2007-2008

ANNUAL REPORT

Northwest Territories Information And Privacy Commissioner

Elaine Keenan Bengts
Information and Privacy Commissioner

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

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

December 1, 2008

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

Attention: Honourable Paul Delorey
Speaker 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, 2007 to March 31st, 2008.

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

COMMISSIONER'S MESSAGE

The summer of 2008 found the world watching China as it hosted one of the most impressive Olympics ever held. A light shone on a country which is a mystery to many of us. Although the country put on quite a show for the world, we were also shown a glimpse behind the veneer and we saw some of the more disturbing aspects of Chinese life. It became clear that China is a country in which it is dangerous to voice dissent or to question government in any way. Some of the stories coming out of Beijing were particularly poignant in highlighting for me the value of a system of government which is accountable to its electorate. In the days leading up to the opening ceremonies and throughout the Olympics themselves, there were news reports highlighting some of the negative impacts of a non-democratic society. We saw, in narrow focus, what can happen when governments are not accountable. From the sometimes brutal repression of people's ability to challenge or even question government policy, to invasive and ubiquitous monitoring and surveillance programs established by the Chinese government, we were reminded in a rather stark way of how different our way of life might be without the protections that we have in our system of government. It re-enforced for me the importance of legislation such as the *Access to Information and Protection of Privacy Act,* particularly in today's technological world.

The Culture of Openness

Over the years, I have voiced a consistent message in my Annual Reports. That message is that there must be leadership from the top on access and privacy matters. I was concerned, therefore, when the name of the Committee which oversees the *Access to Information and Protection of Privacy Act* was changed from "Oversight and Accountability" to "Priorities and Planning". I sincerely hope that this change of name does not signal a step away from accountability in favour of other government priorities. I would repeat my ongoing refrain that every elected official and every senior manager of every public body should be knowledgeable

> As Canadians, we must always question why our personal information is being collected, whether by a government agency implementing a security program, or by a store employee compiling marketing data.
>
> Jennifer Stoddart, Privacy Commissioner of Canada

about the Act, its intents and purposes, and the general principals which underlie it. Perhaps more important than being knowledgeable about the Act, though, is the need for a strong and vocal commitment to its purposes and the maintenance of a corporate culture of accountable government. This includes encouraging routine disclosure and discouraging the use of the discretionary exemptions available under the Act to deny disclosure. It also includes ensuring that there are sufficient knowledgeable staff at a high enough level of management to deal with access requests quickly, efficiently and effectively at the first instance. Every new initiative must include a privacy impact assessment to ensure that the program does not unnecessarily impact on personal privacy.

> The right to be left alone is the beginning of all freedom.
>
> William O. Douglas
> U.S. Supreme Court Justice

Protection of Privacy Needs More Attention

Although most public bodies are familiar with the "Access to Information" sections of the *Access to Information and Protection of Privacy Act* and can deal with access matters fairly efficiently at this point, I am somewhat more concerned about the attention being given to ensuring that personal information is protected and properly managed. It is very easy in the course of the day to day work of government to forget that the information being dealt with is sometimes sensitive personal information that requires special care and respect. More and more of the matters I am being asked to review are complaints about the improper use or disclosure of personal information.

2007 brought a record number of high profile cases across Canada and, indeed, around the world involving serious data breaches, many as a result of carelessness and lack of understanding about the importance of proper security policies and procedures for the protection of data, be it in electronic or paper format. In the last few months both Saskatchewan and Alberta have experienced the discovery of sensitive medical records in dumpsters and abandoned buildings, leaving thousands of people vulnerable not only to identity theft, but to the threat of the exposure

of their medical histories. While there have been no formal complaints made to this office as of yet with respect to a "bulk" loss of personal information data, the potential for such a breach is very real. I have heard anecdotally of at least one incident of medical records being found in the dump in a small, remote northern community. I would, in fact, be surprised in the Government of the Northwest Territories had not experienced the loss or theft of computers, lap tops, PDAs, or jump drives containing third party personal information whether in the form of names, addresses, telephone numbers and e-mail addresses or more significant details. The fact that there have been no reported consequences following from the loss of such devices is most likely more a matter of good luck than good management .

Quite apart from the statutory duty imposed on public bodies to protect personal information, a single high profile case can be devastating financially and result in a loss of public confidence. It has been estimated that for private industry, the average cost of a serious data leak is $1.8 million in direct and indirect costs. The cost to government would be no less and would come with a loss of confidence in the ability of government to manage.

Human error will always be a factor when managing personal information, but there are steps that can be taken to minimize that factor and thereby reduce the possibility of data breaches. Vimal Vaidya, CEO at RedCannon Security, an IT security company that focuses on mobile devices, suggests six steps to minimizing the possibility that human error will result in the loss of sensitive personal information from mobile devices:

- There should be strong policies in place to define the acceptable uses of lap tops and PDAs and the kinds of information that can be stored on them

> We need to make sure that somebody carries the can for failings in this area, and from that taking responsibility and changing the culture will follow, Personal information isn't sufficiently valued by organizations. The price of this is people losing trust in public services. Trust relies on respecting people's personal information, and data protection is about more than security, it's about informing people how their information is used and about minimizing the amount.
>
> David Smith, United Kingdom Deputy Information Commissioner

- Employees should be educated frequently and reminded of the rules of use
- There should be a centralized management of mobile devices, including USB devices
- All data on mobile devices should be encrypted

cept perhaps in health services, where there are long standing and well established policies and practices in place for the protection of personal information, many government agencies are more focused on "getting the job done" than on the privacy implications of what they do. More should be done in all public bodies to educate all employees on the importance of privacy and the security of personal information and the message should be consistent and repeated frequently.

In Canada there are 2,000 healthcare transactions every minute. In one year there are:

- 440 million laboratory tests
- 382 million prescriptions
- 322 million office-based physician visits
- 35 million diagnostic images
- 2.8 million in-patient hospitalizations

Canada Health Infoway Web Site

- Steps should be taken to maintain control over USB ports
- There should be secure remote access to all electronic devices

But privacy breaches don't happen only as a result of lost or stolen mobile devices. At a more basic level is the fact that often, when dealing with the day to day business of government, employees simply do not put their minds to the security and protection of personal information. Ex-

Electronic Health and Medical Records

One of the major challenges facing the Northwest Territories and, in fact every Canadian jurisdiction, is the protection of privacy in the health sector. This year, the Department of Health and Social Services invited me to observe the development of a system of Electronic Medical Records for the Northwest Territories. It is widely accepted that electronic records will, when fully operational, result in a

more efficient, effective and safer medical system. It is also acknowledged, however, that it is critically important that such electronic records are built, from the ground, so as to satisfy the public that their records will remain confidential and that there are sufficient safeguards built into the system to prevent inappropriate or accidental disclosures of their personal health information. I am encouraged that the Department is focusing on the privacy and security aspect of this technology at it's inception rather than trying to fit it into the technology at a later date.

jurisdictions, all of which, with the exception of Nunavut, now have health specific privacy legislation or are very close to tabling such legislation.

Another health related project I have been involved in this year is the Pan Canadian Forum on Electronic Health Records (EHR) Information Governance, sponsored by Canada Health Infoway. The Privacy Forum is intended to provide those responsible for health policy in each Canadian jurisdiction and the

> Another important theme emerging from the past year is the apparent lack of awareness on the part of many public bodies and organizations of the weaknesses in their technical and administrative information security. This is bad for privacy. It is also bad news for the security of corporate or government information assets.
>
> David Loukidelis, Information and Privacy Commissioner of B.C.
> 2007/2008 Annual Report

This year also saw the start of a project which I have been recommending for many years, and that is a plan to implement health specific privacy legislation. The Department is now actively working toward such legislation and to that end has put together a discussion paper and two panels who have each met several times to discuss the issues and give feedback on the things that might be included in such legislation. This is an encouraging development and will bring the Northwest Territories in line with other Canadian

privacy oversight bodies, such as my office, with the opportunity to meet in a setting in which they can share knowledge and experiences and can leverage their collective wisdom to facilitate the development of common solutions to common problems related to the information governance issues of the interoperable Electronic Health Record (EHR). Although there are many aspects to the EHR, health information privacy is definitely one of the most significant issues that my office is

involved in and, without a doubt, one of the most complex. Every jurisdiction in Canada is dealing with these issues now, and the area promises to become far more complex before a workable, national system can be implemented. The technical aspects of electronic health and medical records are beyond my expertise, although I am working hard to maintain a working understanding of the issues. It may be, however, that it is time to consider the possibility that the Office of the Information and Privacy Commissioner may have to engage the services of others with more specific and in depth knowledge of the issues to help to ensure that this office can keep up with the developments in the area. Because the Northwest Territories relies so heavily on the services of other jurisdictions to provide many of our health services, this project is doubly important for us. The long term dream is to have an interoperable system of health records so that when a resident of the Northwest Territories travels to Edmonton or Calgary, or any other place in Canada, for medical attention, the doctors in that other jurisdiction can access the individual's medical record. Although it sounds simple enough as a concept, I am learning quickly about how extremely difficult it will be in practice to implement the ideal. That being said, it is the way of the future and it is important that our government participate fully in these discussions, particularly because we are in a position of being able to mold both our system and our legislation in such a way as to avoid some of the bigger pitfalls and other roadblocks that other jurisdictions have already hit. As the rest of the country moves toward the new electronic systems, the Northwest Territories is going to have to keep pace.

> In particular, I wish to be a strong advocate for the duty of all federal institutions to help in any way they can the individuals and organizations who request information from them to get that information.
>
> Robert Marleau
> Information and Privacy Commissioner for Canada
> Annual Report 2007/2008

Commissioners' Meetings

This year the Information and Privacy Commissioners issued two joint resolutions during their semi–annual meetings. The first, made in July, 2007 called on the Government of Canada to reconsider and revise the Passen-

ger Protect Program (Canada's "no-fly" list) so as to ensure full public debate on the issues raised by the program and, in particular, the need for a formalized review mechanism so that those who think their names are on the list can challenge the inclusion. The resolution also called on the International Civilian Aviation Organization and the International Air Transport Association to defend and advance privacy principles, transparency and strong privacy protections in the establishment of any standards, rules or common practices governing the screening of travelers using watch lists or other passenger assessment programs.

The second joint resolution was issued in February, 2008 and addressed the concerns raised by Canada's Privacy Commissioners and Ombudsmen surrounding the development of Enhanced Drivers Licenses (EDL's) as a substitute identification document for the passport for travel between Canada and the United States. EDL's are being developed in a number of jurisdictions to meet the requirements of American authorities for identification documentation and contain Radio Frequency Identification Devices (RFID's) which contain electronic information about the holder. The Commissioners called on the Government of Canada and participating provinces and territories to ensure that no EDL project proceeds on a permanent basis unless the personal information of participating drivers remains in Canada. The resolution further called on the federal and provincial/territorial governments to ensure that the personal information stored on or in the EDL can be accessed only by the Customs and Border Protection and can be used only for the purpose of determining whether an individual is eligible for admission to the United States.

> ...society has come to realize that privacy is at the heart of liberty in a modern state….Grounded in a man's physical and moral autonomy, privacy is essential for the well being of the individual
>
> R. v. Dyment [1988] 2 S.C.R. 417 at 427-428, 55 D.L.R. (4th) 503 at 513

I was also privileged this year to be able to attend the 29th International Conference of Data Protection and Privacy Commissioners

held in Montreal in September, 2007 as an accredited member of that organization and to hear some of the world's foremost authorities on privacy issues address some of the most pressing privacy issues of our day. This conference, held annually, brings together 78 data protection authorities and privacy commissioners from every continent as well as an international audience from non-governmental organizations.

The public sessions for the Montreal meeting included speakers such as Mr. Simon Davies, the President of Privacy International (UK), Dr. Michael Geist, Canadian Research Chair in Internet and E-Commerce Law, University of Ottawa, and Dr. Bradley A. Malin, Assistant Professor, Department of Biomedical Infomatics, Vanderbilt University (USA) on issues ranging from children's on-line privacy to nanotechnology. In a closed session, the representatives of the accredited authorities had the opportunity to exchange information and adopt resolutions in fields which pose common challenges. There were two significant resolutions passed at the 2007 conference — a resolution on the urgent need for global standards for safeguarding passenger data to be used by governments for law enforcement and border security purposes and a Declaration of Civil Society Organizations on the Role of Data Protection and Privacy Commissioners.

> People expect, and are entitled to expect, that the government will not share their confidential or personal information without their consent.
>
> Cheskes v. Ontario (Attorney General)
> 2007 CanLII 38387 (Ont. Sup. Ct)
> Justice Edward Belobaba

Priorities for the Next Year

I have two priorities for the coming year. One is to bring some prominence to the Right to Know Week, which takes place during the last week of September. The second is to focus some attention on children's on-line privacy and the role that the internet plays in the lives of our children.

The purpose of Right to Know Week is to raise citizen awareness about the public's right to access information under the control of government institutions. 2008 marks the

third year that Canadians have celebrated Right to Know Week, and a number of events were planned all across Canada. Internationally, Right to Know Day began in Sofia, Bulgaria at an international meeting of access to information advocates who proposed that a day be dedicated to the promotion of freedom of information worldwide. Right To Know Day is now celebrated annually by over 60 different countries on September 28th. For the coming year, I will be sponsoring an essay competition for all high school students in the Northwest Territories and will be drawing on the resources of my colleagues from other parts of the country to raise the profile of the access to information provisions of the Act.

The second issue I would like to spend some time addressing in the next year is how to help our children learn more about how to protect themselves on the internet. In an article entitled "Virtual Playgrounds and BuddyBots: A Data-minefield for Tweens" by Valerie Steeves and Ian Kerr which was published in the Canadian Journal of Law and Technology in 2005, they say:

> The online world of tweens - kids between the ages of nine and 14 - is fun, interactive, and cool. It is also a place that is structured by seamless surveillance and the aggressive collection of children's personal information. Whether kids are hanging out with Hilary Duff on Barbie.com, playing with Lifesaver products on Candystand, or chatting with ELLEgirlBuddy about their favorite celebrities, a marketer is listening - and sometimes talking - to them, to measure their likes, dislikes, aspirations, desires, wishes, and propensity to purchase product.

Over the course of the last year, I have begun

In Canada, Right to Know Week is celebrated to promote the right to information as a fundamental human right and to campaign for citizen participation in open, democratic government. This national event offers an opportunity for anyone interested in promoting freedom of information as a fundamental right to engage in an informed dialogue with Canadians of all ages.

Robert Marleau
Information Commissioner for Canada

to learn much more about the dynamic between our children, the internet, and the significant role that it plays in their lives. Canada is one of the most "wired" countries in the world, with almost 90% of households having at least one computer with internet access. Our children are leaving their parents far behind in their understanding and abilities to access the on-line world. Who is teaching these children about how to protect themselves on the internet— from predators and from identity theft? Who is teaching them about why it is important to protect their personal information? Recent studies suggest that while most children have a basic understanding of the most obvious dangers of giving out their personal information on line, there are huge gaps in their appreciation of the serious consequences that might result from giving away too much personal information. Because the internet is so much a part of youth culture, it is important that they have an understanding of the ways that they can be affected. I am, therefore working on some projects to assist teachers and parents to help Northwest Territories children to be more aware of the how they use the internet and what kind of information they share.

> The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding.
>
> Justice Louis Brandeis, United States Supreme Court

THE ROLE AND MANDATE OF THE INFORMATION AND PRIVACY COMMISSIONER

The Northwest Territories' *Access to Information and Protection of Privacy Act* (ATIPPA) came into effect on December 31st, 1996. It binds all Territorial Government departments and agencies. It establishes the rules about how Territorial government agencies collect, use and disclose personal information and about how the public can gain access to government records. Under the Act, the office of the Information and Privacy Commissioner (IPC) is created. The IPC is an officer of the Legislature and is appointed by the Commissioner of the Northwest Territories on the recommendation of the Legislative Assembly. She reports to the Legislative Assembly of the Northwest Territories through the Priorities and Planning Committee. The IPC is an independent officer who can be only be removed from office "for cause or incapacity" on the recommendation of the Legislative Assembly.

The term "access to information" refers to the right of the public to have access to general records relating to the activities of government, ranging from administration and operations to legislation and policy. It is an important aspect of open and accountable government. Under the *Access to Information and Protection of Privacy Act*, the public is given the right to have access to all "records" in the possession or control of a public body 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

> Gaining access to information, participating in discussions and debates and thereby enjoying the guaranteed purpose under the freedom of information and protection of privacy legislation – this is just the first step towards ensuring real equality for all Nova Scotians and to achieve the goal of participatory democracy.
>
> Dulcie McCallum,
> Nova Scotia Access to Information Review Officer

rights, allow elected representatives to research and develop policy and the government to run the "business" of government.

The Supreme Court of Canada has clearly stated that exemptions to disclosure provided for in access to information legislation should be narrowly interpreted so as to allow the greatest possible access to government records.

The Act also gives individuals the right to see and make corrections to information about themselves in the possession of a government body.

tablished by the government. The Information and Privacy Commissioner has several roles under the Act, including:

- independently reviewing the decisions and practices of government organizations concerning access and privacy and providing recommendations to public bodies with respect to those is sues
- providing comment and advice on proposed government legislation and programs;

There is no magic solution to the shortcomings of the system. A healthy access to information system needs:

- All its parts functioning well in order to deliver the outcomes intended by parliament
- The right systems to process requests
- Skilled staff
- Supportive managers and Ministers
- Adequate resources
- Good information management
- Good understanding of the principles and the rules by all, including third parties
- And effective approaches to oversight.

2002 Delagrave Report

Privacy protection is the other part of the legislative equation, and refers to the safeguarding of personal information held by government.

ATIPPA applies to all government departments and most agencies, boards and commissions es-

- educating the public about the Act

When dealing with access to information issues, the Information and Privacy Commissioner has very limited power to make binding orders with respect to matters which come

before her. Rather, in most cases her role is similar to that of an Ombudsman. Recommendations are made to the head of the public body involved who must then make a final decision as to how the government will deal with the matter. If, in the end, the person seeking the information is still not satisfied with the response received, there is recourse to the Supreme Court of the Northwest Territories for a final determination of the matter.

> Overall, the theme of the breaches last year was employee error. We have repeatedly reminded organizations and public bodies that ongoing employee training is a critical tool in preventing privacy breaches
>
> David Loukidelis
> 2007 Annual Report

MAKING AN ACCESS TO INFORMATION REQUEST

Requests for information must be made in writing and delivered to the public body from whom the information is sought. 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. This would include a request made by e-mail but where a request is made by e-mail, it may not be considered complete until the public body receives confirmation of the request with the applicant's signature. Requests for information are subject to a $25.00 application fee except in cases where the information requested is the applicant's own personal information. In such cases, there is no application fee, although there may be a fee for copying records in certain circumstances.

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

Every person has the right to ask for information about themselves. If an individual finds information on a government record which they feel is misleading or incorrect, a request in writing may be made to correct the error.

Even if the public body does not agree to change the information, a notation must be made on the file that the individual has requested a correction.

> The most common cause of disputes, in the information and privacy world as in any other dealings between ordinary citizens and organizations, is communication breakdowns that have little to do with legal rights or obligations.
>
> David Loukidelis
> Information and Privacy Commissioner of BC

PROTECTION OF PRIVACY

Part II of the *Access to Information and Protection of Privacy Act* sets out the rules about how public bodies can collect personal information, how they can use it once it has been collected and how and when they can disclose it to others. The Act also requires public bodies to ensure that they maintain adequate security measures to ensure that the personal information which they collect cannot be accessed by unauthorized personnel. This Part of the Act also provides the mechanism for individu-

als to be able to ask the government to make corrections to their own personal information when they believe that an error has been made.

A recent amendment to the *Access to Information and Protection of Privacy Act* gives the Information and Privacy Commissioner authorization to review privacy complaints where members of the public are concerned that their personal information has been improperly collected, used or disclosed by a public body. Once recommendations are made, the public body has ninety days to respond to the recommendations. There is, however, no appeal available to the court unless the individual seeks to have a charge laid pursuant to section 59 of the Act.

> In an age characterized by revolutionary IT developments and exponential information creation, storage, transmission and use, the case for robust and credible information management has never been greater
>
> Ann Cavoukian
> 2007 Annual Report

REQUESTS FOR REVIEW

Under section 28 of the *Access to Information and Protection of Privacy Act*, a person who has requested information from a public body, or a third party who may be affected by the disclosure of information by a public body, may apply to the Information and Privacy Commissioner for a review of the public body's 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 by public bodies under the Act.

A Request for Review must be made in writing to the Information and Privacy Commissioner's Office within 30 days of receiving a decision from a public body under the Act. There is no fee for making a Request for Review.

When the Information and Privacy Commissioner receives a Request for Review, she will take steps to determine what records are involved and obtain an explanation from the public body. In most cases, the Commissioner will receive a copy of the responsive

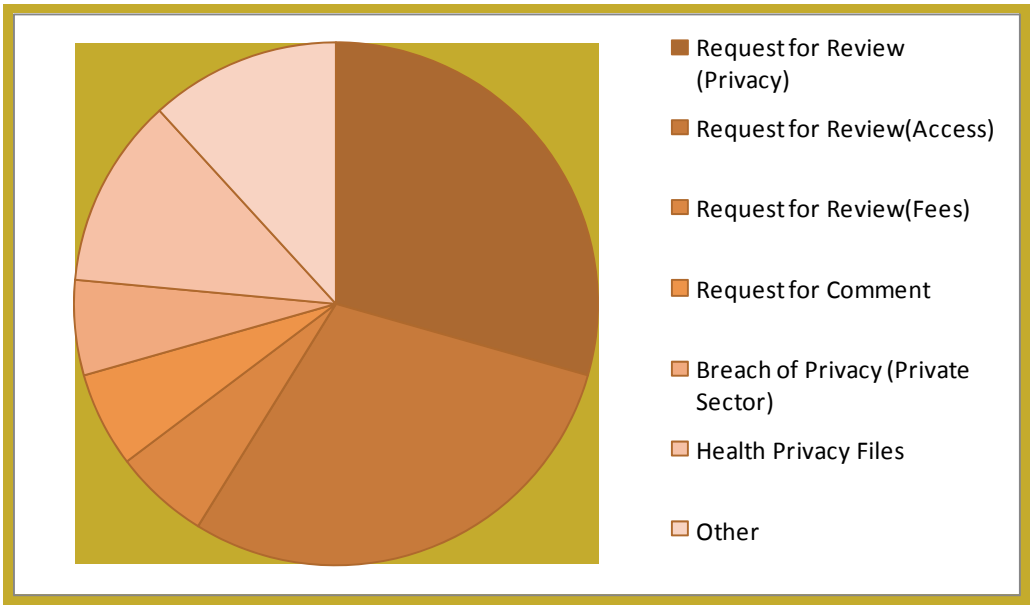
documents from the public body involved and will review the records in dispute. In some cases, it may be necessary for the Information and Privacy Commissioner to attend the government office to physically examine the public body's files.

Generally, an attempt will first be made by the Commissioner's Office to mediate a solution satisfactory to all of the parties. In several cases, this has been sufficient to satisfy the parties. If, however, a mediated resolution does not appear to be possible, the matter moves into a more in depth review.

All of the parties involved, including the public body and any third parties whose information may be disclosed, are given the opportunity to make written submissions on the issues.

In the 2006/2007 fiscal year, the Information and Privacy Commissioner's Office opened seventeen files in a number of different categories as follows:

Request for Review (Privacy)	5
Request for Review (Access)	5
Request for Review (Fees)	1
Request for Comment	1
Breach of Privacy (Private Sector)	1
Health Privacy Developments	2
Other	2



Six of the Requests for Review resolved themselves without a complete review of the issues. Of these

- two were resolved through mediation (both breach of privacy complaints)
- one arose from a situation involving a private sector business and the Applicant was referred to the Privacy Commissioner of Canada after being provided with some basic information.
- one Request for Review of an Access to Information issue was abandoned when the Applicant failed to respond to the Commissioner's request for further information.
- in one case, the Request for Review of an Access issue was premature and the matter was referred back to the public body for processing.
- In one case, the Request for Review (Access) was received in my office approximately 35 days after the response to the initial request had been received by the Applicant (the time period provided for in the Act to ask for a review is 30 days) and this office, therefore, had no jurisdiction to deal with the request unless the public body agreed to participate and they refused to do so.

The Requests for Review received involved six Public Bodies:

- NWT Housing Corporation 2
- Human Resources 2
- Workers' Compensation Board 2
- Hay River Health and Social Services Authority 1
- Dehcho Health and Social Services Authority 1
- Yellowknife Health and Social Services Authority 1

We investigated 96 privacy breaches last year. The majority were caused by thefts of computers or vehicles that contained personal information in the form of computers or hard copy files. One public body alone had ten breaches, all involving the same program area and the same risk – workers taking records out of the office and leaving them in a car that was stolen or broken into.

Another large category of breaches involves employee error or misconduct.

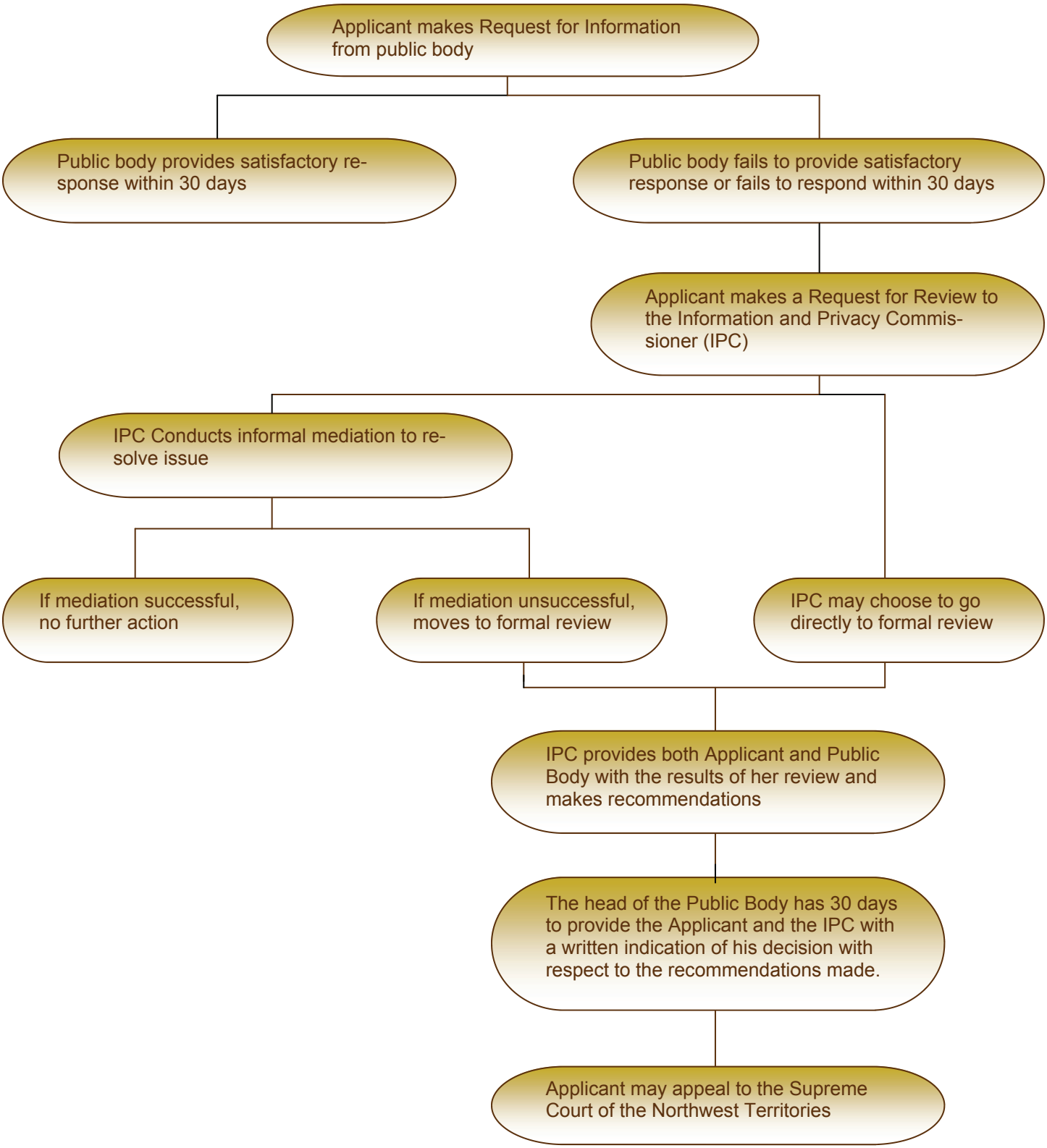
David Loukidelis
2007 Annual Report

One request was received by the Information and Privacy Commissioner to comment on a government initiative that involved privacy considerations. That matter involved the use and disclosure of the personal information of employees to a third party for the purpose of issuing credit cards. In addition, the Information and Privacy Commissioner asked the Department of Human Resources to provide her with an explanation as to certain issues which came to her attention with respect to the security of the government's "PeopleSoft" system, which is used by the Department for employee record keeping.

Seven Review Recommendations were issued by the Information and Privacy Commissioner's office during the fiscal year.

> This case shows how important it is for institutions to keep on top of the proliferation of communications technology and to ensure that employees understand that communications with devices such as BlackBerrys produce records, just like documents, e-mails and voice mails, and that employees have a responsibility to manage them properly.....
>
> However, there is no uniform federal policy on PIN to PIN communication and institutions have been advised to each craft their own policy.
>
> Through our investigation, it became apparent to us that the goals of consistency and simplicity favour a single government policy
>
> Robert Marleau
> Information Commissioner for Canada
> Annual Report 2007-2008

MAKING AN ACCESS TO INFORMATION REQUEST



REVIEW RECOMMENDATIONS MADE

Review Recommendation 07-061

In this case, the IPC received a request from a member of the media to review the response he had received to a request for a certain report related to an Oil and Gas Impact Assessment which had been prepared for the Department of Education, Culture and Employment. The Department refused access to the entire record, relying on section 16(1)(a) of the Act, which gives public bodies the discretion to refuse disclosure of information if the disclosure could reasonably be expected to impair relations between the Government of the Northwest Territories and another government, in this case the Acho Dene Koe Chief and Council. They also relied on section 16(1)(c) which provides that a public body may refuse disclosure of a record where the disclosure would be likely to reveal information received from such an organization, either explicitly or implicitly in confidence.

The Information and Privacy Commissioner found that the public body did not provide enough background information about the history of the report or how it came to be in their possession to be able to rely on section 16(1)(c). She was, however, satisfied that the public body had properly applied section 16(1)(a) in that they had consulted with the First Nation organization involved and were convinced by their input that the disclosure of the records would clearly be over the objections of the First Nation and that could reasonably be expected to impair the Government's relationship with that organization, and perhaps others with whom they must work on an ongoing basis. The Information and Privacy Commissioner found, therefore, that the public body fully exercised their discretion and she recommended that no further action be taken.

> Considering that the onus is on the public body to establish that there is no right to disclosure, the absence of background information is critical. They cannot tell me, for instance, why they have a copy of the report. They tell me that they had nothing to do with the preparation of the report so they therefore assume that it was 'received" by them though they don't know from whom, when or why they received it.
>
> Review Recommendation 07-061

The IPC's recommendation was accepted.

Review Recommendation 07- 063

The issue in this case was whether or not the Worker's Compensation Board (WCB) had improperly used or disclosed the Complainant's personal information. He had received a report from the WCB's Review Committee Registrar in connection with his claim for compensation benefits. The same report had been provided to his employer and he was upset because it contained sensitive medical information which he did not intend to be shared with his employer and which he felt had nothing to do with the claim being made. He was concerned that he had not consented to the disclosure of this information to his employer. He was also upset that he had not been told that his medical history would be used in this fashion.

The IPC concluded that both the employer and the employee have a legitimate interest in the outcome of decisions made by the WCB. Furthermore, the decision process contemplated by the Workers' Compensation Act is quasi judicial in nature, which means that the rules of natural justice require that all parties be privy to the details of the case in which they are participating. As such, if the employer chooses to participate in the claim process (which they are entitled to do under the Act), they will have access to the personal information of the employee involved. She left the question open as to whether or not an employer who chose not to participate in the claim process would have a similar right to the information. She also suggested that the WCB should consider how much personal medical information is truly necessary for inclusion in reports issued by its Committees in order to allow both parties to assess whether an appeal is appropriate, knowing that these reports will be shared with the employer and, potentially, therefore, with others. The IPC concluded that it is important that these reports contain only that information absolutely

> By its very nature, the Workers' Compensation Board collects a staggering amount of personal information about individuals.....Despite this, it does not appear that the organization has taken the step of outlining in any detail the scope of what might be collected in the course of a claim investigation or how, specifically, that information might be used. It seems to me that in light of the very sensitive nature of medical records.....it is not unreasonable to expect them to be more specific and up front about how that information might be used and to whom it might be disclosed
>
> Review Recommendation 07-063

necessary to the decision being made and that steps should be taken to protect or mask reference to the worker's medical information where possible. She made three specific recommendations to assist the WCB to improve the way in which the reports are written. She also made recommendations to improve the claim forms which workers complete when making a claim to ensure that there is a clear understanding on the part of the worker that his/her personal information may be shared with the employer. This would include a listing of the possible ways in which the Claimant's personal information may be collected, used and disclosed in accordance with the Workers' Compensation Act during the course of the claim process.

At the time of the writing of this report, the public body had yet to respond to the recommendations made.

riod of time. The public body initially refused to disclose the information requested and that refusal was referred to the IPC's office for review. On review, the IPC had recommended that the information be disclosed, but suggested that the Act required that the third parties involved be advised of the intention to disclose the information and that they be given the opportunity to object to the disclosure as provided for in the Act. When the consultation was undertaken, seventeen third parties objected to the disclosure of the information in question and this review was undertaken.

The IPC heard from nine of the seventeen third parties, and in each case the concerns raised were that the corporate entities involved did not want their corporate financial information disclosed to an unknown party

> It seems to me that it would be contrary to the spirit and intention of the Act for the government to be able to hide how it spends its money simply by establishing societies to administer its programs and then hiding spending behind the wall created by the establishment of a "third party"
>
> Review Recommendation 08-065

Review Recommendation 07-064

This review arose when a member of the press asked for a list of the companies which had received loans from the Northwest Territories Business Development Corporation over a stated pe-

and felt that the information they had provided to the NWTBDC was provided in confidence.

On review, the IPC felt that the disclosure of the names of companies who received funding did not constitute a disclosure of a statement of financial assistance given to the com-

panies (which are protected from disclosure pursuant to section 24(1)(f) of the Act). The Applicant was not asking for any details about the loans or when the loans were made or any other background information about the loans. He was seeking only the names of the companies who had received loans, nothing more. In the circumstances, she recommended that the names of the companies be disclosed.

The recommendation of the Information and Privacy Commissioner was accepted.

disclosure of all responsive records.

At the time of the request, the Treatment Centre and the union were in contract negotiations. The Applicant was a member of the bargaining unit for the union. The Treatment Centre was on contract to the Health Authority and under the terms of that contract, the Health Authority was paying the legal costs of the labour negotiations. They claimed solicitor/client privilege over the information sought with respect to legal costs and argued that

> If there is a reasonable possibility that the assiduous inquirer, aware of background information available to the public, could use the information requested concerning the amount of fees paid to deduce or otherwise acquire communications protected by the privilege, then the information is protected by the solicitor/client privilege and cannot be disclosed. If the requester satisfies the IPC that no such reasonable possibility exists, information as to the amount of fees paid is properly characterized as neutral and disclosable without impinging on the client/solicitor privilege
>
> Ontario (Attorney General) v. Ontario (Assistant Information and Privacy Commissioner), [2005] O.J. No. 941 (Ont. CA)

Recommendation 08-065

In this case, the Applicant had asked for information regarding the legal costs associated with certain labour negotiations between the Nats'ejee Ke Treatment Centre (the Treatment Centre) and the PSAC, a union which represents government employees. The applicant was also asking for the salary of the current CEO of the Treatment Centre. The public body, which in this case was the Deh Cho Health and Social Services Authority (the Health Authority), refused

the disclosure of the CEO's salary would be a breach of her personal privacy. The Treatment Centre also objected to the disclosure of the information requested, as did the CEO.

The Applicant argued that the Treatment Centre was an agent of the government and not a third party and that the information being sought with respect to that entity was for the amount spent on the negotiations only and that that, in and of itself, did not constitute information that was subject to solicitor/

client privilege. They also argued that the information requested with respect to the salary of the CEO was not the CEO's personal information but information about a position in the employer's organization.

The IPC found that the disclosure of the CEO's salary was prohibited as a presumed invasion of the CEO's personal privacy pursuant to section 23 of the Act.

represented by the same union which represents GNWT employees. She was not convinced that the Treatment Centre should be considered a "third party" as that term was defined in the ATIPP Act.

She also noted that, regardless of whether the Treatment Centre was a third party, the Health Authority clearly had possession and control of the information in question and that

> Thus statements of fact are not themselves privileged. It is the communication of those facts between a client and a lawyer that is privileged ….
> Thus, the jurisprudence in this area is not really in conflict. It merely reflects the existence of broad exception to the scope of the privilege, namely that it is only communications which are protected. The acts of counsel or mere statements of fact are not protected
>
> *Stevens v. Canada (Privy Council)* (1998) 161 DLR (4th) 85 (F.C.A.)

With respect to the disclosure of the cost of legal services attributable to the negotiations in question, the IPC questioned whether the Treatment Centre was governed by the ATIPP Act. She concluded that, although the Treatment Centre was a registered society, it was fully funded by the Health Authority and the Health Authority had financial control of the organization, although its day to day operations was administered by a separate board. That board, however, appeared to be appointed the Health Authority or the Department of Health and Social Services. The unionized workers of the Treatment Centre were

information was, therefore, subject to an access request.

She also pointed out that, although the labour negotiations were ongoing at the time the Request for Information had been made, by the time the response was provided, the labour dispute had been resolved and there was no longer any possibility that the information requested could in any way influence the negotiation process.

Finally, the IPC relied on precedent from the

Ontario Information and Privacy Commissioner, the Ontario Court of Appeal and the Federal Court of Appeal to conclude that the disclosure of a number representing the amount spent on legal fees was not information that was protected by reason of solicitor client privilege because the disclosure of the number alone could not reasonably be expected to reveal to anyone the nature of the solicitor/client communications concerning the legal issue in question.

The IPC recommended that the Health Authority should disclose the amount spent on legal fees with respect to the negotiations.

The recommendation was accepted.

YHSSA filed an affidavit with the court in which they relied heavily on information obtained from a file they had with respect to the Complainant on an unrelated matter. The affidavit also referred to a report addressed to YHSSA from a therapist who the Complainant had been seeing. The Complainant was very upset that that specific information was used in a manner that was certainly not contemplated either by her at the time of the therapy sessions.

The Special Information and Privacy Commissioner appointed to deal with this file found that most of the information about the Complainant which YHSSA used in the affidavit had been properly collected by the YHSSA in accordance with the relevant legislation. The question really whether the information was improperly disclosed when it was included in an affidavit on an issue entirely separate and distinct from the issue for which it was originally collected. In reviewing the legislation, the IPC pointed out that the *Child and Family Services Act* of the Northwest Territories, pro-

> In my opinion, the way the Act is structured suggests that the Applicant should be entitled to review all of the responsive materials before having to make a decision whether or not to request a review.
>
> Review Recommendation 08-067

Recommendation 08-066

In this case, the Complainant felt that her personal information was used and disclosed inappropriately by Yellowknife Health and Social Services Authority (YHSSA). The Complainant was seeking to have a child, who was an extended family member, placed in her home while the child's mother dealt with some issues. In court documents filed in response to that application,

vides that, notwithstanding the ATIPP Act, a social worker may disclose information when giving evidence in court. With one exception, therefore, the use and disclosure of the information on the Complainant's unrelated file was not improper. The exception was in the use of the therapist's notes. The IPC found that the therapist was contracted to the public body and, to that extent, was by definition an "employee" of the public body and subject to the Act. He further found that YHSSA did not have a contractual basis for the disclosure of the information about the Complainant from the therapist to YHSSA and that disclosure was, therefore, wrongful. However, once the information was in the possession of the YHSSA, the *Child and Family Services Act* allows it to be used as evidence in court.

The IPC recommended that the YHSSA review its practices respecting contracting for services to ensure that they comply with the *Access to Information and Protection of Privacy Act*. If YHSSA contracts with non-governmental agencies for the provision of services, YHSSA has responsibility for that person's collection, use and disclosure of the personal information collected by them and must ensure compliance with the Act. The recommendation provided that any contract between YHSSA and a contractor should specify the nature of the work to be done, what information is to be collected, what uses may be made of it and who it can be disclosed to. If the contractor is to report to someone, what and to whom should be specified.

The public body did not respond to the recommendations made, as required by section 49.6 of the *Access to Information and Protection of Privacy 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])

Recommendation 08-067

In this review, the Applicant had requested certain information and been advised that 532 pages had been identified as being responsive. The Applicant had been given access to all but 9 pages and he sought a review of the refusal to disclose those nine pages. The public body in this case felt that the Request for Review had been submitted after the 30 days allowed for such a request and that the IPC had no jurisdiction to undertake the review.

On the first issue, in this case the Applicant had requested that she be given access to the records in electronic form. As a result, the records in question were scanned and put on a CD. The public body sent the Applicant a letter listing all of the records which had been identified as responsive to his application, including a notation indicating whether or not the record was being disclosed. The scanned records were not sent by e-mail, but the CD was sent to the Applicant by mail. He received the CD several days later. The Request for Review was received more than 30 days after the date of the e-mail correspondence to the Applicant but within 30 days of his receipt of the CD in the mail.

> Although the Act provides that the public body must provide a copy of requested records to an Applicant, the Act does not require that copy to be provided in the form requested by the Applicant. The public body in this case went above and beyond what they were strictly required to do and acceded to the Applicant's request that the records be provided electronically. This was despite the fact that it required more effort than simply providing a paper copy and it is a credit to them and in accordance with section 7(1) which requires a public body to make every reasonable effort to assist an applicant
>
> Review Recommendation 08-068

The IPC came to the conclusion that the process was structured so as to provide an applicant with a reasonable period of time (30 days) to review records received in response to a Request for Information in order to evaluate whether they agree with the exceptions applied to the response and to determine whether the response is complete. That can only be done once the Applicant is in receipt of the actual records. The time limit for requesting a review, therefore, should be 30 days from the date that the actual records are delivered to the Applicant, not simply a list of the records being disclosed.

With respect to the pages which were not disclosed to the Applicant, the public body was relying on section 14 of the ATIPP Act, which gives public bodies the discretion to refuse access to records where that disclosure could reasonably be expected to reveal "advice and recommendations" given in the internal decision making process between the Minister and his Deputy.

The IPC reviewed the records in question and agreed with the public body that there were some parts of the records in question that constituted advice given and received in the decision making process. She also pointed out, however, that those bits were only a very small portion of the whole record and that those parts could be easily severed and the remaining part of the record provided to the Applicant. The IPC recommended that the records be disclosed, subject to the redaction of certain parts of the records identified as being "advice or recommendations".

The Commissioner's recommendations were accepted.

Recommendation 08-068

This review involved the Applicant's objection to a fee assessment issued pursuant to the Act. The fee estimate provided to him was approximately $75.00 for the copying of records. The Applicant, however, had asked to have the records provided to him electronically. The public body had also indicated that that fee could be reduced to $58.00 if the Applicant were willing to forego receiving records which were, in essence, copies of other records.

The Applicant challenged the fee for "copying" on the basis that he should not be charged for hard copies when he had specifically requested the response be given electronically.

The IPC reviewed the fee structure outlined in the Act and the Regulations. She noted that in order to properly comply with the Act, public bodies must review each responsive record and that in many cases there are some

> 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

parts of the record that are subject to either mandatory or discretionary exemptions. In such cases, the Act requires that the public body sever the exempted portions of the record and then provide the Applicant with the balance of the record. That cannot be done electronically. The public body must make at least one copy of the record for review and editing.

In this case, the IPC observed that the public body had no obligation to provide the response electronically and that in doing so it actually took more time and more effort than simply providing the paper record. The IPC was of the opinion that the fee estimate was reasonable and within the limits provided for in the Act and recommended that the fee estimate stand.

The recommendation was accepted.

Information – especially personal information – is a core commodity in our digital era. Growth and success in the digital age depends, in part, on the extent to which the public trusts how personal information is collected, used, disclosed and retained by the organizations that hold it. There is a profound need for these organizations to manage personal information credibly. This requires not only adherence to fair information practices, but also intelligent technology choices

Ann Cavoukian, Ontario Information and Privacy Commissioner
2007 Annual Report

LOOKING AHEAD

There is always room to improve any system and this holds true as well for access and privacy. Some of the recommendations which follow have been made before. With respect to those, I would urge the Government of the Northwest Territories to take steps to address them in some fashion or another. Some of the recommendations being made would require amendments or revisions to the Access to Information and Protection of Privacy Act. It may be that the time has come for a more comprehensive review of the Act to ensure that it keeps up with the challenges of access and privacy in a wired world.

> The access provisions of the Freedom of Information and Protection of Privacy Act are not harsh in terms of what has to be disclosed: there are ample exceptions to disclosure which protect specific interests of public bodies. Leadership is everything: if the head of the public body upholds openness, that will influence the entire organization.
>
> Frank Work
> Information and Privacy Commissioner of Alberta

Limitation Period for Requesting Reviews

The Act, as it is currently worded, allows an Applicant only thirty days after receiving a response to a Request for Information to ask the Information and Privacy Commissioner to review that decision. This is really a very short time frame when one takes into consideration the often slow delivery of conventional mail and the fact that people do not always have fax machines or computers at their disposal. There have been numerous instances in which the Request for Review has been received in my office a day or two after the end of the 30 day period.

Because the Act does not give the Information and Privacy Commissioner any jurisdiction to review a request made after the deadline, or to extend the time where appropriate, the Request for Review cannot proceed. In a number of cases, I have asked the public body to agree to allow the review to proceed notwithstanding the delay and the public bodies have usually complied with those requests. This year, however, there was one incident in which the public body refused to consent to the review, even though the request was received only a few days after the 30 day limitation period. This kind of position is, simply, contrary to the spirit and intention of the legislation which is to promote open-

ness. This is particularly true when one considers that it would be easy for a determined Applicant to simply ask for the information a second time, presumably get the same response as the first time and seek a review in a more timely fashion the second time. The only thing gained by refusing to agree to the extension is delay. As in the case of justice, information delayed is information denied. The only instance in which a limitation period for asking for a Request for Review is important and necessary is where the public body has decided to disclose the information of a third party and the third party seeking to restrict disclosure. In such a case, unless the Request for Review is received from the third party within the 30 days, the information will be disclosed at the end of those 30 days and the third party who has failed to request the review in time will be out of luck. There is, however, no other situation which I can think of in which a few days delay in making the application would cause difficulties for any party.

In order to correct this problem, it would be my recommendation that the Information and Privacy Commissioner be given discretion to extend the time for requesting a review in appropriate circumstances.

> The protection of citizens' personal data is vital for any society, on the same level as freedom of the press or freedom of movement, As our societies are increasingly dependent on the use of information technologies, and personal data are collected or generated at a growing scale, it has become more essential than ever that individual liberties and other legitimate interests of citizens are adequately respected.
>
> Conference of International Data Protection and Information Commissioners Joint Communiqué, London, 2006

Municipalities

A recommendation which has been made several times is that municipalities should be subject to access and privacy legislation. Not only is it important that municipal authorities be accountable to the public through access to information rules, it is also important that municipalities have rules regarding how they gather, use and disclose personal information about individuals.

Every jurisdiction in Canada, except for Nunavut, the Northwest Territories, the Yukon, New Brunswick, and Prince Edward Island have legislation which addresses access and privacy at the municipal level. This is for the benefit not only of the public, but also of the municipalities who currently

have no guidelines or rules which can assist them in governing what can and cannot be disclosed to the public.

I therefore repeat my recommendation that steps be taken to add municipalities as public bodies under the existing act, or that new legislation be developed to apply to municipal governments in the Northwest Territories.

> 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.

Electronic Records Management

As more and more reliance is placed on electronic mediums for communication and for storage of records, the importance of addressing strong security, organization and storage increases. In a paper presented to the 5th International Conference of Information Commissioners by Sandy Hounsell, the Assistant Information and Privacy Commissioner of Newfoundland and Labrador, he made the following observation:

> A crucial aspect of the modern records management system is the explosion over the last number of years of electronic information. The modern workplace has become more and more digital and our reliance on electronic records and databases is unprecedented. It is estimated that more than 90% of all records being created today are electronic.
>
> There is no doubt that the advantages are numerous. We can search it, cut and paste it, update it in real time, e-mail it, automate it, audit it, secure it, and control it in ways that paper-based systems simply would not allow. Ultimately, this allows us to work faster, save money and accomplish much more with significantly less effort.
>
> …..
>
> However, organizations often have difficulty cataloguing, organizing and preserving this infor-

mation, while maintaining a reasonable ability to access it. This is in part due to the failure of many organizations to properly recognize and manage the records management life cycle. This life cycle is equally relevant to both paper records and electronic records, a fact often overlooked by these organizations. More importantly, however, many organizations appear to be overwhelmed by the volume and variety of electronic records. The technology has simply surpassed the capacity to react appropriately.

> The spontaneous nature of e-mail leads to the creation of records containing information that in the past would never have been committed to paper. Such information is often quite sensational to applicants, particularly journalists, who routinely seek out this type of "juicy" information.
>
> Sandy Hounsell
> Assistant Information and Privacy Commissioner of Newfoundland

So many of the reviews which I have conducted in the last number of years involve primarily e-mail records. There is always a concern with such records that they have been properly stored and can be identified as responsive when an application for information is received. Electronic records are only going to increase in volume with time. It is important that the Government of the Northwest Territories keep up with the technologies in terms of its records management system and that the necessary policies are consistent, clear and well enforced. Perhaps more importantly, it is vital that all government employees working with electronic medium and using the internet to communicate and exchange information fully understand those rules and use them in a consistent way so that when a record needs to be found, it is filed in such a way that it can be easily identified as responsive and can be found without difficulties. The alternative will result in a complete inability to fully track and account for records created and government accountability as s whole will suffer as a result.

Security of Electronic Medium

As noted in my last Annual Report, there do not seem to be any government wide policies in place with respect to the security of electronic records or the apparatus which carry them. I could not, for example, find any policy on the use of laptop computers or flash drives

and the management of records stored on those devices. Is there a policy on the kinds of data that can be stored on flash drives and taken out of the office? Are there rules and regulations about the encryption of sensitive data, whether stored on portable devices or on a desktop computer or server? If there are such policies, how well are they known and how well are they enforced?

It is important that there be written government policies regarding electronic medium and that these policies are reviewed regularly to ensure that they keep pace with changing technologies . To the extent that these policies already exist, they should be made part of all orientation programs and should be repeated and reinforced continuously and strenuously enforced with serious consequences attached to a failure to comply with the policies.

Sadly in today's society one of your biggest worries will be how to keep your valuable IT equipment such as laptops, PDAs and i-phones and the even more precious data they contain out of the hands of thieves. Laptop and mobile phone thefts from parked cars and conference rooms may grab headlines, but a far greater number of devices simply get left behind in cabs, on trains, and even on airplanes.

Becky Waring
PC Advisor (London, UK), February 2, 2008

Protecting our Children

Today's young people are growing up in an era in which electronic gadgets are the norm. Most of them are far more comfortable with a computer than their parents. In Canada today, the computer, almost by definition, includes access to the internet. In a recent press release, the Privacy Commissioner for Canada, Jennifer Stoddart, made the following observation:

> We know children and young people in this country are using the Internet for all sorts of activities – primarily to socialize with their friends. And while the Internet provides a way for our kids to connect with their peers in ways we could have never imagined a generation ago, we also realize that there are a whole new set of risks that accompany this new medium.

As I read more about the way in which young people use computers, often starting as young as 2 years of age, I have become more concerned about whether or not they, or their

parents, fully understand the consequences of some of their activities on line. This generation has grown up with the Internet and they are, therefore, comfortable enough with the medium to experiment, to play with it and on it. They may well recognize the risks associated with their online activities but most often they lack the knowledge to mitigate those risks. Their parents often don't even recognize all the potential risks.

More must be done to educate our young people and to provide them with the knowledge they need to protect themselves while they work in the wired world, not only from the obvious risks of pedophiles and identity theft, but also from the less obvious and perhaps more insidious risks that lurk on line. I would recommend that consideration be given to including in school curriculums specific information about electronic medium and strategies for protecting children from on-line risk, beginning at the elementary school level .

The Role of the Information and Privacy Commissioner

The workload of the office of Information and Privacy Commissioner is becoming more significant as the public becomes more familiar with the Act and their rights under it. At the moment, the Information and Privacy Commissioner role is filled on a part time "as needed" basis. In past years, the work for this office amounted to a few hours each month. Each year, the time commitment becomes more significant. The number of Requests for Review, particularly on the privacy side, are increasing year by year and the issues are becoming more and more complex, sometimes requiring significant amount of research. The "active" role of the Information and Privacy Commissioner is to conduct reviews and make recommendations where there are problems with access to information and privacy issues. These have a clear process and antici-

From a child's point of view this boundary between the real world and the online world is becoming increasingly meaningless.

Valerie Steeves
Associate Professor, Department of Criminology,
University of Ottawa in address to the Terra Incognita Conference, Montreal, September 2007 on Childrens' Online Privacy

pated outcome. The time spent on those issues, however, tends to limit the amount of time that can be spent on keeping current with the "big picture" issues. The nature of the IT world, with its ever changing technologies and expanding uses of those technologies make it difficult to remain current on security and privacy issues. The "privacy file" is , by far, the more dynamic of the two mandates of the IPC. Privacy issues require a significant commitment of time to stay abreast of developments but that time is often not available when the position is "part time". It therefore becomes more and more difficult to maintain an appropriate level of expertise on some of the privacy issues. The issues raised by the move toward electronic health and medical records, for example, are very complex and demand specialized background knowledge of medical, technical and technological issues. At the moment, the health sector is very active in terms of developing new technologies and new systems and it is imperative that we get it right the first time when we are dealing with such sensitive information bases. . I note in particular that the project currently underway at the Department of Health and Social Services to develop health specific privacy information will, when implemented, likely involve a considerably expanded role for the Information and Privacy Commissioner and this should be kept in mind as the legislation is rolled out.

> Good privacy training of employees is critical to preventing privacy breaches. Human error is one of the most common factors in the cases we investigate. The best privacy policy in the world is of little use if staff doesn't understand it.
>
> Jennifer Stoddart
> Privacy Commissioner for Canada

Another of the mandates of the Information and Privacy Commissioner is to provide a public education component. This aspect of the office is not being well met because of the shortage of time to develop and deliver effective programs.

All this is to say that it may be that it is time to consider a different approach to the office, perhaps by making it a half time or even a full

time position so as to ensure that the Information and Privacy Commissioner has the dedicated time to commit to these other aspects of the job that are otherwise difficult to address. Alternatively, it may be that the Information and Privacy needs to be given a budget to allow her to hire staff (on contract or otherwise) to carry out some of the functions of the office, to assist in investigations, with technical issues or with a public education campaign. The reality is that the time commitment necessary to do an adequate job is growing and eventually it may be necessary to expand the resources dedicated to the office

The language in the Access to Information and Protection of Privacy Act, like other access and privacy statutes in Canada, creates a bias in favour of disclosure. By providing a specific right of access and by making that right subject only to limited and specific exceptions, the legislature has imposed a positive obligation on public bodies to release information, unless they are able to demonstrate a clear and legitimate reason for withholding it. Furthermore, the legislation places the burden squarely on the head of a public body that any information that is withheld is done so appropriately and in accordance with the legislation.

Newfoundland and Labrador
OIPC Report 2005-002