developed by or for a public body or a member of the Executive Council. The Information and Privacy Commissioner found that the report made no recommendations, proposals, analysis or policy options. Rather, it merely set out the findings of an investigation done in response to a complaint and came to conclusions as to whether or not the complaints were well founded.

The Public Body accepted the recommendations of the Information and Privacy Commissioner and disclosed an edited version of the report.

Review Recommendation #04-40

This request was by an individual for access to a report commissioned by the Department of Justice with respect to personnel and hiring matters at the South Mackenzie Correctional Centre and the Dene K'onia Youth Facility known as the "Gullberg Report". The report had been undertaken in 2001 in response to allegations of improprieties in the hiring practices at the Correctional Centres between 1999 and 2001.

The first thing that should be noted is that this is a discretionary section. Should it apply to the record in question, the Department still has to show that it exercised the discretion given to it to refuse access. This would usually be shown by indicating the reasoning behind the refusal.

Elaine Keenan Bengts Review Recommendation 04-041

The Department of Justice in this case refused to provide a copy of the report, although it did provide the Applicant with a copy of the recommendations portion of the report. The department took the position that the Report constituted "plans that relate to the management of personnel or the administration of a public body that have not yet been implemented" (S. 14(1)(d)). The Information and Privacy Commissioner noted that the report did not contain any plans or conclusions. Instead, it contained a statement of findings and recommendations. She found that section 14(1)(d) did not apply to the Report.

The Information and Privacy Commissioner went on, however, to consider whether other sections of the Act might apply to the Report and found that a large section of the report did contain information about the employment histories of several individuals and that this information was protected from disclosure pursuant to the Act.

In the end, she recommended that the Report be disclosed in part after severing the personal information of the individuals.

The public body chose not to follow the recommendations made by the Information and Privacy Commissioner.

Review Recommendations #04-41

This Request also involved the Department of Justice. The Applicant in this case had applied for a position with the Department and was, apparently, an unsuccessful candidate.

I begin my comments by expressing my frustration and concern with the total lack of understanding of and clear disdain for the privacy provisions of the Access to Information and Protection of Privacy Act which was demonstrated both in the actions of the HSS Authority and in their responses to my correspondence. My concern is augmented by the fact that we were dealing with doctors and health professionals who are expected to have a keen appreciation of confidentiality and privacy issues.

Elaine Keenan Bengts
Review Recommendation 04-043

He was requesting a copy of the references obtained by the department in relation to the job competition.

The Department relied on section 22 of the Act which provides that access to a record may be refused where the record contains personal information that is evaluative or opinion material compiled solely for the purpose of determining the applicant's suitability, eligibility or qualifications for employment when the information has been provided to the public body, explicitly or implicitly, in confidence.

The Information and Privacy Commissioner reviewed the records in question and concluded that they constituted evaluative and opinion material compiled solely for determining the Applicant's suitability, eligibility or qualifications for employment in a position which he had applied for. She recommended that the record not be disclosed.

The recommendation was accepted.

Review Recommendation #04-42

This case involved a privacy complaint against one of the Regional Health Authorities. The complainant was an employee of the Health Authority. The complaint, however, was made by the individual as a private citizen as a user of the health system. This person had reason to seek medical attention and was unhappy with the services she received. As a result, she wrote a letter of complaint to the Minister of

If, as has been suggested by the public body, the manager acted within the tenets of the prevailing policy, then the prevailing policy is obviously inadequate and not in accordance with the Access to Information and Protection of Privacy Act. It is simply not good enough to use adherence to policy as an excuse when the policy is clearly not in accordance with the legislative requirements. Further, to suggest that requiring an employee to take an oath of confidentiality is enough to comply with the privacy provision of the ATIPP Act is short sighted at best and negligent at worst.

Elaine Keenan Bengts
Review Recommendation 04-042

Health and Social Services. The Minister referred the claim back to a senior manager to investigate and deal with. The senior manager completed her investigation and wrote a letter to the complainant dismissing her complaint and chastising her for writing a letter to the Minister. The letter suggested that , because she was an employee of the Health Authority, the complainant should know the proper channels for complaints and follow those channels. This letter contained a significant amount of personal information about the complainant, including some medical history which the complainant had not provided in her complaint letter and the fact that she had filed a complaint to the Minister. A copy of this letter was sent to the complainant's immediate supervisor at work.

The complainant's concerns were two-fold. The first was that the senior manager who conducted the investigation of the complaint appeared to have had access to the complainant's entire medical record, even though the complaint filed was very specific and was focussed on the way the complainant had been treated as an individual and not on the treatment of her medical condition. The second concern was that a copy of the letter responding to her request was sent to her supervisor at work.

The public body said that the manager who reviewed the complaint was a medical professional whose job it was to review complaints and that, in her position, she would routinely review "any pertinent facts concerning the client's prior, current and future medical condition" as this was the

only way to reach an objective conclusion on the appropriateness of the care provided. With respect to the letter being sent to the complainant's supervisor, the public body made no bones about the fact that the letter had been copied to the supervisor "in an attempt to be proactive and re-enforce with [the complainant] that client complaints are to be addressed to the most appropriate authority". They dismissed the fact that the letter contained personal medical information about the complainant as being "trivial" because the medical issues were referred to only in the most general of terms.

The Information and Privacy Commissioner found that it was not necessary for the person investigating the particular complaint in question to have full access to her medical file. Furthermore, she suggested that if access to her medical history was necessary, consent should have been obtained from the complainant before access to the file was given. With respect to the letter sent to the complainant's supervisor, the Information and Privacy Commissioner found that it was wholly inappropriate.

A number of recommendations were made and addressed to the Health Authority in question and all other Health Authorities in the Territories as well as to the Department of Health and Social Services.

The recommendations were accepted in part.

To say that the sending of a copy of the letter to AB's work supervisor was done to send a message to AB about the proper channels to take to make a complaint belies the statement made in the same paragraph of the HSS Authority's letter to me that the disclosure was "unfortunate but completely innocent". It was not an innocent disclosure. It was calculated and intentional.

Elaine Keenan Bengts Review Recommendation 04-042

It is true that the report does, indeed, contain portions that would constitute advice or recommendations made to the public body. It also contains a good deal of background information and findings of fact. Background and findings of fact do not constitute "recommendations" or "advice".

Elaine Keenan Bengts
Review Recommendation 04-043

.Review Recommendation #04-43

The Applicant in this case sought access to a copy of a report prepared by an outside consultant for the Department of Education, Culture and Employment. The report had been commissioned and undertaken as a direct result of complaints made by the Applicant about harassment in the workplace. Although the report was prepared for the Department of Education, the Financial Management Board was the public body in possession of the report.

The public body in this case relied on section 14(1) (a) of the Act which provides that the public body may refuse to disclose information to an applicant where it could reasonably be expected to reveal "advice" or "recommendations" developed for a public body. Further, they relied on section 23 which prohibits disclosure of personal information of a third party where that disclosure would be an unreasonable invasion of the third party's privacy.

The Information and Privacy Commissioner agreed with the public body that the report did include sections that would constitute advice or recommendations made to the public body. However, it also contained a lot of background information and findings of fact. The Commissioner suggested that background and findings of fact do not constitute "recommendations" or "advice". She suggested that those portions that constituted recommendations and advice could be easily identified and severed from the report.

However, when an MLA , or any other government employee, owes money to the government of the Northwest Territories and the debt arises as a direct consequence of the role or duties of the employee, the details of that debt cannot be said to be personal information of the debtor. The expenditure of public funds should always be a matter of public scrutiny and when an employee of the public body owes money to the public body as a direct result of his or her role and responsibilities as a member of the public body, that is not a personal matter, but a public one. In my opinion, the details of these debts do not constitute personal information and section 23 does not apply..

Elaine Keenan Bengts
Review Recommendation 04-044

The Commissioner recommended that the report be disclosed to the Applicant after it had been reviewed and certain sections of it severed so as to protect the privacy of individual third parties referred to in the report.

The recommendations made were followed in part.

Review Recommendation #04-044

In this case, a request was made to the Financial Management Board by a member of the press for the names of all Members of the Legislative Assembly who had outstanding debts to the Territorial Government. The Applicant also sought further details with respect to those debts, including when the debt was incurred, the nature of the debt, how far in arrears the debt was, when the last payment was made and the balance owing on the debt. The request was originally denied completely because it was stated to be "overly broad" and that such information was protected from disclosure pursuant to section 23 (personal privacy) in any event. In response to Information and Privacy Commissioner's involvement with the file, however, the public body did disclose some information which was partially responsive to the Applicant's request and included a list of amounts owing by Members of the Legislative Assembly where those debts were incurred by reason of the MLA's role as an elected official. However, no names were provided. The Applicant indicated that he still wanted the names of the individual MLA's who owed the amounts indicated and he still

The Applicant poses the following questions:

Does the public have an interest in knowing whether the Minister responsible for setting policy for collecting rental arrears is behind on his rent? Does the public have an interest in knowing whether the minister who oversees the Business Development Corporation owes any money to that corporation? Does the public have any interest in knowing whether the minister responsible for the Power Corporation has any outstanding debts to the corporation?

In his opinion, the answer to these questions is "of course". I agree that the public may have an interest in knowing the answer to these questions. However, the fact that the public has an interest in knowing these things does not necessarily mean that the public interest is more important, in this particular case, than the MLA's right to privacy.

Elaine Keenan Bengts Review Recommendation 04-044

wanted the list of debts owed by MLA's in their private capacities as well as in their capacities as elected officials.

The Information and Privacy Commissioner recommended that the names of the MLA's who owed money to the government in their capacity as elected officials should be disclosed and that that information was not protected from disclosure pursuant to section 23 of the Act.

The public body indicated that there were some amounts owing by MLA's to the government in their private capacities by way of property taxes, mortgage payments, electrical bills and similar items. The Information and Privacy Commissioner found that this kind of information was personal information the disclosure of which would be an unreasonable invasion of the privacy of the individuals involved. The Applicant urged the Commissioner to apply section 48 of the Act which allows a public body to disclose personal information about a third party where, in the opinion of the Minister, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure. The Commissioner pointed out that only the Minister could not invoke section 48. However, she did encourage the ministry to review the public policy reasons for withholding the information requested and to discuss the matter with the MLA's involved.

The Information and Privacy Commissioner recommended that the names of MLA's who owed money in their capacity as elected officials be disclosed and that , subject only to the

The issues that surround the use of e-mail and other electronic records in business today are numerous, from security issues to retention issues. It is very easy to destroy a public record by simply hitting the 'delete' button on an e-mail record and, although I have asked the question of various government agencies, none have given me a clear indication of the policy with respect to e-mail communication or how that policy is monitored.

Elaine Keenan Bengts
Review Recommendation 05-045

Minister's discretion, the disclosure of the details of amounts owed by MLA's in their capacity of private citizens was personal information and should not be disclosed. The Commissioner encouraged the Minister to speak with the affected individuals to determine their position on the matter before deciding whether or not to exercise his discretion

The Commissioner's recommendations were accepted in part.

Review Recommendation #05-045

The Applicant in this case was initially unhappy with the decision of the Department of the Executive to extend the time for responding to his request for information.

The information requested by the Applicant in this case was a complicated one. The department had indicated that they needed further particulars from the Applicant in order to respond to it. They also pointed out in the same letter that the request potentially involved a number of different government agencies. The Applicant complained that section 11 of the Act, which provides the process for extending the time for responding to a request, was not properly applied in that the public body did not provide a date on which they expected to provide the response.

Before this review could be completed (and within 45 days of the original request) the Applicant received his response to the request for information and I was then asked to review the

response received because some records had been edited to sever some exempt information and because the department indicated that some e-mail records could not be recovered for technical reasons.

The Applicant had a number of concerns with the response received. Among other complaints, he was not satisfied that the e-mail records had been "lost" and felt that there was an attempt to cover up correspondence relating to his situation. He also took exception to the severing of information from some of the records which were provided to him.

The Commissioner found that the department's extension of time was within the requirements for an extension pursuant to section 11 of the Act, with the exception that no date was provided as to when the Applicant might expect to receive the response. She recommended that the department review its "standard form" letter used for this purpose and take steps to ensure that in future a date is provided.

The Commissioner then did a record by record review of the documents identified as being responsive to the Applicant's request and made various recommendations with respect to the disclosure granted. She also made a recommendation that the department, in conjunction with the agency responsible for communications, review policies and procedures with respect to electronic documents and take steps to ensure the appropriate manner of storage, retrieval and destruction of such records.

With more and more business being done "on the internet" and by e-mail, it becomes more important to have clear and unequivocal policies, guidelines and measures to control how these records are disbursed, used and stored. There must be clear policies in place to deal with the organization and retention of e-mail and other electronic records and those policies must be well disseminated and understood by those who work in the public sector.

Elaine Keenan Bengts
Review Recommendation 05-045

Canadian jurisprudence is consistent in holding that the general philosophy behind this type of legislation is full disclosure of information. Access, not secrecy, is the dominant purpose insofar as it relates to government documents. The provisions of the Act must be given a liberal and purposive construction. The legislation recognizes that there are legitimate privacy interests that must be respected but any exceptions to the rule of disclosure must be clearly delineated in the legislation.

CBC v. The Commissioner of the Northwest Territories [1999] N.W.T.J. No. 117

The Commissioner's recommendations were accepted.

Review Recommendation #04- 46

The Applicant in this case asked for access to certain documentation regarding the awarding of a contract for the provision of chartered air medevac services from the Stanton Regional Health Authority. Many of the records requested were disclosed, but there were a number instances in which some of the information had been severed. The Applicant objected to the severance of that information and sought a review.

The Public Body relied on section 24 of the Act, which is designed to protect the business interests of Third Parties with whom the public body does business.

There were three kinds of records under consideration in this matter. The first was a contract between the public body and a private sector business for the provision of medevac services. The public body disclosed a major part of the contract, but refused to disclose two schedules attached to the contract because they contained confidential financial, commercial or technical information obtained in confidence from the third party, the disclosure of which could be reasonably expected to result in undue financial loss or prejudice to the competitive position of the Third Party Contractor. The Information and Privacy Commissioner agreed with the public body .

Clearly, the government must enter into contracts with the public sector in order to accomplish its obligations. To that end, it is important for the government, as a business interest, to be able to maintain the confidentiality of its business associate's information. There is a difference between disclosing its own financial information and accounting for its own spending and disclosing the commercial, technical and financial information of its business partners. In my opinion, it is important for the government to be able to contract with third parties in such a way that the third parties can be confident that their commercial and financial confidentiality will be maintained as far as possible.

Elaine Keenan Bengts
Review Recommendation 05-046

The second kind of record was described by the public body as being an evaluation prepared by the public body's "evaluation team" for the proposals received in response to the public body's Request for Proposals. The Information and Privacy Commissioner concluded that this report was prepared specifically for the purpose of providing analysis of the various proposals received in response to the public body's Request for Proposals and, except for the first four pages which contained only a statement of "methodology", the balance was either a transposition of the confidential third party information or "analysis" and "recommendations". The third party information was protected for the same reasons as the schedules to the contract. The analysis and recommendations were subject to a discretionary exemption and the public body had applied that discretion and decided not to disclose the record.

The last set of records responsive to the Applicant's request were copies of invoices submitted to the public body under the medevac contract. The public body refused to disclose the invoices themselves, but instead prepared a summary. The Health Authority took the position that they could not provide the more detailed invoices themselves because they contained sensitive medical and personal information about third parties. The Information and Privacy Commissioner felt that the compromise that the public body suggested, which would provide the Applicant with the financial details of the public monies spent on this public service, was a reasonable one. It was detailed enough to ensure that the government was subject to public scrutiny, but not so detailed as to

breach personal privacy of individuals or to reveal the specific fee structures of the Third Party.

The Information and Privacy Commissioner found that the public body properly applied the various sections of the Act to the request for information and, with the exception of the first four pages of the evaluation document, which should be disclosed, the public body had otherwise made an appropriate disclosure.

The recommendations of the Information and Privacy Commissioner were accepted. The Applicant has appealed the Minister's decision to the Supreme Court.

Review Recommendation # 05-47

This file involved a request to the Department of Resources, Wildlife and Economic Development for a list of businesses who received loans from the NWT Business Credit Corporation (BCC) from 1999 to 2004. The public body refused to disclose the information requested on the ground that section 24 of the Act prohibits public bodies from disclosing "a statement of financial assistance provided to a third party by a prescribed corporation or board". The Information and Privacy Commissioner agreed that it would be contrary to the Act to disclose a list of companies who had received financial assistance from BCC and how much had been received. She found, however, that it would not be contrary to the Act to provide a list of businesses who had received funding without indicating how much funding had been provided. She recommended that a list of businesses

In my opinion, the mere fact that a company received a loan from BCC is not a "statement of financial assistance" in that it does not indicate credits and debits or any other details. A statement that financial assistance has been given to a particular company is not the same as a "statement of financial assistance given" to a company. There is nothing in the Act which, in my opinion, prohibits the public body from disclosing which companies have received financial assistance from BCC, provided that the details of that financial assistance are not disclosed.

Elaine Keenan Bengts
Review Recommendation 05-047

that had received BCC funding during the relevant period be disclosed.

The public body declined to follow the recommendations made by the Information and Privacy Commissioner on the basis that the section of the Act that they had relied on in submissions to the Commissioner did not , after all, apply to the facts of the case.

Recommendation #05-48

In the summer of 2004, there was a flurry of news articles with respect to the activities of the Liquor Licensing Board, which led to an investigation by the Conflict of Interest Commissioner. In the midst of this, a number of requests were received in this office from members of the press and members of the public body for access to various records of the public body. This particular request was from a member of the board, who requested copies of certain documents for a specific time period including "correspondence between" certain Board members. The Board responded to the request and provided all of the records they could gather. In their response to the Applicant, however, they indicated that they were unable to collect information from one or more of the individuals who sat as members of the board. They advised both my office and the applicant that, although they had requested records from all Board members, they had not received a response from one former member.

The issue in this case was whether members of independent

As a corollary to this, it is important that all Boards and other independent bodies created by the government who are subject to the Access to Information and Protection of Privacy Act develop policies for board members with respect to their handling of records which are created by the boards.

Elaine Keenan Bengts
Review Recommendation 05-048

board appointed by the government are subject to the Access to Information and Protection of Privacy Act. In this case, the Board itself is subject to the Act. Does that make the individual members of the Board subject to the Act? In this case, the member was no longer a board member when the request for information was made. Board members are not public servants. If individual board members take papers home with them or make notes while on a conference call with other board members while sitting at their kitchen table, are those records still "in the control" of the public body such that those records are subject to the access provisions of the Act?

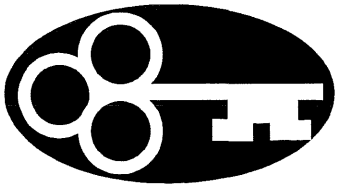
The Information and Privacy Commissioner found that at the time the Request for Information was made, the board member who did not respond to the Board's request no longer had any records in her possession. She was further satisfied that the Board disclosed all of the records "in its control" and thereby complied with their responsibilities under the Act.

The Commissioner recommended, however, that the Government of the Northwest Territories take steps to amend the *Access to Information and Protection of Privacy Act* so as to clarify the responsibilities of individuals appointed to independent Boards and other bodies which are, by regulation, subject to the Act and that policies be developed for all public boards with respect to the collection, use and disclosure of information.

The Commissioner's recommendations were accepted.

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,



Upon taking office, New York mayor Michael Bloomberg made it his mission to clean up city streets by filling potholes and eliminating other similar annoyances. Bloomberg's approach was based on the premise that safer and cleaner streets start with taking responsibility for the little issues.

So too with our personal privacy - we may not be able to eliminate identity theft or invasive surveillance overnight, but respecting consumer choice about the use of their personal information is surely a part of the solution.

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

VIII. RECOMMENDATIONS

Many of the recommendations which have been made in previous Annual Reports remain outstanding. My recommendations, therefore, will continue to seek that these matters be addressed.

A. In my last Annual Report I recommended that the Government of the Northwest Territories prepare and publish an updated "Access and Privacy Directory" as required by Section 70 of the Act and that it should be made available at no cost or a nominal fee to the public. I further suggested that the Directory be made available on-line with a link directly from the Legislative Assembly's web page. Since my last Annual Report, the Department of Justice has updated and published on its website an updated "Access and Privacy Directory" as required by section 70 of the Act. It does not appear, however, that the Directory has been published in paper form so that it is available to people who do not have internet access. Nor has the Directory been linked to the Legislative Assembly's web page. As it is right now, the Directory is difficult to find, even if one were to know that the information is available on the Department of Justice web page. I therefore recommend once again that the Directory be

   a) published in paper form and that copies be made available throughout the Northwest Territories and

   b) that a link to the directory be added to the Legislative Assembly's web page

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

B. The regulations naming the public bodies subject to the act should be reviewed annually to ensure that they remain up to date and reflect changes that are made in the way government does business. I recommended last year, for example, that the Legislative Assembly may wish to consider whether the new Human Rights Commission should be made subject to the Act. Changes have been made this year to Resources, Wildlife and Economic Development and, as I understand it, the NWT Business Credit Corporation and the NWT Development Corporation have also been amalgamated into one lending authority. Currently, under the regulations, the new entity is not subject to the Act. This is a problem because there are currently a number of review requests before me that concern these entities. The regulations need to be changed contemporaneously with restructuring efforts to ensure that the flow of information continues.

C. I would continue to encourage the Government of the Northwest Territories to do an inventory of all boards, tribunals and agencies to which it appoints members and to ensure that these organizations are both aware of and knowledgeable about the rules regarding access to information and the collection, use, disclosure and retention of personal information. In the best case scenario, all persons appointed to such bodies should be required to undertake basic ATIPP training. As a minimum, the leadership of such bodies (Executive Directors and Board chairs) should be required to receive basic training in the principals of access and privacy issues and be required to update that training periodically.

D. This year, problems have come to light about the role of individuals appointed to government boards and tribunals. This issue was directly before me in Recommendation 05-48 discussed above. The *Access to Information and Protection of Privacy Act* needs to be amended to clarify that individuals appointed to public bodies are personally subject to the Act by virtue of their membership in such bodies and that there are positive obligations placed on them with respect to the collection, use and disclosure of personal information. It also needs to be clarified that records in the hands of such agencies are subject to access to information requests and should be treated accordingly, including ensuring appropriate retention policies. Policies need to be developed for all such boards and agencies which direct what happens to records of an individual sitting on a board when that individual's term ends or they quit. These policies might, for example, include a requirement that 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.

E. Since my first Annual Report in 1998/1999, I have recommended that municipalities should be included as "public bodies" under the Act or that separate legislation be

There's no predictive modeling system available now to predict the activity of terrorists. In the days of suicide bombers and disposable terrorists, those aren't people like consumers who you can determine their credit worthiness."

Ann Cavoukian
Ontario Information and Privacy Commissioner

passed to govern access and privacy issues in the municipal sector. 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. Every jurisdiction in Canada, except for the Northwest Territories, Yukon, Nunavut, New Brunswick, and Prince Edward Island have legislation which addresses access and privacy at the municipal level. 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. I would once again encourage the Government of the Northwest Territories to take a close look at its contractual relationships with outside service providers and outsourcing, particularly in those sensitive areas which include the collection, retention and use of financial and/or medical information of individual residents of the Northwest Territories. I have previously recommended that there be clear provisions included in all contracts for such services to compel contractors to comply with the *Access to Information and Protection of Privacy Act* and making them subject to access requests and responsible for the privacy of individuals whose personal information they acquire as a result of the contractual relationship. My counterpart in British Columbia, David Loukidelis has recently completed a very detailed and extensive study of outsourcing in his

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.

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

Ann Cavoukian
Information and Privacy Commissioner for Ontario

province and, in particular, the effect of the anti-terror legislation in the United States on outsourced contracts. The question arose in that province as a result of a proposal to contract out certain health information management work. Questions were raised about the risk that personal health information of British Columbia residents might be vulnerable to disclosure to the FBI and US authorities under the Patriot Act. Mr. Loukidelis's report is available on-line at www.oipc.bc.ca. In the report, he recommends many of the same kinds of precautions as I have suggested such as:

⇒ imposing direct responsibility on contractors to ensure that personal information provided to the contractor by the public body, or collected or generated by the contractor on behalf of the public body, is used and disclosed only in accordance with the *Access to Information and Protection of Privacy Act.*

⇒ requiring contractors to notify the public body of any subpoena, warrant, order, demand, or request made by a foreign court of other foreign authority for the disclosure of personal information to which the *Access to Information and Protection of Privacy Act* applies.

⇒ requiring contractors to notify the public body of any unauthorized disclosure of personal information under *Access to Information and Protection of Privacy Act.*

⇒ giving the Information and Privacy Commissioner the powers necessary to fully and effectively investigate

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

Auditor General Sheila Fraser

The computerization of data and the possibility of carrying out full-text searches creates an unlimited number of ways of querying and sorting information, with Internet dissemination increasing the risk of collection for improper purposes. Furthermore, computerization has made it much easier to combine publicly available data from different sources, so that a profile of the situation or behaviour of individuals can be obtained...[P]articular attention should be paid to the fact that making personal data available to the public serves to fuel the new technologies of data warehousing and data mining. Using these technologies, data can be collected without any advance specification of the purpose and it is only at the stage of actual usage that the various purposes are defined. This is why it is important to check, on a case-by-case basis, what the negative repercussions on individuals might be, before taking any decision on computerized dissemination. In some cases, a decision will have to be taken on either not to release certain personal data, to let the data subject decide, or to impose other conditions.

The European Commission Working Party on the Protection of Individuals with Regard to the Processing of Personal Data

contractors' compliance with the *Access to Information and Protection of Privacy Act*

⇒ making it an offence under the *Access to Information and Protection of Privacy Act* for a contractor to use or disclose personal information in contravention of the Access to Information and Protection of Privacy Act, punishable by a significant fine, or a term of imprisonment, or both.

⇒ requiring all public bodies to ensure that they commit, for the duration of all relevant contracts, the financial and other resources necessary to actively and diligently monitor contract performance, punish any breaches, and detect and defend against actual or potential disclosure of personal information to a foreign court or other foreign authority.

⇒ requiring public bodies entering into outsourcing contracts to regularly monitor the contractor for compliance through regular compliance audits performed by a third party auditor.

I can do no better than to encourage the Government of the Northwest Territories to consider these recommendations in its own contracting process when dealing with private sector contractors.

G. Another one of my ongoing recommendations is that there be consideration given to creating "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. 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 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 identity theft. Although most parts of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to the private sector throughout Canada, it is legislation administered by the Privacy Commissioner in Ottawa. That office has limited effectiveness in dealing with the smaller, more localized issues as she concentrates on the larger issues of national import. It is to be noted as well that PIPEDA does not protect the privacy of employees in the private sector unless the employee is working in a federally regulated business such as banking, airlines, telecommunications or interprovincial transportation. Yet employers have records relating to some of their employee's most sensitive personal information including income, health and family relationships. It is important that this issue be addressed, particularly as more larger companies begin to set up business in the north.

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

Canadians expect much more from the institutions they entrust with their personal information. As Privacy Commissioner, I was disappointed that an apparently well-organized institution such as CIBC failed to recognize that the misdirected faxes were a privacy issue. That the bank's privacy policies and practices were not functioning on a practical level should serve as a wake-up call to all organizations in Canada,

Jennifer Stoddart
Privacy Commissioner for Canada

H. One of my ongoing concerns as Information and Privacy Commissioner has been the trend to allow "on-line" access to public registries. As noted in previous Annual Reports, public registries such as the Land Titles Registry, Companies Registry, and the Personal Property Security Registration System have historically been open to public inspection. These registries contain significant amounts of person information and create a valuable resource. When public registries are paper based and in fixed locations, although there is public access, the practical barriers prevent mass collection of data and the possibility of "data mining" so that a measure of privacy is maintained. As those registries become digitalized, however, access becomes much easier and the reality is that digital information is far easier to gather, manipulate and combine with other information. It becomes much easier to gather large amounts of personal information to create profiles of citizens for marketing purposes. Although there is nothing inherently wrong with such profiling, particularly for business purposes, the public does not anticipate that the information they provide to secure their ownership of land will be used to create a marketing tool for the sale of widgets. More troublesome is that this kind of data is like gold to identity thieves and those with less than legitimate business interests in the gathering of personal information. Before the Government of the Northwest Territories moves too far down the line of allowing access to these registries in digital form, questions need to be asked and answered. The Office of the Victoria Privacy Commissioner has

suggested that these questions should include:

- What is the purpose of a public registry?
- Should certain personal information be masked?
- Should individuals be asked at the time of registration whether they consent to use or their personal information for other purposes such as direct marketing of goods or services?
- Should bulk registry data be disclosed only for certain purposes or at all?
- Before a public registry is put 'online', have privacy enhancing measures been considered?

I would encourage the Government of the Northwest Territories to study and consider these important privacy issues before moving into more "on-line" and digital access to public registries.

I. As discussed in my opening remarks, I was quite taken aback when Resources, Wildlife and Economic Development (as they then were) took the position that the Business Credit Corporation was not a "prescribed corporation" under the Act and that section 24 (f) did not, therefore, apply. Section 24 (f) says that a public body must not disclose information where that information is a statement of financial assistance provided to a third party by a prescribed corporation or board. I read that section to mean any corporation or board subject to the *Access to Information and Protection of Privacy Act*. The public body felt that it required a specific designation as a "prescribed corporation or board". I strongly recommend that this section be amended to clarify what

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

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

Canadians expect much more from the institutions they entrust with their personal information. As Privacy Commissioner, I was disappointed that an apparently well-organized institution such as CIBC failed to recognize that the misdirected faxes were a privacy issue. That the bank's privacy policies and practices were not functioning on a practical level should serve as a wake-up call to all organizations in Canada.

No one denies the reality of the threat that the Act was intended to address, but we must ask ourselves whether what the Act gains us in security justifies the sacrifice of our privacy and other rights enshrined in our democracy

Jennifer Stoddart
Privacy Commissioner for Canada

is meant by the term "prescribed corporation or board" . Furthermore, in my opinion, the way in which this department dealt with the Request for Review and the recommendations made by the Information and Privacy Commissioner seriously undermined credibility of the process. The Act provides that, on review, the public body has the onus of establishing that an exemption applies. This, however, means little if, after receiving review recommendations based on the department's own submissions, that same department changes its mind about the applicable sections of the Act. If the process is to retain any credibility, the process must be respected. To that end, I recommend that the Act be amended so as to require public bodies to refer to all relevant sections of the Act when responding to the Information and Privacy Commissioner and to be bound by submissions made to the Commissioner insofar as any recommendations made are concerned.

J. As noted in my last Annual Report, the Government of the Northwest Territories is involved in a devolution process to give the aboriginal peoples of the Northwest Territories their own government. Recent news articles have led me to believe that there are serious issues within aboriginal organizations, particularly with respect to access to information. I would encourage this government to raise the issues of access to information and protection of privacy in devolution discussions and that aboriginal governments be encouraged to include some form of access and privacy regulation within their

government structures. The aboriginal peoples of the 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. 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.

J. One of my consistent themes in the last few years has been that there is a need to encourage a "corporate culture" consistent with the goals of the *Access to Information and Protection of Privacy Act.* I have often said that this culture must be embraced from the top in order to become engrained. I therefore encourage the Premier and each of the Ministers 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. A good example of this kind of leadership was shown by the Premier of Ontario last year when he issued a memorandum to all ministers and deputy ministers in his province calling upon them, "to strive to provide a more open and transparent government", emphasizing that the significance and the substance of that province's *Freedom of Information and Protection of Privacy Act*

At its root, I feel the best privacy protection is grounded in attitude — an attitude which should flow naturally from an appreciation of the nature of the relationship between government and members of the public. Governments exist at the pleasure of the governed — and privacy protection is an essential part of the relationship.

A Special Report to the Legislative Assembly of Ontario on the Disclosure of Personal Information at the Ministry of Health
February 20, 1997
Submitted by Tom Wright Information and Privacy Commissioner/Ontario

(FIPPA), could not be overstated. In the memorandum he directed that the government "should ensure that information requested of it should continue to be made public unless there is a clear and compelling reason not to do so." This memorandum was followed by a second joint memorandum from the Chair of the Management Board and the Attorney General which emphasized the importance of the Freedom of Information legislation in the democratic process . This joint memorandum encouraged a proactive approach for disseminating information to the public. Additionally, and perhaps most importantly from my perspective, the memorandum noted that although exemptions from disclosure will sometimes be necessary, discretionary exemptions should not be claimed solely on the basis that they are technically available; instead, they should be claimed only where there is a clear and compelling reason to do so. This last point is one that I would urge public bodies to embrace as one of the trends I have noticed is that where a discretion is provided in the Act, that discretion is inevitably used to refuse disclosure without any apparent thought being given to the possibility that access should be granted. There have been a number of instances in the last year where I could think of no "clear and compelling" reason to deny access to information which was subject to a discretionary exemption and yet access was denied. More than that, the only explanation often given for refusing disclosure in these circumstances appears to be "because we can". Unfortunately, the worst offender in this regard is, the Financial

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.

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

Management Board who, instead of showing leadership by allowing access except in the narrowest of circumstances, use every tool available to them, including discretionary exemptions, to deny access. My strongest recommendation, therefore, would be to encourage the Premier, the Ministers and the Financial Management Board to take the lead and take positive steps to foster a corporate culture of openness and accountability.

Respectfully submitted

Elaine Keenan Bengts
Northwest Territories
Information and Privacy Commissioner

Not only does the loss of control of information about one's self have some possible serious negative consequences, such as no protection from misuses of the information, it also means a loss of autonomy... Loss of autonomy means loss of one's capacity to control one's life... A right to control information about one's self is fundamental to being a self-determining and responsible being.

Deborah G. Johnson, Computer Ethics , (Englewood Cliffs, NJ: Prentice-Hall, 1985), p. 66,