INFORMATION AND PRIVACY COMMISSIONER OF THE NORTHWESTTERRITORIES

2005/2006 ANNUAL REPORT

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

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

December 29, 2006

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, 2005 to March 31st, 2006.

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

INDEX

Annual Report 2005/2006

INFORMATION AND PRIVACY COMMISSIONER

I. COMMISSIONER'S MESSAGE

"Privacy is the right to be alone - the most comprehensive of rights, and the right most valued by civilized man."

~Louis D. Brandeis

Introduction

As I head into my second full five year term as the Information and Privacy Commissioner of the Northwest Territories, I find that each year I learn to appreciate more and more the importance of the principals embodied in the *Access to Information and Protection of Privacy Act*. In 1997, in the case of *Dagg v. Canada (Minister of Finance)* [1997], 2 S.C.R. 403, Mr. Justice La Forest of the Supreme Court of Canada made what has proven to be the most enduring statement about the purpose of access to information legislation

> The overarching purpose of access to information legislation … is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process and secondly, that politicians and bureaucrats remain accountable to the citizenry ...

Parliament and the public cannot hope to call the government to account without an adequate knowledge of what is going on; nor can they hope to 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 …

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

"Smart enterprises know security and privacy are good for business, and yet many companies in Canada and around the world don't take this message to heart,"

~ Andy Canham, President, Sun Microsystems of Canada Inc.

Every year, every month, and every day new technologies expand our ability to collect, combine, store, manipulate, exchange and disseminate information. The use of these technologies undoubtedly promises efficiencies and positive change. It also, however, carries significant risk and there is a clear tendency to overlook the often negative impact that such technologies can have. The state of the world and its politics have accelerated the development and use of such technologies. New technological and digital products have been hailed as the

"What we really want to understand is why are people turning almost uncritically to cameras? There's an almost blind faith in the technological object, which is the camera, but- we have very clear evidence to show that they'll never be used for terrorist activity and sensational violent crimes. They're going to be used for good old-fashioned moral regulation."

~ Sean Hier
Professor, University of Victoria

best way to deal with the threat of terrorism and technological advances are held out as the panacea which governments say are **the** way to prevent terrorist acts. National governments in particular are discovering that the challenge of finding the balance between security and privacy rights is not a simple one. National governments continue to introduce new laws which expand the ability of governments to take extraordinary and invasive steps in the name of national security and to expand the use of information gathered. Justifications are being found to use information ostensibly gathered for the purpose of preventing terrorism (the extraordinary) for general law enforcement purposes (the ordinary) often without the checks and balances of warrants or judicial oversight. The Canadian government, for example, is expected to re-introduce a "lawful access" bill in the near future which will expand the ways in which governments and law enforcement agencies can collect information without warrant. Over the course of a very few years, it has become increasingly acceptable for governments to gather and use information in ways which would never have been considered appropriate only a few years ago. This is not unique to federal governments. Provincial and even municipal governments are actively beginning to encroach into this kind of legislation as well. British Columbia's Information and Privacy Commissioner has recently found it necessary to comment on this trend in a report released by his office on August 30th, entitled "Local Governments and the Growth of Surveillance" where he says:

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

~ David Loukidelis
British Columbia
Information and Privacy Commissioner

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

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

....this Office strongly believes that municipalities should not be in the business of passing surveillance bylaws. They clearly have privacy implications of varying degrees, depending on the nature of the personal information being collected, for ordinary members of the public who are going about their lawful business. Among other things, the bylaws we reviewed contain no measures to ensure that personal information is used properly and is protected against

unauthorized use or disclosure. Against the clear privacy impact of such bylaws, it is doubtful that such bylaws are really effective, and there are certainly tools that may more effectively achieve the community safety objectives that the bylaws purport to address. This Office is therefore firmly of the view that municipalities should not pass bylaws compelling citizens to give up their privacy in a wholesale and indiscriminate manner. Consistent with long-standing law and practice in Canada, it should be left to the courts to issue warrants or orders to businesses to turn over customer information on a case-by-case basis where justified.

In my annual report last year, I quoted from the 2004/2005 Annual Report of the Information and Privacy Commissioner of Alberta who asked us to remember and learn from the experience of history. His comments bear repeating:

- 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

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

~ Richard Thomas, UK Information Commissioner

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?"

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

~ Brian Beamish
Assistant Information and Privacy Commissioner, Ontario

Ombudsman Powers v. Order Powers

One of the features of access and privacy legislation which makes it so important in the democratic process is the independent oversight provided for in the office of the Information and Privacy Commissioner. In the Northwest Territories, the Information and Privacy Commissioner's role is that of an ombudsman. When a member of the public is unhappy with the public body's interpretation of the Act, there is recourse to the Information and Privacy Commissioner for an independent opinion given in the form of recommendations. One of the features of the ombudsman format is that the Commissioner's recommendations are not binding. As I noted in last year's annual report, the ombudsman format has both its strengths and its weaknesses. It's strength lies in the flexibility which the format allows, giving the Information and Privacy Commissioner the scope to make suggestions

knowing that governments have some room to work within those recommendations. This will often lead to more innovative resolutions to disputes. Recently, however, some of the weaknesses of the ombudsman system have started to show. Public bodies responding to inquires to my office often tend to be cursory and incomplete. Where, for example, a discretion is given to the public body as to whether or not to disclose a particular record, I am finding that there is a strong bent toward non-disclosure, apparently "because we can". There is rarely any indication that consideration has been given to the possibility of exercising the discretion in favour of disclosure. Instead, I am finding that more often than not, where a discretionary exemption applies, disclosure is likely to be denied without any apparent analysis being done. Although I tend to point this out in almost every recommendation that I make, there does not appear to be much progress on this issue. It is, apparently, simply easier to deny access than to actually weigh the pros and cons of disclosure and make a reasoned decision.

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

~ Harry S. Truman

I am also finding that public bodies spend very little time on their submissions to me on Access to Information Reviews. The submissions often provide very little background information or detailed argument. Although the onus in most instances is on the public body to establish that there is no right of access to a record, it is only rarely that a public body takes the time to provide detailed reasoning and/or precedent for their position when making

submissions in the review process. Perhaps if the Information and Privacy Commissioner had "order" powers such that there might be more serious consequences for not thoroughly canvassing the issues and providing detailed argument, more effort might be made to fully develop and present the arguments needed to support the position taken by the public bodies. As matters currently stand, however, there is little incentive for public bodies to work through that exercise and to consider, based on precedent and background, whether a particular exemption properly applies. As a consequence, the submissions received by my office on reviews are often very short, unsupported with background facts and not well thought out. Public bodies rarely provide thorough analysis and rarely come close to meeting the onus the Act places on them to establish that an exemption applies. Although the Act specifically provides that there is an onus on the public body to establish that exemptions apply, that onus is of little import when the department knows that in the end, the matter is going to be referred back to them (or at least their minister) for a final decision in any event. It may be that the time has come to consider changing the Information and Privacy Commissioner's role from that of an ombudsman to that of a decision maker.

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

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

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, in each

of my last three Annual Reports, said that this culture must be embraced from the top in order to become ingrained. So long as the Information and Privacy Commissioner's mandate is to give direction and make recommendations only, the purposes of the Act will only be met if there is a commitment on the part of the government as a whole and support from the highest levels of management to the concept of openness. Without this commitment from the top, the ombudsman role of the Information and Privacy Commissioner has limited impact. 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. As noted, the alternative may be to give the Information and Privacy Commissioner the ability to make orders instead of recommendations on access to information issues.

``I have spent 30 years seeing nothing but how people are harmed [in their] reputation or livelihoods when sensitive medical records are seen by anyone . . . outside of the few people you trust to actually take care of you. If privacy is not fully protected we won't be building anything except the most valuable mother lode of information for data mining on earth."

~Dr. Deborah Peel , Founder, Patient Privacy Rights Foundation, Austin, Texas

Electronic Health Records

Many projects which governments take on have implications for the personal privacy of the general public. Perhaps no single project, however, has more potential to affect the privacy of individual citizens than the national strategy to move toward electronic health records. I understand that the Northwest Territories is moving fairly quickly toward such an "on-line" system. It was of some concern to me that this significant project with huge privacy

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

Getting it right - at both design and operational levels - is vital to ensure the public trust and confidence which is needed to deliver the benefits of information sharing.

~ Richard Thomas, UK's Information Commissioner

2006 Annual Report

implications, was apparently well under way without any consultation with my office. Having heard of the project, I contacted the Department of Health and Social Services and expressed my concerns that privacy issues needed to be addressed at the outset of the planning of such systems. In response, the Department provided me with a copy of a privacy impact assessment done by a private contractor. Although it is heartening to hear that such an assessment has been done, and the department has agreed to meet with me to discuss the plan, I do have concerns that privacy issues may not be given the prominence appropriate in the planning and implementation of this project. As part of the mandate of the Information and Privacy Commissioner is to make comment on proposed projects and legislation insofar as they relate to privacy impacts, I would have hoped that those planning the project would have thought to involve this office from the very earliest states. Be that as it may, I intend to continue to monitor the e-health records project and to offer my comments where I can and where given the opportunity. To this end, I would again point out the need for legislation specific to the protection of privacy in the health sector. This is one of the prime concerns raised by the privacy impact assessment prepared for the Department of Health and Social Services. With the planning for e-health records in the Northwest Territories well underway, the absence of health specific legislation which would regulate the collection, use and disclosure of personal health Information becomes a more pressing

issue. The project, as I understand it, is being carried out under the auspices of the federal Advisory Council on Health Infostructure. In 1999, that Federal/Provincial / Territorial organization produced a report entitled "Paths to Better Health" which outlined a Pan-Canadian strategy for the establishment of a common system for electronic health records. In the council's interim report, the council recommended that "all governments in Canada should ensure that they have legislation to address privacy protection specifically aimed at protecting personal health information through explicit transparent mechanisms". In early 2005, all but two Canadian jurisdictions approved the "Pan-Canadian Health Information Privacy and Confidentiality Framework", designed to achieve consistency of privacy protection for electronic health records. Manitoba, Alberta, Ontario and Saskatchewan now have stand-alone health information laws and other jurisdictions are moving in the same direction. I have long recommended that the Northwest Territories needs health specific privacy legislation to address the unique issues that come into play when it comes to health records. In light of the fact that this project appears to be well along in the planning stages, it is critical that privacy issues be addressed.

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

~ Philip Johnston

Telegraph (UK),

September 18, 2006

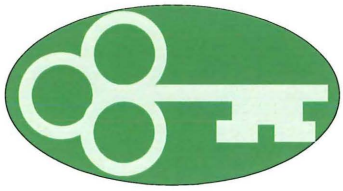
Conclusion

Democracy is under assault. The right of the public to access information about the way government does

business and the obligation of governments to protect the personal privacy of individuals are two very important cogs in the wheel of democracy. It behooves us to ensure that we pay close attention to these values and continue to remind ourselves on a daily basis how vital they are to our way of life. Because technology evolves so quickly, and the positive uses of new technologies seem so obvious, we sometime forget to consider the negatives. It is, however, important that we continue to be vigilant to ensure that we do not become a surveillance society and that governments remain accountable for their actions.

Citizens cannot participate meaningfully in the democratic process, and hold politicians and bureaucrats accountable, unless they have access to information held by the government, subject only to necessary exemptions that are limited and specific. Ultimately, taxpayers are responsible for footing the bill for any lawsuits that the City settles with litigants or loses in the courts. Consequently, taxpayers have a right to know, at a minimum, how many lawsuits or claims have been filed against the City, and how much money the City has paid out in damages or in settling such matters in specific years.

~ Order MO-1947
Office of the Ontario Privacy Commissioner



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

~ James Madison

II. AN OVERVIEW OF THE ACT

1. ACCESS TO INFORMATION

Background

Purposes of the Act

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

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

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

essential to the health of our democracy.

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

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.

~ Dr. Ann Cavoukian, Ontario Information and Privacy Commissioner

Address to Management Board Secretariat Access and Privacy Conference

2004

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

The Act also recognizes that government agencies hold considerable amounts of confidential personal information

about individuals which must be protected from improper use or disclosure.

The spirit of openness suggested by the Act is clear. However, it is not always easy to apply the law to individual records. Simple common sense is an important and valuable resource in the interpretation of the Act. There is often a fine balancing to be done in applying the Act and interpreting the provisions *vis a vis* specific records and whether or not the exemptions apply. Each request for information must be dealt with on its own terms.

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 applies and binds all Territorial Government ministries and a number of other governmental boards and agencies. All "records" in the possession or control of a public body are available to the public through an access to information request, unless the record is subject to a specific exemption from disclosure as provided for in the Act. The exceptions to the open disclosure rule function to protect individual privacy rights, allow elected representatives to research and develop policy and the government to run the "business" of government. The Act also gives individuals the right to see and make corrections to information about themselves in the possession of a government body.

Isn't it odd that when something big and bad happens, take your pick here, Sponsorship Scandal, Enron scandal, there are no records. The records are the first things to go, to the extent they existed in the first place.

But I will tell you this, based on my 11 years working in this area: no matter what you do wrong, no matter how goofy or misguided your actions, it is the cover-up that will do you in. Every time.

~ Frank Work
Alberta Information and Privacy Commissioner

Access and Privacy Conference 2006

Plenary Address

The regulations identify which government agencies (other than ministries) 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. Currently there are 12 ministries and 31 other agencies which fall under the Act. The list of public bodies subject to the Act is amended from time to time to include new agencies as they are created by the government to meet the needs of the people of the Territories.

Openness can improve bureaucratic decision-making by allowing criticism of poor or inadequate analysis. It can also temper extremist viewpoints by exposing them to public scrutiny.

~ Meredith Fuchs "Judging Secrets: The Role Courts Should Play in Preventing Unnecessary Secrecy."

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 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 that there also be a written version of the Directory.

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. The only requirement is that the request be in writing, which would include an e-mail request. An e-mail request may require, in addition, written correspondence signed by the Applicant, depending on the requirements of the public body. Requests are submitted, along with the $25.00 fee, to the appropriate public body. There is no fee if an individual is requesting his or her own personal information.

Once a request for information is received, the public body has a duty to identify all of the records which are responsive to the request and 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 are discretionary. The discretionary exemptions require the public body to consider whether or not to disclose the information, keeping in mind the general philosophy of disclosure.

E-mail, though widely considered to be ephemeral because it can be written so spontaneously and vanishes magically from the computer screen at the click of a mouse, can be quite permanent-and also far more widely distributed than intended.

~ John Shovic

Professor of Cyber Security, Eastern Washington University

Public Bodies must exercise their discretion in favour of disclosure unless there is good reason not to disclose, keeping in mind the purpose of the Act.

Every person has the right to ask for information about themselves. 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.

If a government is seen to act on the basis of evidence and sound advice, those actions will be seen to be more legitimate than actions which are not explained or justified. This is especially so in countries, like ours, where the public is well-educated, informed, empowered and used to being able to find out what is going on. As soon as we cannot find out what is going on, we get suspicious.

~ Frank Work
Alberta Information and Privacy Commissioner

Access and Privacy Conference 2006

Plenary Address

The Role of the Information and Privacy Commissioner

The legislation provides for an independent review officer who plays an ombudsman like role, known as the Information and Privacy Commissioner. The Commissioner's job is to provide an independent review of decisions made by Public Bodies under 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 ability to provide an impartial review of the government's compliance with the Act. Under the Act, a Commissioner is appointed for a five (5) year term. The current Information and Privacy Commissioner was reappointed for a five year term in June, 2005 and will serve until June, 2010.

The erosion of liberty. Four words sum up four years. Since the attacks of September 11 2001, we have seen an erosion of liberty in most established democracies.....In the always difficult trade-off between liberty and security, we are erring too much on the side of security. Worse still: we are becoming less safe as a result.

~ Timothy Garton Ash
Thursday November 17, 2005
The Guardian

The *Access to Information and Protection of Privacy Act* gives the Information and Privacy Commissioner the powers of an ombudsman which means that she has the obligation to provide recommendations to public bodies but no power to make orders or require the public body to act on the recommendations made. The Commissioner 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 ministry, the "head" is the minister. For other public bodies, the "head" is determined in accordance with the regulations. Public bodies must consider the recommendations made, but have no obligations to accept the 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 by the Information and Privacy Commissioner, reject them, or take some other steps he or she feels is advisable based

on the information in the recommendation. The decision must be in writing and must be provided to both the person who requested the review and to the Information and Privacy Commissioner.

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. To date the Commissioner is aware of one decision made on appeal to the court from the decision of the head of a public body after recommendations of the Information and Privacy Commissioner.

> The thing that really should worry people is that once the capability is there, people will abuse it. The opportunity for abuse is so much greater, because so much more of our private information is transmitted over the network.
>
> ~ Jennifer Granick
> Executive Director of Stanford University's Center for Internet and Society.

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.

2. 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:

1. No personal information is to be collected unless authorized by statute or consented to by the individual
2. Personal information should, where possible, be collected from the individual, and not from third party sources
3. Where information is collected from third parties, the person who is the subject of the information should be informed of that fact and be given the opportunity to review it
4. Where personal information is collected, the agency collecting it must advise the individual exactly the uses for which the information is being collected and will be utilized and that if the public body wishes to use it for another purpose, the consent of the individual will be obtained first.
5. The personal information collected must be kept safe and secure and the public body must ensure that it is available only to those who require the information to provide the service or conduct the business for which the information was collected.
6. Personal information collected by a government agency must be used only for the purpose it is collected; and

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

~ George Orwell
"1984"

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

We shouldn't be so quick to assume that the only thing the watchers care about is criminal acts. Once the government gathers information about you (for example, what you read, who your friends are, what organizations you join), it then has the capacity to use that information in ways that have nothing to do with terrorists.

~ Geoffrey R. Stone

Harry Kalven Jr. Distinguished Professor of Law at the University of Chicago

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. 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.

3. 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 receive a copy of the responsive documents from the public body involved and will review the records in dispute. In some cases, it may be necessary for the Information and Privacy Commissioner to attend the government office to physically examine the public body's 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

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

~ Jerry Kang, Professor of Law , UCLA

Nothing is more corrosive to the social fabric of a city than unwarranted police surveillance. This is what all veterans of bloody battles for democracy and justice in countries around the world throughout history tell us, and our own most observant commentators, from George Orwell to Robert Fisk and John Pilger, repeat it: the encroachment of the police state marches in lock-step with the shrinkage of the democratic and just state. It is our well-founded fear of the potential use of this information as a tool of corruption and abuse of power-and the equally frightful potential for mistakes made with that information-that brings on the chill we feel at the mere mention of unwarranted police surveillance and monitoring in any of its forms, no matter how little we have to hide.

~ Kevin Potvin

The Republic (East Vancouver, BC), May 25, 2006

process. All of the parties involved, including the public body, are given the opportunity to make written submissions on the issues.

In the 2005/2006 fiscal year, the Information and Privacy Commissioner's Office received thirteen (13) new requests for review, of which ten (10) of which are related to each other in that they all arose out of one request for information. In addition, this office received one privacy complaint and one request for comment.

Review recommendations were issued with respect to the privacy complaint. One Request for Review was withdrawn before recommendations were made and one file was resolved through mediation prior to the making of recommendations. Eleven requests for review remained active as at the end of the fiscal year.

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

Business Development and Investment Corp.	10
Education Culture and Employment	1
Transportation	1
Public Works and Services	1

In total four recommendations were issued by the Information and Privacy Commissioner's Office in fiscal 2005/2006.

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

~ Terri Dowty,

Director of Action for the Rights of Children

III. REVIEW RECOMMENDATIONS

We must stand on guard against state access to the data-banks of the corporate world. Fears of terrorist attacks or impending pandemics provide superficially attractive justifications for intrusive powers, but the real need for these powers is often not apparent.

~ Jennifer Stoddart

Privacy Commissioner of Canada

Review Recommendations #04-48

This was an application by an individual who had formerly been employed by a public body but had had a falling out with his employer and was in the process of preparing for certain hearings in relation to his dismissal. The request for information was directed to the Financial Management Board.

The Applicant had two general complaints and a number of more specific ones with respect to the response he had received from the public body. The two general complaints were:

1. He felt the response he had received was "significantly incomplete".
2. He felt the that the Information and Privacy Commissioner should have been involved in the initital request process

In addition, the Applicant was concerned that one document was "coverless, unsigned, undated" and "plain" so that "authenticity cannot be established". He also complained that the record was "an amalgam of legislative breaches, corruption, lies, misrepresentations and flawed recommendations" that could not have been produced in a

vacuum, yet no research notes, correspondence, e-mails etc. were provided to document sources, opinions or circulation. He felt that all supporting records should have been provided.

Leadership on openness and transparency must come from the top. Public servants are more apt to disclose information without claiming inapplicable exemptions if they feel that their decisions will be supported by both the politicians and senior executives who lead their ministry, agency, board, commission or local government."

~Dr. Ann Cavoukian

Ontario Information and Privacy Commissioner Annual Report 2005

With respect to the first complaint, the Information and Privacy Commissioner, after reviewing all of the responsive documents, concluded that in most cases, the public body had not appropriately applied the correct provisions of the *Access to Information and Protection of Privacy Act*. In particular, the public body had relied heavily on section 13(1) of the Act which provides that records must not be disclosed if those records would reveal the confidence of the Executive Council or the Financial Management Board. The Information and Privacy Commissioner found, however, that the public body had not satisfied her that the records in question qualified as "cabinet confidences". She did, however, suggest that section 14 might apply to the records instead. Section 14 provides that a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to reveal consultations or deliberations involving officers or employees of a public body. Unlike section 13, section 14 requires the public body to exercise a discretion in deciding whether or not to disclose the information. Because the public body had not considered section 14, they had not exercised that discretion. The Commissioner recommended in each case that the public body review the record and exercise their

discretion, and provide the applicant with an indication of the considerations which went into the exercise of that discretion in those instances in which they chose not to disclose the document.

There were also records for which the public body had relied on section 15 of the Act, which gives public bodies the discretion to refuse to disclose records subject to solicitor/client privilege. The Information and Privacy Commissioner acknowledged that those records were covered by solicitor/client privilege but noted that there was no indication that the public body had actively exercised its discretion. She recommended that they do so and provide the Applicant with an explanation as to the reasons for the manner in which they had exercised their discretion.

The recommendations were, for the most part, accepted, but the public body still failed to provide the Applicant with any real explanation as to the reasons for the manner in which they chose to exercise their discretion in those cases in which they chose to refuse disclosure.

Review Recommendation #05-051

This Request for Review had a fairly long history. The Applicant was a former employee of the Department of

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

~ Richard Thomas

UK Information Commissioner

2006 Annual Report

Renewable Resources and Economic Development. He had made a request of the Department to provide him with, in essence, a copy of every record on which his name had appeared over a period of approximately seven years. Efforts were made to encourage the Applicant to revise or refine his request so as to narrow the scope of the request. When the Applicant refused to do so, the public body provided the Applicant with a cost estimate of a minimum of $2500.00, as it is entitled to do under the Act and Regulations. The Applicant requested the Minister to waive or reduce the fee applicable pursuant to section 50 (2) of the Act. The Minister considered the request and declined to reduce the fee. The Applicant then requested this office to review that decision.

After reviewing the provisions in the Act with respect to the application of fees to Requests for Information, the Information and Privacy Commissioner indicated that she did not feel that the department had followed the correct procedure in providing the fee estimate and recommended that a more thorough calculation be done. She also, however, concluded that the head of the public body had, in this case, thoroughly considered the discretion granted to him to waive or reduce the fees and that there was nothing further, therefore, that need be done in terms of that issue.

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

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

Review Recommendation #05-052

In this case, an application had been made for certain information in the possession of the Labour Standards Board. Two affected third parties had been given notice that infomation concerning them was going to be disclosed and both third parties objected to that disclosure and requested this office to review the decision to disclose. The Third Parties were two of several former officers or directors of a non-profit organization which had received significant public monies to conduct a specified program. The organization ceased operations at some point, although no winding-up process had taken place. An employee or employees of the organization filed a complaint with the Labour Standards Board about allegedly unpaid wages and the Board conducted an investigation and made a finding. Because the organization itself was no longer in operation, the Board determined that the individual former officers and/or directors were responsible for the payment of the debt found to exist. The Applicant had requested information relating to this decision of the Board.

The Information and Privacy Commissioner reviewed the records in question and concluded that many of the

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

~ Dr. Ann Cavoukian, Ontario Information and Privacy Commissioner

Order (MO-1947)

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

~ Frank Work

Alberta Information and Privacy Commissioner

records were already in the public domain and therefore their disclosure would not be an unreasonable invasion of any person's privacy. With respect to the remaining records, she identified a number of items which, if disclosed, would constititue an unreasonable invasion of the third party's privacy and recommended that these portions of the records be severed before being disclosed.

The Information and Privacy Commissioner's recommendations were accepted.

Review Recommendation #06-053

This recommendation arose as a result of a request from an individual who felt that her privacy rights had been infringed by the Department of Education, Culture and Employment when they relied on information received from a third party to deny her student financial assistance without providing her with the opportunity to refute or even see the information upon which the decision was based. She says the information upon which the decision was based is untrue.

The Information and Privacy Commissioner pointed out that she had no jurisdiction to deal with the issue of whether or not the complainant's former employer had breached her privacy rights, as the employer was a private

sector organization and beyond the jurisdiction of her office.

With respect to the allegations that the public body improperly disclosed the complainant's personal information, the public body pointed out that they had policies in place within the workplace which indicate quite clearly that no personal information about a client can be disclosed to others without the written consent of the individual in question. The Information and Privacy Commissioner acknowledged the policies as a good starting point but emphasized that policies, in and of themselves. were not going to be sufficient to guarantee that information will be properly handled. The human element is not always reliable. The public body, she indicated, has an obligation to take steps to ensure that the policy is adhered to, and to monitor its employees in the exercise of their duties. This duty would also include ongoing training and reminders about the importance of confidentiality.

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

~Dr. Ann Cavoukian, Ontario Information and Privacy Commissioner

The Information and Privacy Commissioner found, however, that the public body did not comply with the spirit of the Act in its refusal to be completely forthcoming with the Complainant about the information it received from a third party, and in its refusal to provide her with a copy of the information received or advising her of the source of the information upon which certain decisions affecting her

student financial assistance were based. She suggested that although there may be instances in which it is important to protect the identity of a source of information, there is nothing in this situation which suggested that that was necessary in this case. It did not appear that theComplainant was in a position of power *vis a vis* the third party such that there may be repercussions for that person or agency for "whistle blowing". Nor was there any suggestion that the third party provided the information in confidence. Furthermore, in this case, the alleged third party was not an individual, but a corporate entity. Corporate entities do not have the same rights to privacy as individuals. Opinions stated belong to the person about whom the opinion relates. Where the opinion is expressed by an individual in his or her own capacity, there may be an argument that the author's name is his personal information and should not be disclosed. But where the opinion is expressed in the name of a corporate entity, as appears to have been the case here, there is no such protection. It was recommended that ECE provide the Complainant with a copy of all information received by it in connection with her application for SFA, whether that information was received as a result of inquiries made or from an unsolicited source.

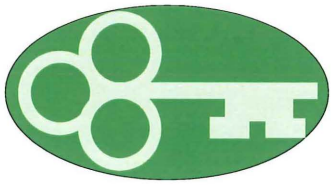
If children learn to live with constant surveillance, random drug testing and sniffer dogs in schools, what kind of citizens will they become?

Two dangerous trends collide in the debate about children's privacy.

On the one hand, we are not respecting the rights of our children generally, and on the other, we're complacent about the importance of privacy in a free society.

~ Shami Chakrabarti

Director, Centre for the Study of Human Rights, London



Ten years ago, they wouldn't have compiled such a database because they didn't have the technological tools to use it once they did compile it. Now, computers can plow through the equivalent of a national library in short order and pluck out critical information, using pattern recognition, keywords and other so-called data-mining techniques. The resulting portrait says a lot about who a person is: It can describe one's tastes, interests and appetites - things a person might not want others to know.

~ Marc Rotenberg

Executive Director, Electronic Privacy information Center, Washington

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. Boards and Tribunals

As noted in my Annual Report last year, problems have come to light about the role of individuals appointed to government boards and tribunals. When individuals are appointed by the government as members of boards or commissions, they do not always become employees of the government and, therefore, are not subject to the same policies which apply to employees. They keep their own records and their own filing systems, outside of the government record management system. They also often deal with the kind of business which should require accountability to the public and with personal information of individuals which should have the protection afforded by the *Access to Information and Protection of Privacy Act*. I recommend that the Act be amended to clarify that individuals appointed to public bodies but who are not employees are, nontheless, subject to the Act by virtue of their appointment by a government agent. This would create for appointees the same obligations which the rest of the bureaucracy has with respect to the collection, use

and disclosure of personal information. It would also clarify that records in the hands of such agencies and appointees and the papers they create as members of such boards and agencies are subject to access to information requests. It is further recommended that steps be taken to create policies for all boards and agencies to establish the necessary protocols for proper handling of records produced by them. These would include policies for proper security of records, and appropriate retention and destruction rules as well as policies which direct what happens to records of an individual sitting on a board his or her term ends or they quit. I have received no indication, as of yet, that legislative amendments are being considered or that any policies have beed developed to deal with these issues.

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

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

B. Municipalities

Since my first Annual Report in 1998/1999, I have maintained that municipalities should be subject to access and privacy legislation. Not only is it important that municipal authorities be accountable to the public through access to information rules, it is also important that municipalities, particularly tax based municipalities, should have rules regarding how they gather, use and disclose personal information about individuals. Municipalities gather and maintain significant information about individuals in their day to day dealing with the business of

[P]rivacy matters because in a self-governing society we must vigilantly reinforce the sense of independence of the individual. For a self-governing society to function, the citizen must feel that he is the governor, not the subject. Perhaps it is difficult to feel like the governor when your government monitors your every move. Perhaps limiting government surveillance is essential to democracy itself. Certainly, life in the former Soviet Union, with its pervasive government surveillance, illustrates how such monitoring can crush the life out of a society. If we do that to ourselves, perhaps we will be worse than the terrorists

~Geoffrey R. Stone, Professor of Law at the University of Chicago

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. This year I was consulted by the City of Yellowknife who are actively considering by-laws to deal with access and privacy matters and my impression was that all of the elected respesentatives at the meeting considered access and privacy guidelines or rules to be of significant importance and were supportive of such policies being established. It would, in my opinion, be far more effective to have the same legislation apply to all municipalities than to have each municipality create its own set of rules. I would again encourage the legislative assembly to consider either an amendment to the *Access to Information and Protection of Privacy Act* to include municipalities as "public bodies" or to create separate legislation which deals with access and privacy matters at the municipal level so as to provide consistent access and privacy rules which will apply to all municipalities within the Northwest Territories.

C. Contracting Out of Information Management

In the last eighteen months, an issue which has become significant in many jurisdictions in Canada is the contracting out of what have traditionally been government activities. In many jurisdictions, for instance, motor

vehicle registries have been privatized. I would once again encourage the Government of the Northwest Territories to take a close look at its contractual relationships with outside service providers and its outsourcing contracts, 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. This has become a major concern for many of my provincial counterparts. This is a particularly sensitive issue when it relates to health information management work.

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

~ Richard Thomas, UK Information Commissioner

D. Openness of Contract Details

Many of the requests for review which I receive involve questions about how the government has been spending public funds. The public wants to know what contractors are being paid for government work. As has been pointed out by Dr. Anne Cavoukian, the Ontario Information and Privacy Commissioner in her most recent annual report:

Trust and confidence are key. Put simply, mishandling personal information will lead to an erosion of confidence and businesses and government will suffer. Information is a valuable asset and poor data quality or controls can cost millions. The cost of getting it wrong is not just financial.

~ Richard Thomas

Information Commissioner UK

The right of citizens to access government-held information is essential in order to hold elected and appointed officials accountable to the people they serve. This is particularly true for details of government expenditures and the right of the public to scrutinize how tax money is being spent. When government organizations use individuals or companies in the private sector to help develop, produce or provide government programs or services, the public should not lose its right to access this information. Any government office planning on hiring a consultant, contractor, etc., should make it clear to that future agent that the *default position* is that the financial and all other pertinent information related to the contract will be made available to the public, except in rare cases where there are very unusual reasons not to do so.

I would echo these comments and encourage public bodies to make it clear that private companies contracting with the government should do so knowing that the accountability of government may well require that details of the contract will be shared with the public unless either the goverment or the company can provide cogent evidence that the disclosure of those details would be reasonably expected to harm the financial interests of either the government or the business.

E. Private Sector Privacy Legislation

As Privacy Commissioner I am faced with the challenge of regulating a value which is essentially dynamic. It is likely that someone who grew up in a world without the internet has a different idea of privacy to someone who has grown up communicating with friends via MySpace. Different people have different privacy expectations and those expectations are strongly influenced by the rise of new technologies.

~ Karen Curtis

Privacy Commissioner, Australia

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

F. First Nations Governance

As I have said in previous Annual Reports, I believe that it is important that, to the extent that the Government of the Northwest Territories is involved in the process of devolution and transferring governmental responsibilities to the aboriginal peoples of the Northwest Territories to include provisions with respect to access and privacy. It is clear from my observations that there are accountability issues within aboriginal governments just as there are in every other form of governance. Access and privacy legislation provides for the checks and balances necessary to help address these issues. 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 to the credibility of 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.

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

~ Murrary Mollard, Executive Director of the B.C. Civil Liberties Association.

G. Adequate Resources

This year it has come to my attention that at least one government department, the Department of Education, Culture and Employment, may require more resources to respond to the volume of requests they have received pursuant to the *Access to Information and Protection of Privacy Act*.. That department has apparently received a large number of requests for personal information in a fairly short period of time, arising largely as a result of the residential school issue. As a consequence of the volume of requests, the department has found itself completely unable to respond in a timely fashion to access to information requests they receive. In one instance, an applicant waited almost three months for a response to his request for information and, once I became involved, it took nearly six additional months to respond to my request for copies of the responsive records and the department's submission on why the response was not received earlier. The explanation given was that there had been an inordinate number of applications for information and that the ATIPP Co-Ordinator was unable to keep up with the demand, and maintain her other workload as well. I would urge all public bodies to ensure that adequate numbers of personnel are dedicated to compliance with the Act. In some instances, that might mean the creation of a position in the department solely for the purpose of addressing ATIPP requests. Another alternative might be to establish

Companies must take the protection of personally identifiable information seriously because customers see privacy and security as a matter of trust.

~ Marjorie Shield, Director of the Privacy Office, BMO Financial Group (March 22, 2005)

a central ATIPP office to oversee all access requests, regardless of which department the request originates in.

H. Legislative Gap - Motor Vehicle Records

It has recently come to my attention that there may be a problem with access to information regarding motor vehicles. The issue arose when the Department of Transportation received an application from the legal representative of a person who had been involved in a motor vehicle accident. The other vehicle involved in the accident was licensed in the Northwest Territories and driven by an NWT driver who, as it turned out, was not insured. It also appeared that the address which had been on the the driver's licence was inaccurate. The request was to obtain updated address information for the driver. The Department of Transporation took the position that the *Access to Information and Protection of Privacy Act* prohibited the public body from disclosing the personal information of a third party because that would be an unreasonable invasion of the third pary's privacy. Although the *Motor Vehicles Act* provides for the disclosure of information to a lawyer acting in a matter relating directly to the ownership of a motor vehicle, there is no such provision which would allow the disclosure of information about a driver of a vehicle if they are not the owner. Other jurisdictions do have provisions which allow for the disclosure of personal information about drivers as

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

well as about vehicle and their owners and this does seem to be an oversight. It would seem to be a reasonable expectation that when we are given the privilege of being allowed to drive,we should be accountable to a third party if we injure them in a motor vehicle accident. It seems equally reasonable that a person injured in a motor vehicle accident should have access to contact information about the driver of the other vehicle, as well as about the owner of the other vehicle. I would suggest that this be reviewed and that necessary amendments be made to the *Motor Vehicles Act* to allow for the disclosure of this kind of information in appropriate circumstances.

Democracy dies behind closed doors."

~ Circuit Court Judge
Damon Keith
August 2000

Respectfully submitted

Elaine Keenan Bengts
Northwest Territories
Information and Privacy Commissioner