TABLED DOCUMENT NO. 54-14(5) TABLED ON OCT 16 2002

NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER

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

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

ANNUAL REPORT 2001/2002

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

NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER

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

August 21, 2002

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

Attention: David Hamilton
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, 2001 to March 31st, 2002.

Yours very truly

Elaine Keenan Bengts
Information and Privacy Commissioner
Northwest Territories

In Yellowknife: 403-873-8631 ♦ Toll free: 888-521-7088 ♦ Fax: 403-920-2511 ♦ E-mail: privacy_comm@internorth.com

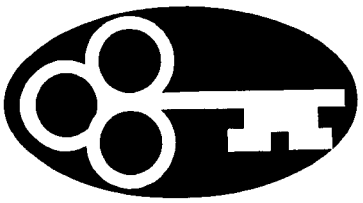
NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

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

ANNUAL REPORT

INFORMATION AND PRIVACY COMMISSIONER

2001-2002



Canada has taken a number of measures, including the passage of the federal *Anti-Terrorism Act* and the expenditure of significant financial resources to promote security and to fight terrorism. However, it is important to remember that the goal of these efforts is to protect our democratic society and its citizens - not to create a state in which people fear for their privacy as much as their security, or one where public openness, transparency and accountability are swept aside under the misguided view that these fundamental democratic principles must be subservient to the needs of security.

Dr. Ann Cavoukian
Ontario Information and Privacy Commissioner
Annual Report 2001

1. COMMISSIONER'S MESSAGE

In 2001/2002, the world changed as the events of September 11th reverberated throughout the world. The reaction of governments in the western world was swift. The Canadian government took steps to increase security and, in so doing, seriously curtailed some of the rights and freedoms that Canadians have always enjoyed. The public's right to receive government information and the individual's right to privacy were both victims of this response to the new threat facing the democratic world. There is a delicate balancing act that must be done to ensure that the rights and freedoms that make democracy strong are not sacrificed to security issues. While increased diligence and security is clearly a new priority, if they come at the expense of our democratic rights, the terrorists may win indirectly what they could not win directly. In the north the effects of September 11th are somewhat remote. Except for tighter security and higher costs for security measures when we travel, we have probably not really noticed a lot of changes. They do, however, exist in the way that law enforcement does their job, in the approach taken by Immigration Officers and in other ways which the ordinary citizen might not immediately notice. We must be diligent to ensure, in all these changes, that our right to privacy and our right to know what government is doing are not so restricted as to change the nature of our democratic ideals.

The *Access to Information and Protection of Privacy Act* is one of the major tools by which these important rights and freedoms are protected at the Territorial level. It helps to pro-

mote openness and accountability of government agencies while at the same time giving us, as individuals, the comfort of knowing that information which the government collects about us will be kept private and be used only for the purposes it was collected.

This is relatively new legislation and it has taken a few years for government employees at all levels to understand and appreciate the impact that the legislation might have on the way government business is done. There is still much education to be done amongst governmental agencies. However, my experience is that those designated as ATIPP Co-Ordinators for the various public bodies designated under the Act appear to have good knowledge of it. Many of the guidelines provided in the Act require the exercise of discretion on the part of the ATIPP Co-Ordinator when it comes to answering requests for information. It appears from my dealing with the Requests for Review that I do receive that there is a genuine effort to apply the rules and guidelines set out in the Act in accordance with the spirit and intent of the legislation. There are open lines of communication between my office and many of the ATIPP Co-Ordinators, particularly in those government agencies whose records are most often sought, and we often are able to discuss general issues which arise.

Apart from the ATIPP Co-Ordinators, it is also my experience over the last few years that more and more government employees generally are becoming more familiar with the legislation. There is always more work to be done to impress upon government employees generally the importance of keeping the provisions of the Act in mind in their day to day work, particularly in the context of e-mail and other communications. I

It is a truism that people do not comply with rules that they do not know or understand. In our consultations with various public service communities, the Task Force found a generally low awareness of the principles set out in the *Access to Information Act*, significant misconceptions about how the Act is meant to operate, and a gap between existing work practices and what would be required to enable the Act to be implemented effectively.

Excerpt from *Access to Information: Making it Work for Canadians*
Report of the Access to Information Review Task Force
June 2002

More protection is needed - there is cause for alarm. For example, a government-commissioned KPMG study of British Columbia's Pharmanet (the computer network of residents' prescription drug histories) revealed that too many people have access to this confidential and sensitive data. More recently, the fate of Manitoba's Smart Health projects, such as the building of the Health Information Network, have been called into question by allegations of mismanagement. In a climate of such uncertainty, citizens can be forgiven for wondering whether governments are giving top priority to protecting their personal health information.

Bruce Phillips
Privacy Commissioner for Canada
Annual Report, 1999-2000

would encourage the Department of Justice to continue to offer educational session for all government employees and to encourage all government agencies to encourage all employees to become familiar with the legislation.

In my last Annual Report, I commented that it would be useful to have statistics to show the number of access requests received by each government agency each year. I have not received any such statistics, but trust that some effort is being made to track these requests.

Once again this year, several of the complaints that did hit my desk were those which arose out of concerns about the inappropriate use of personal information held by a public body. With today's electronic recording and storing of information, people generally are becoming more and more concerned about how that information is being used. Medical records are particularly sensitive. As noted in last year's Annual Report, the amount of personal health information which is shared without our informed knowledge or consent would surprise most of us. To the extent that the information is held by one of the various Health Boards or the Department of Health and Social Services, there is some mechanism in the Access to Information and Protection of Privacy Act to control inappropriate sharing of this information. However, not all personal medical information is in public hands. Pharmacists, dentists, chiropractors and private medical laboratories also have significant amounts of personal medical information and none of them are subject to the protections of the ATIPP Act, which applies only to governmental agencies. Although most

of these private businesses are responsible in the use they make of personal health information, they are not always. Just in the last few months a story came to light about a drug company in the United States which used pharmacist's customer lists to compile a demographic map to define areas within which their antidepressant drug might be successfully marketed and they then proceeded to mail samples of the drug to those areas as a marketing strategy. This is clearly not what these individuals had in mind when they purchased their prescribed drugs from their local pharmacist. Currently, our Act can only deal with breaches of patient confidentiality if that breach comes from a government run or operated institution. Many southern jurisdictions, including Alberta and Manitoba, have passed or are considering separate legislation to deal with the protection of privacy in the health industry. Because of the very sensitive nature of personal medical information, this is an area that deserves serious consideration in the Northwest Territories in terms of developing our own legislation to deal with the privacy of health information.

I would also repeat my recommendation from last year's Annual Report that the Government of the Northwest Territories seriously consider privacy legislation to govern the private sector generally as soon as possible. The *Personal Information Protection and Electronic Documents Act,* (PIPEDA) , federal legislation intended to regulate the collection, storage and use of personal information in the private sector, has been in place since January, 2001, when it came into effect for "federal works" and for companies who transfer information over provincial/territorial boarders except for those in the

The line between clinical practice and medical research is becoming increasingly blurred. The tools of medical investigation and of information gathering are being applied to human subjects with escalating intensity. The expansion of research...may, before long, turn every patient into a research subject (or rather a research object) simply by virtue of a decision to seek medical care.

Beverly Woodward
1999

The (Personal Information Protection and Electronic Documents) Act is coming into effect in stages. It has applied since January of this year to personal information, other than health information, of customers or employees of works, undertakings, or businesses under federal jurisdiction - principally banks, telecommunications, broadcasting, and interprovincial or international transportation, as well as in the Northwest Territories, Yukon and Nunavut, where it applies to the whole private sector, which, under the constitution, is federally regulated.

George Radwanski
Privacy Commissioner of Canada
Annual Report 2000-2001

health sector. On January, 2002, the health related private sector was added. The Act comes into effect for all other commercial activities on January 1st, 2004 unless, prior to that date, provincial legislation is passed which is similar or substantially similar to the federal legislation in the individual provincial/territorial jurisdictions. The intention was to give the provinces and territories time to formulate their own legislation to deal with this issue in each province or territory. As noted in my last Annual Report, however, the Federal Privacy Commissioner has taken the position that all of the Northwest Territories (and the other two territories) are "federal works" and, therefore, subject to the Act immediately. This means that complaints can be made to the Federal Privacy Commissioner about a private sector company in the Northwest Territories and it will be dealt with by an individual who works and resides in Ottawa and has no understanding or knowledge of the local economy. The Federal Privacy Commissioner's failure to recognize the true nature of Canada's three Territories does not give me, personally, a good feeling about leaving him to make these kinds of decisions about our businesses and economy.

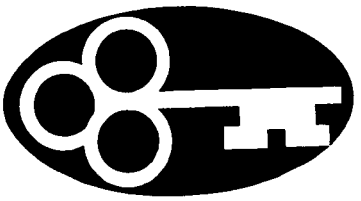
It was my pleasure to host the Information and Privacy Commissioners from across the country in Yellowknife for our annual get together in June, 2001. We had two days of very good discussions and I was very proud to be able to show my counterparts some of the wonderful hospitality that Northerners are famous for. Several of the participants took part in the Annual Midnight Golf Tournament and all were treated to a wonderful evening at Hidden Island, where we were enter-

tained by local musicians. It was a successful meeting and all left with a better appreciation for the North.

It continues to be my honour to be able to hold this position and to work with the government to ensure that the goals and objectives contemplated by the Access to Information and Protection of Privacy Act are met.

From a privacy point of view this tremendous growth will allow us to build PCs that might recognize emotions and talk like human beings. A multi-media telephone might record each conversation, and automatically identify the calling voice recognition and provide all the information about the caller it can find on the Internet. Everything one ever communicated electronically, or did, or said in a public place, might be recorded. Information once collected will never disappear. Anything can be observed - nothing remains local anymore. Even non-digital transactions will leave digital traces.

Matthias Kaiserswerth
Vice President of IBM Research, Laboratory Director, Zurich. Switzerland
Address to the 23rd International Conference of Data Protection Commissioners
September 24-26, 2001



II. INTRODUCTION

A. ACCESS TO INFORMATION

Background

Access to Information and Protection of Privacy legislation was developed as a tool to encourage and promote open and accountable government while recognizing that government agencies hold considerable amounts of personal, private information about individuals which need to be protected from improper use or disclosure. In the Northwest Territories, our legislation came into effect on December 31st, 1996.

The Act provides the public with a means of gaining access to information in the possession of the Government of the Northwest Territories and a number of other governmental agencies, subject to certain exceptions which are spelled out in the Act. These exceptions function to protect individual privacy rights, and allow elected representatives to research and develop policy and run the business of the government. The Act also gives individuals the right to see and make corrections to information about themselves in the possession of a government body. The current regulations list 38 departments, boards and other agencies subject to the Access to Information and Protection of Privacy Act. Unfortunately, the regulations do not appear to have been amended since the creation of Nunavut and at least some of those governmental agencies listed no longer exist within the Northwest Territories. This list should be reviewed and revised to reflect an accurate listing of those agencies which come under the Act.

[The] many valid public policy reasons for creating and keeping records are sometimes ignored or difficult to implement. Government internal communications have become increasingly casual, aided b the growing ease and convenience of electronic mail, voice mail, fax and similar tools. Some key decisions and directions are conveyed orally with no record of the transaction.

Ian Wilson
National Archivist of Canada
3rd Annual ATIP Conference
Ottawa, November 2001

Since the [Access to Information] Act came into force in 1983, debate has centred largely on the design of exemptions, interpretation of the various provisions, and denouncing instances of non-compliance. Government efforts have focused mainly on publishing implementation guidelines, recruiting and training access officers and putting in place processes and systems needed to handle a growing volume of requests and meet legislated deadlines. Neither at the time the Act came into force, nor since, has there been a comprehensive strategy to raise awareness of, and support for, access to information in the federal public service.

Excerpt from
Access to Information: Making it Work for Canadians, Report of the Access to Information Review Task Force
June, 2002

The Process

Each of the public bodies governed by the Act has appointed an ATIPP Co-ordinator to receive and process requests for information. Requests for information must be in writing but do not require any particular form (although there are forms available to facilitate such requests). Requests are submitted, along with the $25.00 fee, to the appropriate public body. There is no fee for a request to access an individual's own personal information.

The role of the public body is to apply the specific requirements of the *Access to Information and Protection of Privacy Act* to each request received while at the same time protecting private information of and about individuals which they have in their possession as well as certain other specified kinds of information. Because of the exceptions to disclosure contained in the Act, the ATIPP Co-Ordinators are often called upon to use their discretion in determining whether or not to release the specific information requested. The ATIPP Co-Ordinators must exercise their discretion to ensure a correct balance is struck between the applicant's general right of access to information and the possible exceptions to its disclosure under the Act.

In the case of personal information, if an individual finds information on a government record which they feel is misleading or incorrect, a request in writing may be made to correct the error. Even if the public body does not agree to change the information, a notation must be made on the file that a request has been made that it be changed.

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

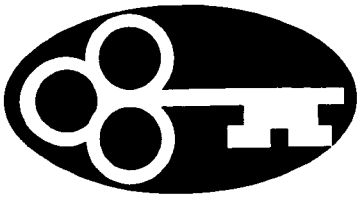
Parliament and the public cannot hope to call the government to account without an adequate knowledge of what is going on; nor can they hope to participate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view. Access laws operate on the premise that politically relevant information should be distributed as widely as possible.

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

The role of the Information and Privacy Commissioner is to provide an independent review of discretionary decisions made by the public bodies in the application of the Act. The Commissioner's office provides an avenue of non-binding appeal to those who feel that the public body has not properly applied the provisions of the Act. The Commissioner is appointed by the Legislative Assembly but is otherwise independent of the government. The independence of the office is essential for it to maintain its credibility and ability to provide an impartial review of the government's compliance with the Act. Under the Act, a Commissioner is appointed for a five (5) year term.

The ATIPP Commissioner is mandated to conduct reviews of decisions of public bodies and to make recommendations to the Minister involved. The Commissioner has no power to compel compliance with her recommendations. The final decision in these matters is made by the "head" of the public body involved. 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.

In addition to the duties outlined above, the 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 effect access to information or the distribution of private personal information in the possession of a government agency.



A truly effective access scheme requires governments to move beyond the reactive nature of the law, and embrace routine disclosure and active dissemination (RD/AD) of information as key elements of transparent and fully accountable public administration. Furthermore, many organizations that have benefited from implementing RD/Ad are looking to use recent developments in information technology to advance the concept and maximize the benefits of RD/AD can offer both organizations and the public.

Dr. Ann Cavoukian
Ontario Information and Privacy Commissioner
"Opening the Window to Government: How e-RD/AD Promotes Transparency, Accountability and Good Governance"
June, 2002

B. PROTECTION OF PRIVACY

The *Access to Information and Protection of Privacy Act* also provides rules with respect to the collection and use of personal information by government agencies. Part II of the Act outlines what have become generally accepted rules for protection of privacy internationally. They include:

No personal information is to be collected unless authorized by statute or consented to by the individual;

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

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

The personal information collected shall be secured and the government agency will ensure that it is available only to those who require the information to provide the service or conduct the business for which the information was collected.

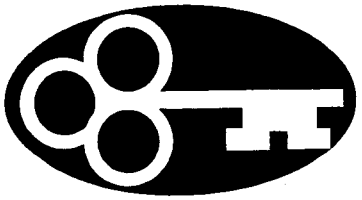
Personal information collected by a government agency will be used only for the purpose it is collected; and

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

Although the Information and Privacy Commissioner does not have any specific authority under the Act to do so, this office has been receiving privacy complaints and making inquiries and recommendations with respect to breaches of the provisions of the Act dealing with personal privacy. The only option other than a review process with recommendations, is for the offending government employee to be prosecuted under the Act. Prosecution, however, is both unlikely except in extreme cases, and not very instructive. The Standing Committee on Accountability and Oversight has recommended that the Information and Privacy Commissioner be given specific authority to investigate and make recommendations with respect to breaches of the privacy provisions of the Act but this recommendation has yet to be acted upon, leaving the privacy provisions of the Act weak and ineffectual should a governmental agency choose not to co-operate with the Information and Privacy Commissioner. The public's ever increasing insistence on the protection of personal privacy requires that this part of the Act be amended as soon as possible.

Personal health information - information about the state of our own bodies and minds - is arguably the most private information of all. All inappropriate disclosure can have devastating consequences. Indeed, fear of losing control over their health information can deter people from seeking medical care at all, with detrimental results not only for them but also for society as a whole. That's why any privacy protection legislation that does not fully protect health information is scarcely worthy of the name.

George Radwanski
Privacy Commissioner of Canada
Annual Report 2000/2001



III. REQUESTS FOR REVIEW

Under section 28 of the *Access to Information and Protection of Privacy Act*, a person who has requested information from a public body, or a third party who may be affected by the release 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 of discretionary and other decisions made under the Act.

Perhaps the hardest dilemna of privacy is not just how much is optimal, or the ways it must be balanced with communal needs, but it large fragility as a human situation — how quickly it can be harmed by other, more predatory, human impulses.

Janna Malamud Smith
1997

A Request for Review is made by a request in writing to the 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. A Request for Review may be made by a person who has made an application for information under the Act or by a third party who might be mentioned in or otherwise affected by the release of the information requested.

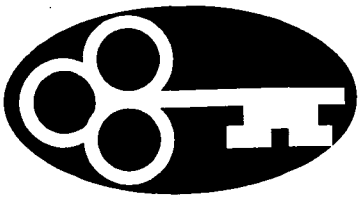
Requests for Review are reviewed by the Commissioner. In most cases, the Commissioner will first request a copy of the original request made and a copy of all responsive documents from the public body involved. In most cases, the Commissioner will review the records in dispute. Generally, an attempt will first be made by the Commissioner's Office to mediate a solution satisfactory to all of the parties. In several cases, this has been sufficient to satisfy the parties. If,

however, a mediated resolution does not appear to be possible, the matter moves into an inquiry process. All of the relevant parties, including the public body, are given the opportunity to make written submissions on the issues. In most cases, each party is also given the right to reply, although this has not always proven to be necessary.

Several matters were reviewed by the Commissioner in the last year and Recommendations made. Other requests were resolved without the necessity of a complete review process. In addition, the Information and Privacy Commissioner was asked on several occasions to provide comment and input into various government initiatives and/or legislation.

This globalisation of data exchange and the use of the Internet has modified the boundaries between public and private sector. These have become more changeable and often more tenuous. Progress in the means of communication has never before given rise to such a need for individual guarantees. It is essential that the proliferation of files containing private information, whose use may be discriminatory, be controlled by law, whether it concerns establishing employment or insurance contracts or allocating housing.

Mr. Lionel Jospin
Prime Minister of France
Address to the 23rd International Conference of Data Protection Commissioners
September, 2001



IV. REVIEW RECOMMENDATIONS

Review Recommendation #01-018

This Request for Review came from a somewhat unusual source in that it came from The Stanton Regional Health Board (SRHB), which is itself a public body subject to the terms of the Access to Information and Protection of Privacy Act. SRHB is an agency created by the Government of the Northwest Territories to provide health services to the Yellowknife region. Individuals receive goods or services from the SRHB and the SRHB, in turn, bills NWT Healthcare for insured services. Not all goods and services provided by the SRHB, however, are insured. For these services, the individual is billed directly. SRHB was trying to collect on a number of outstanding receivable and found that in many cases they could not do so because the individual had moved out of the Northwest Territories.

NWT Healthcare, a division of the Department of Health and Social Services, receives "migration reports" from the other provinces and territories for individuals who apply for healthcare coverage elsewhere in Canada. These reports include the individual's new address.

SRHB sought addresses for specific individuals from NWT Healthcare. NWT Healthcare was reluctant to share this information because of the ATIPP Act, as well as the provisions of the Medical Health Care Act. SRHB asked me to review NWT Healthcare's decision to refuse to share the information

Without a copy of the agreements by which the various governments exchange this information, it is impossible for me to say that the use SRHB wishes to put the information to is or is not a "consistent purpose". I think, however, it is incumbent on NWT Health Care to review those agreements carefully to determine specifically what the "purpose" of exchanging this information is.

Elaine Keenan Bengts
Information and Privacy Commissioner, NWT
Review Recommendation #01-018

requested.

The Review Recommendation reviewed the relevant provisions of both pieces of legislation, pointing out that Section 4(2) of the ATIPP Act provides that, to the extent that its provisions are inconsistent with access or privacy provisions in another piece of legislation, the ATIPP Act prevail unless there are specific provisions in the other legislation to the contrary. In this case, there were no such provisions in the Medical Health Care Act.

Section 4(d)(i) clearly allows the release of personal third party information for the purpose of collecting a fine or a debt owed by an individual to the Government of the Northwest Territories or a public body. SRHB, itself a public body, is owed money by certain individuals. Another public body, NWT Health Care, has the information that would assist in collecting those debts. The Act clearly and unequivocally provides for an exception to the protection of third party private information in such circumstances.

Elaine Keenan Bengts
Information and Privacy Commissioner, NWT
Review Recommendation #01-018

Section 48 (d)(i) of the ATIPP Act provides that personal information may be disclosed by a public body for the purpose of collecting a debt owed by an individual to the Government of the Northwest Territories or a public body. As the information in question was being requested for the specific purpose of collecting a debt owing to a public body, the recommendation was that the information should be released to the SRHB with the proviso, however, that it be used only for the purpose stated, that is, to collect debts owing to the SRHB.

<u>Recommendation # 01-019</u>

The Applicant in this case sought certain information from the Workers' Compensation Board, mostly from his own file, but including other information as well, such as a definition of a particular ailment.

It appeared from the information which was provided with the Request for Review that the Applicant's contact with the WCB

had a bit of a history. As a result, the Board's response to the Applicant's request for information was somewhat terse. It appeared that the information was refused because:

a) the form upon which the request for information had been requested was a federal government form, not an NWT form;

b) a disclosure had been made to the client in Oc tober, 1999 and that the Board would not pro vide additional copies of documents already provided unless the Applicant paid a $25.00 fee.

The letter pointed out that if the proper form was filled out, the Workers' Compensation Board would provide copies of any material on the Applicant's personal file but only subsequent to October, 1999 (the previous disclosure date).

The ATIPP Commissioner pointed out that the Act specifically requires public bodies to assist Applicants to obtain the information they are requesting and that there was no specified form for making a request. The fact that the request had been received on a federal government form should have no impact on the application and should have been acted upon.

In addition, the Commissioner pointed out that there is no fee payable for requesting personal information. If the individual seeks the same information every year, he is entitled to it with no application fee. It was suggested that the WCB contact the Applicant to determine if he needed to have previously

[T]he *Access to Information and Protection of Privacy Act*, provides quite clearly that when an Application if made for access to information, there is a duty on the government agency involved to assist the Applicant. That would include, in my respectful opinion, accepting a request for information even though it is made on the wrong form without requiring the Applicant to re-do the request on the "correct" form. In fact, the Act does not provide for any specific form of application. It merely requires the request to be in writing. It was improper, therefore, to reject the request merely because it was on the wrong form.

Elaine Keenan Bengts
Information and Privacy Commissioner, NWT
Review Recommendation #01-019

provided information repeated, but that if he insisted on receiving all personal information a second time, he was entitled to receive it. There may, however, be a fee for processing and copying the file a second time. Specifically in this case the Commissioner suggested that the WCB needed to communicate more effectively with the Applicant to explain its response to his request.

Recommendation 01-020

In this case, the Applicant requested that certain information about him be corrected pursuant to section 45 of the ATIPP Act which provides that an individual who believes that there is an error or omission in his or her personal information may request the head of the public body who has the information in his custody or under his control to correct the information.

The documents in question were two letters written by two employees of the Department of Justice. The letters were, in essence, witness statements setting out their recollection of an incident involving the Applicant. The information which the Applicant wanted to have corrected was a statement attributed to him in the letters. The Applicant wanted the record to be changed to remove the alleged statement because he says he never made it.

The Information and Privacy Commissioner pointed out that the documents in question were subjective statements made about an incident and the respective individual's recollection of what was said. They were not personal information about

In this case, I believe that the Department was correct in refusing to alter the statements made by the writers of the two letters with respect to the words they allege they heard the Applicant say. It is not for the Applicant to say what a third party heard. He can disagree that he said the words attributed to him, but he is not in a position to say the writer did not hear those words. The only person who can say what they heard is the person who heard it.

Elaine Keenan Bengts
Information and Privacy Commissioner, NWT
Review Recommendation #01-020

the Applicant, but a subjective observation by a third party respecting the Applicant. It was not for the Applicant to say what a third party heard. He could disagree that he said the words attributed to him, but he was not in a position to say the writer did not hear those words. What the Applicant could, and in fact, had done was to ask that a notation be made, cross-referenced to the documents in question, that he denied that he made the statement attributed to him.

In this case, the information in question had been provided to a third party. Under the provisions of the ATIPP Act, the third party who received the documents in the first instance would receive a copy of the denial, and the denial will appear on the file in question so as to alert any other person who sees the file in the future that the Applicant did not agree with the statements attributed to him.

Recommendation 01 - 021/022

This matter came before the Information and Privacy Commissioner from a Third Party who objected to the release of her employment contract with the Government of the Northwest Territories. A request had been received by the Department of the Executive seeking a copy of the Third Party's employment contract. In accordance with the provisions of the Access to Information and Protection of Privacy Act, the Access Co-Ordinator for the Department advised the Third Party, that it was their intention to release the information requested with certain specifics edited out. The Third Party objected to the release of the contract. After reviewing the Third

Public funds are used to pay the Third Party. The terms of the employment contract are, therefore, of public interest. Section 23(4) specifically provides that the release of information relating to pay ranges, benefits, and employment responsibilities is NOT to be considered an unreasonable invasion of privacy. This holds true for all employees of the government, be they highly or lowly placed within the public service.

Elaine Keenan Bengts
Information and Privacy Commissioner, NWT
Review Recommendation #01-021/022

Party's objections, the ATIPP Co-Ordinator confirmed that the majority of the contract would be released with reference to actual salary severed from the document. The Third Party then requested that I review that decision.

The Third Party was a highly placed public servant. The contract at issue outlined the terms and conditions of employment, the responsibilities of the position, termination and other related employment issues. Also included were provisions with respect to salary and benefits.

The Third Party's request that any release of the document be under the supervision of her lawyer and that the Applicant not be provided with a hard copy of the contract, is also specifically dealt with in the Act. Where the Applicant has requested a copy of the document, and the document can be readily reproduced, it must be provided to the Applicant. There is no provision in the Act which would allow the public body to restrict access to simply reviewing it.

Elaine Keenan Bengts
Information and Privacy Commissioner, NWT
Review Recommendation #01-021/22

In making her recommendation, the Information and Privacy Commissioner pointed out that public funds were paying the Third Party. The terms of the employment contract were, therefore, of public interest. Section 23(4) specifically provides that the release of information relating to pay ranges, benefits, and employment responsibilities is NOT to be considered an unreasonable invasion of privacy and this was true for all employees of the government, be they highly or lowly placed within the public service.

Section 23(4) provides only that the release of information relating to "pay range" is not be to be considered an unreasonable invasion of privacy. By extension, the release of specific and exact income information would be considered an unreasonable invasion of the Third Party's privacy.

The recommendation made by the Commissioner was that a copy of the contract be provided to the Applicant with those parts relating to specific income being severed. She felt that

the Department had properly applied the provisions of the ATIPP Act.

Recommendation #02-023

The City of Yellowknife requested advice and direction with respect to what they considered to be a refusal of the Department of Transportation to provide information they had been receiving for several years. In particular, the City wanted to have the continued ability to download motor vehicle information from the Department of Transportation's database for the purpose of enforcing the *Motor Vehicles Act* and the City's Highway Traffic By-Law.

The City of Yellowknife took the position that, as a law enforcement agency, the By-Law Department of the City should continue to have downloadable access to the full motor vehicles database. Although they concede that there was more information in the database than they needed to strictly enforce their by-laws, their law enforcement function put them within an exception to the prohibition against release of information. They pointed out that only the By-Law Department had access to the database and that the information downloaded was never manipulated or changed in any way. They also indicated that they required the downloadable version of the data to make use of their Interactive Voice Response System.

There is no suggestion that the information which the City seeks is, or has been, used for any other purpose than for law enforcement. That having been said, the City is not bound by the provisions of any access or privacy law. Once the information is out of the hands of the Department of Transportation, there is no control over the use that the information is put to. There is, as I understand it, no written or even any verbal agreement between the City and the Department of Transportation to limit the use of the information available to the City.

Elaine Keenan Bengts
Information and Privacy Commissioner, NWT
Review Recommendation #02-023

Although the release of personal information for law enforcement purposes is contemplated by the ATIPP Act, one of the main objects of the Act is to limit the dissemination of personal information. Although I have not seen the Department of Transportation's database, I expect that it contains far more information than is needed by the City for the enforcement of its laws. For one thing, it will contain information for all license holders in the Northwest Territories and the By-Law Department has jurisdiction only in Yellowknife..... Nor does the City need all of the information on the database. They need only the limited information required to identify the vehicle owner, such as name, license number, address and telephone number. If personal information is to be released to a third party, no matter what the purpose, the amount of information released should be limited to that information actually needed to accomplish the purpose for which it is given.

Elaine Keenan Bengts
Information and Privacy Commissioner, NWT
Review Recommendation #01-023

The Department of Transportation took the position that, although the City could have access to their database, they were not prepared to continue to provide them with the ability to download all of the information on the database. That this full access was given to the City in the past, they say, was an error. They pointed out that the City continued to have "query" access, which means that they could access the database on a case by case basis for law enforcement only.

The ATIPP Commissioner, after reviewing both the ATIPP Act and the Motor Vehicles Act, found that, for the purposes of this review, there was no conflict between the two Acts on what "may" be released. The result was that any release of information beyond that mandated by the Motor Vehicles Act was governed by the Access to Information and Protection of Privacy Act. The latter legislation required that any information provided should be limited to that information reasonably necessary to enforce the By-Laws of the City of Yellowknife. The City did not establish that they required full downloadable access to the full database in order to achieve this purpose. The Commissioner pointed out that this was particularly so because there is no legislation which governs the use of the information once it leaves the Department of Transportation as the ATIPP Act does not bind municipalities.

She felt that the Department of Transportation had come up with a reasonable compromise, providing the same limited access to the database as it provides to other law enforcement agencies. However, until such time as the City of Yellowknife is subject to its own privacy legislation, no informa-

tion should be provided to the City until such time as there was a contractual agreement between the City and the Department limiting the use that could be put to the information provided to the City.

Recommendation 02-024

This matter involved an individual who was convinced that one of several government agencies had untrue information about him in their files and that that information had been improperly used to his detriment in several ways. Various government departments and agencies were involved, including the Department of Justice, Stanton Regional Health Board, the Hay River Medical Clinic and H.H. Williams Memorial Hospital. He was convinced the information was being used to deny him access to government programs and the assistance he needed.

In view of the Applicant's adamant insistence that the allegations against him had been made, and that they were on his files, the Information and Privacy Commissioner did a thorough review and search of the relevant files. The Applicant provided the names of a number of individuals who he says had, in times past, told him that they had personally seen the allegations in question. The Information and Privacy Commissioner personally contacted most of the individuals mentioned in the Applicant's complaint letter to determine from them whether each of them could corroborate the Applicant's statements. She also personally attended the Stanton Yellowknife hospital in Yellowknife and reviewed each of the Ap-

In its traditional meaning, privacy protection goes against the requirements of the community's interests, which are the basis for the limits imposed on medical secrecy for three sorts of reasons: public health and sanitary safety, medical and epidemiological research, and expense control (pursuit of efficiency). States are responsible for defining the balance between both types of equally legitimate but potentially contrary concerns.

Gilles Johanet
General Manager of National Health Insurance Fund (France)
Address to the 23rd International Conference of Data Protection Commissioners
September, 2001

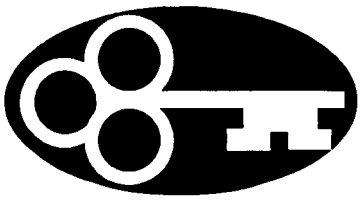
plicant's personal medical files as well as hearing from the Department of Justice and the Hay River Community Health Board.

Despite the Applicant's insistence on the existence of these allegations, the only evidence of them that could be found anywhere were references made by the Applicant himself. Each of the individuals spoken to also confirmed that, although they were aware of the Applicant's belief in the existence of the allegations, the only knowledge they had of them was what the Applicant himself had told them personally or by means of a flyer which the Applicant had distributed fairly widely.

The Commissioner recommended that nothing further be done.

One approach...is to devise and rigorously implement a government-wide system for routine disclosure of information without access requests having to be made. A principled argument for doing this, of course, is that it promotes openness and accountability. but it can also be an effective response to the scarcity of resources and the ensuing delays experienced in many jurisdictions, since it would obviate resort to the potentially costly and time-consuming processes inherent in any modern access law.

David Loukedelis
British Columbia Information and Privacy Commissioner
FOIP 2000 Conference - Edmonton, Alberta
May 29, 2000



VII. STATISTICS

In 2001/2002, nine new Requests for Review were received. This is same number as last year. Of these, one was resolved by the issuance of recommendations, three were resolved by means of negotiation and mediation between this office and the parties and two were withdrawn. The three remaining are currently under review and recommendations are expected within a short period of time.

During the 2001/2002 fiscal year, six reviews were completed and recommendations made. The ATIPP Commissioner's recommendations were accepted in all cases. This is up from four in the last fiscal period.

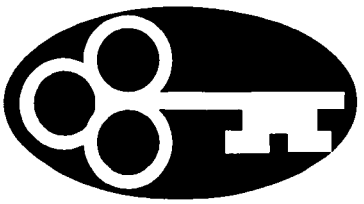
In addition, the Information and Privacy Commissioner was asked for her input and advice on two issues raised by public bodies and that input was provided.

In 2000/2001, the Department of the Executive and the Department of Health and Social Services were the departments most often involved in Requests for Review.

There is no evidence of the slackening of the pace or the weakening of the resolve of those who wish to take forward law enforcement initiatives. It is the important task of the data protection community to make sure that those measures that impact on privacy are a proportionate and effective response to the menace that they seek to combat.

Elizabeth France
Information Commissioner of England
Annual Report for year ending March 31, 2002

June 2002



Good information management is a precondition to good access to information. Information management in the federal government is in need of serious attention. A government-wide information management strategy is required....and with supporting monitoring and accountability regimes. Public servants need to be made aware of their responsibilities for the creation, management and disposal of information, and provided with the knowledge, skills and tools necessary to carry out those responsibilities. A significant investment of resources will be required, both to address the current information management deficit, and to implement longer term strategies.

Excerpt from *Access to Information: Making it Work for Canadians Report of the Access to Information Review Task Force*
June, 2002

VIII. RECOMMENDATIONS

Many of the recommendations made in the Information and Privacy Commissioner's annual report in the last few years have been accepted in whole or in part by the legislative assembly. However, we have yet to see the changes made. For this reason, many of my recommendations for change are simply repeated from previous years.

One of the issues that I feel most strongly about is that municipalities either be included as "public bodies" under the Act or that new legislation be created to make rules and regulations with respect to both access to information and protection of personal privacy. This matter has been referred to the Association of Municipalities, the Department of Justice and the Department of Municipal and Community Affairs for further discussion but I have heard little more about the matter. The issue which arose between the City of Yellowknife and the Department of Transportation about the sharing of information is a good example of why such legislation is needed. In point of fact, the Department of Transportation should not be providing any personal information to the City, even in accordance with the Access to Information and Protection of Privacy Act, without a proper information sharing agreement which limits, by contract, the use that can be made of such information. News reports from both Yellowknife and Hay River over the last year about access to information issues also underline the need for guidelines and consistency in determining what is, and what is not, subject to an access request. I continue to consider this to be a priority.

Most companies need to collect, use and disclose some information about their customers in order to conduct their business. But organizations must be reasonable and fair in their treatment of personal information, not only for the good of their customers, but also for the good of their own business reputations. consumers are no longer willing to overlook a company's failure to protect their privacy. High profile misuses of personal information have shown that a lack of respect for personal information can bring both harsh criticisms from consumers, and significant devaluation of company shares.

Excerpt from "Privacy Diagnostic Tool (PDT) Workbook"

With information technologies becoming ever more sophisticated and powerful as each year goes by, I would once again emphasize the need to regulate personal privacy in the private sector, most particularly in the health sector. Health care is not only a public sector service. There are many private sector businesses (and I stress the word business) which receive and hold very sensitive personal information. One of the fastest growing private sector businesses is the buying and selling of personal information databases. Most private business in the health sector is careful and responsible in the use they make of this information and one might hope that they would continue to be so. However, to rely exclusively on volunteer adherence to a privacy policy by the private sector in today's world is, I would suggest, short sighted and overly optimistic. Furthermore, legislated guidelines can provide guidelines and consistency in practice. Even if the government does not want to tackle generalized private sector legislation, I would strongly recommend that it does consider health sector legislation.

I also repeat my assertion that this government should consider generalized privacy legislation over private sector businesses. With all due respect to my colleague, the Federal Privacy Commissioner, I do not believe that he is adequately informed about the North to be making the kinds of decisions which the PIPED Act allows him to make about our local economies. I strongly believe that these are issues that are more effectively dealt with at the local level.
Along the same lines, as noted in previous Annual Reports,

although the Act sets out a number of rules dealing with the collection, use and disclosure of personal information, the Act does not specifically allow the ATIPP Commissioner to investigate or provide recommendations when there is a complaint that an individual's privacy rights have been breached. We receive a number of these kinds of complaints each year. The absence of specific authority to investigate and provide recommendations in such circumstances has not prevented me from doing those investigations and providing recommendations. There is, however, nothing in the Act which requires public bodies to comply with any requests I might make of them in such circumstances and nothing which requires the head of a public body to deal with recommendations made. I believe that the intention of the legislature when passing this legislation was to ensure a mechanism which would allow a review of breaches of privacy under the Act and I would recommend, once again, that the specific authority be given to the ATIPP Commissioner to review complaints of breaches of the privacy sections of the Act and to provide recommendations with respect to same which must be dealt with in some manner by the government body involved.

I would also like to see the Regulations under the Access to Information and Protection of Privacy Act which list the names of the public bodies which are subject to the Act updated. This needs to be done for two reasons. Firstly, and perhaps most importantly, the named public bodies need to reflect the fact that Nunavut has separated from the Northwest Territories. In reviewing the Regulations under the Access to Information and Protection of Privacy Act as posted

Efficiency is a worthwhile aspiration. But, as I have emphasized repeatedly, efficiency has to be properly understood, as a relation between means and ends - choosing the best means of achieving defined goals. What is critical is how we define the goals. For government, and for society, those goals have to include the preservation and protection of privacy.

George Radwanski
Privacy Commissioner for Canada
Annual Report 2000-2001

If certain personal data can or must be disclosed to the general public, does dissemination via Internet ad "something" to this and should one start from different assumptions in terms of limitations or safeguards applying to data subjects' personal rights?

The answer would seem to be obvious; however data protection safeguards and issues are not always top priorities on the to-do list of the experts striving, fully in good faith, to improve transparency of public administrative action.

It is reasonable to conceive of Internet as a unique opportunity for simplifying and reducing costs for citizens in accessing publicly available information, so as to reduce information monopolies, ensure that databases are as effective and complete as possible, enhance the sharing of the available information and improve the citizen-government relationships.

However, dissemination on Internet is different from other types of dissemination.

Giovanni Buttarelli
General Secretary of the Italian Data Protection Commission (Italy)
Address to the 23rd International Conference of Data Protection Commissioners
September, 2001

on line through the Government's web page, I note that the regulations still include entities such as the Keewatin Regional Health and Social Services Board, the Baffin Divisional Education Council and many similar bodies which are no longer in the Northwest Territories or, for that matter, in existence at all. The Regulations posted were stated to be updated to July 1st, 2002. Secondly, I suspect that there have been new public bodies created since 1998 (which is apparently the last time these Regulations were amended) and perhaps others which have been disbanded. This list needs to be reviewed and updated regularly to ensure that it reflects accurately the public bodies which exist in the Northwest Territories from time to time.

A new concern that is attracting much attention from my colleagues across Canada and internationally is access to public registry databases. Information and Privacy Legislation throughout the country, including the Northwest Territories, exempts records made from information in a registry operated by a public body where public access to the registry is normally permitted. There is good reason to maintain certain information open to public review. For example, public access to personal property and land registry systems provides a means for buyers to inspect the title to a property before purchasing it. However, when these registry systems were developed, they were paper based and, although accessible, could not be accessed *en masse* or downloaded from the Internet. As noted by the Ontario Information and Privacy Commissioner in her 2001 Annual Report to Parliament, "In a paper and microfiche-based world, public registries enjoyed a

limited measure of privacy protection because of what has been described as their "practical obscurity". In order to inspect a registry, list, or role, an individual would have to travel to a government office during the prescribed office hours. In addition, the documents in public registries could only be copied or searched on a record-by-record basis." She goes on to point out, however, that as public registries become available "on line" or in electronic form, they can be easily "retrieved, searched, sorted, manipulated and used for purposes that have no connection to the original purpose for which the information was collected". She goes on to point out a series of consequences from "on line" accessibility, including:

- direct marketing firms can use computer software to collect, sort and combine names, addresses and telephone numbers from public registries and target consumers with junk mail and unsolicited telemarketing pitches;

- public registries posted on web sites can be searched by name and address, and criminals such as stalkers and domestic abusers may be able to trace the whereabouts of their victims through a government database

- identity thieves can more easily access and combine personal information from such registries with information gleaned from other sources in order to steal identities

This is not an outlandish or hypothetical threat. It has already happened in Oregon. In November of 2001, police in Hillsboro, Oregon found death certificates and social insurance cards for a large number of people, along with two CD-ROMs

Collectively, public records reveal "a vast array of detail about an individual's activities and personal characteristics". When collected, compiled and maintained over years and across jurisdictions, the records contain a more complete reflection of the events, habits, and occupations of individuals and families. The effect of technology on the use of public record information is notable. Professor Mary Cunan observed that technology has stripped much of the privacy that used to exist because of the difficulty of finding and obtaining records.

Robert Gellman
Privacy and Information Policy Consultant (United States)
Address to the 23rd International Conference of Data Protection Commissioners
September, 2001

containing bulk lists that had been legitimately purchased from the Motor Vehicle Registry.

Information and Privacy Commissioners across the country are advocating the establishment of some form of control over these public registry systems and I join them in both their concern and their recommendation to take a good look at this area.

In closing, I return to the one recommendation which I have been making for at least the last three years with respect to what I consider to be a considerable gap in the legislation. Once my recommendations are made, the head of the public body has 30 days within which to accept the recommendations, reject them or make some other decision based on them. There is no provision in the Act to say what happens when the head of the public body fails to deal with the recommendations within the 30 day period and there has been at least one instance in which it was almost a full year after the recommendation was made before the head of the public body dealt with it. My recommendation has been that there be a deemed acceptance rule implemented such that if the head of the public body fails to deal with the matter within the 30 days, the recommendations are deemed to have been accepted. For some reason, the government feels more comfortable with a deemed rejection rule such that if no response is received from the head of the public body within the 30 days, my recommendations are deemed to have been rejected. I am strongly against this approach as I believe it will cause far more mischief than the alternative. The best way

For access to become part of the organizational culture, it needs to be recognized by managers as a legitimate aspect of their staffs' work, on the same footing as their other duties. It should be routinized in day-to-day work processes and activities, and reflected in job descriptions and in performance reviews. It should be discussed in management meetings and reflected in the organization and resourcing of new programs, and in corporate plans. Several institutions have taken steps such as these to provide visibility, positive incentives, and accountability for access. These practices should be encouraged across the public service.

Excerpt from *Access to Information: Making it Work for Canadians*
Report of the Access to Information Review Task Force
June, 2002

to demonstrate the issue is by way of example, which follows:

> An applicant has made a request for a series of documents which includes personal health information of a third party and certain business information relating to another third party. The public body agrees to release most of the information requested but refuses to release the personal health information of the first third party and some of the business information of the second third party. The Applicant requests that the ATIPP Commissioner review the decision of the public body to refuse access to the third party information. The ATIPP Commissioner reviews the matter and recommends that the personal health information of the first third party should not be released but that the second third party's business information should be subject to more extensive disclosure than that proposed by the public body.

If the head of the public body fails to deal with the recommendation within the thirty days, a deemed rejection rule would leave all kinds of questions. Does this then mean that the first third party's personal health information should be released? And does it mean that all of the second third party's business information should be released or only some of it? Who then decides what should and should not be released? Does the matter revert to the original decision made by the

To live by the worst-case scenario is to grant the terrorists their victory, without a shot having been fired.

Salman Rushdie, 2000

public body? Or does it mean that the Applicant's position is the correct one and that he/she should be provided with all of the information requested despite the fact that both the public body in the first instance and the ATIPP Commissioner have agreed that some of it, at least, is exempted from disclosure under the Act? A deemed acceptance rule is far more certain and straight forward. I would, respectfully, request the government to rethink this issue one more time and to resolve the matter in favour of a deemed acceptance rule. This is particularly so as most of the recommendations made by this office are accepted in full in any event.

Respectfully Submitted

Elaine Keenan Bengts
Information and Privacy Commissioner

Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.

Justice La Forest, 1998
(R. v. Dyment)