NUNAVUT

INFORMATION AND PRIVACY COMMISSIONER

ANNUAL REPORT

2001 - 2002

In Yellowknife: 867-669-0976 ♦ Toll free: 888-521-7088 ♦ Fax: 867-920-2511 ♦ E-mail: AtippComm@theedge.ca

NUNAVUT

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

October 17, 2002

Legislative Assembly of Nunavut
P.O. Bag 1200
Iqaluit, NU
X0A 0H0

Attention: Speaker of the Legislative Assembly

Dear Sir:

I have the honour to submit the second Annual Report of the Information and Privacy Commission of Nunavut to the Legislative Assembly for the period April 1, 2001 to March 31st, 2002.

Yours truly,

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner

In Yellowknife: 867-669-0976 ♦ Toll free: 888-521-7088 ♦ Fax: 867-920-2511 ♦ E-mail: AtippComm@theedge.ca

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

Even in our relatively isolated and quiet corner of the world, the events of September 11th, 2001 had an emotional and practical impact on our lives. Not only did we have to acknowledge that we are not immune from terrorist activity, we also learned that terrorists will think the unthinkable and will do the unbelievable to make their point. The reaction of governments in the western world was understandably 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. In the shadow of the horrific events of September 11th, governments were quick to sacrifice rights and freedoms to improve security. However, as noted by author Salman Rushdie, "To live by the worst-case scenario is to grant the terrorists their victory, without a shot having been fired." 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 fear of terrorism. While increased diligence and security is clearly a new priority, if this comes at the expense of our democratic rights, the terrorists may win indirectly what they could not win directly. In Nunavut, the effects of September 11th are somewhat remote. Except for tighter security and new taxes 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's stated goal is to promote 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 in a very new Territory and, with everything else that has had to be attended to, there was a bit of a slow start in getting everything in order. Again this year, progress has been made and more and more employees appear to be receiving some training in how the Act affects them in their jobs. I would encourage the Government of Nunavut to ensure that every new employee receives some basic information and training about the Act within the first few months of their employment. For the Act to work best, all employees of public bodies must be aware of the Act and the basics of its application.

This year was a busier one for the Information and Privacy Commissioner's Office than the last fiscal year, largely as a result of one persistent Applicant who made four separate

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

Requests for Review in the months of February and March of 2002. The heavier traffic has revealed some weaknesses in the ability of public agencies to handle the requests for information. I will make more comments and recommendations in this regard later in my report. I am somewhat concerned that some Requests for Information are not being answered fully or completely at the first instance and suffer from what appears to me to be an incomplete understanding of the Act on the part of those responding to the requests. That having been said, many of the guidelines provided in the Act require the exercise of discretion on the part of the public body when it comes to answering requests for information and it is my observation that for the most part 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.

I would again encourage all ATIPP Co-Ordinators to feel free to call my office to ask for direction and advice when needed. I am happy to discuss these matters and provide my input where I can.

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 would encourage the Government of Nunavut to continue to offer educational sessions for all government employees and to encourage all government employees to become familiar with the legislation and to implement rules with respect to the use of government communication mechanisms.

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.

With today's electronic recording and storing of information, people generally are becoming more and more concerned about how their personal 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 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 those entities are not subject to the protections of the ATIPP Act because they are not public bodies as defined in the Act.. 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 individu-

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

als had in mind when they purchased 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, Ontario 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 Nunvaut 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 Nunavut 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 borders except for those in the health sector. In 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 or territorial legislation is passed which is similar or substantially similar to the federal legislation in each individual Canadian jurisdiction. 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. How-

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

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

ever, as noted in my last Annual Report, however, the Federal Privacy Commissioner has taken the position that all of Nunavut (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 Nunavut 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 current law respecting the constitutional 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 is my hope to be able to invite my counterparts from across Canada to come to Nunavut for their annual meeting in the summer of 2004. The Information and Privacy Commissioners from the other provinces and territories have expressed an interest in seeing Nunavut and I would be proud and excited to host them in Iqaluit. To this end, I will be seeking a small amount of additional funding to allow me to host this annual meeting.

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.

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. The legislation came into effect on December 31st, 1996, prior to division and, of course, followed us to Nunavut on separation.

The Act provides the public with a means of gaining access to information in the possession of the Government of Nunavut 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. It does not appear that Nunavut has yet passed new regulations under the Act to designate the public bodies subject to the Act. As a result, the current law still applies only to those public bodies that were listed in the regulations as those regulations were made in the Northwest Territories prior to division. New regulations must be made as soon as possible to ensure the proper operation of the Act. The De-

[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 by 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

partment of the Executive's web page currently lists the names and contact numbers for 13 public bodies.

The Process

The Act provides that each public body subject to the Act is to appoint an ATIPP Co-ordinator to receive and process requests for information. Requests for information must be in writing 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. The right to access is subject to a number of exeptions, some of them mandatory and some of them discretionary. ATIPP Co-Ordinators are often called upon to use their discretion in determining whether or not to release the specific information requested and to interpret the Act in various ways.. 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

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

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 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 for 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 Nunavut Court of Justice.

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 leg-

Once again we are....confronted with the reality that bureaucrats like secrets — they always have; they will go to absurd lengths to keep secrets from the public and even from each other. Bureaucrats do not yet grasp the profound advance our democracy made with the passage, in 1983, of the *Access to Information Act*. They continue to resent and resist the intentional shift of power, which Parliament mandated, away from officials to citizens. A bureaucrat's dream of "reform" is to get back as much lost power over information as possible.

Hon. John M. Reid
Information Commissioner for Canada
Response to the Report of the Access to Information Review Task Force
September, 2002

slative and other government initiatives which affect access to information or the distribution of private personal information in the possession of a government agency.

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

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

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

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

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 Government Operations and Services 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. However, 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 cooperate 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 its 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.

The Information and Privacy Commissioner's Office received six new requests for review and one request for comment in 2000/01. One recommendation was made, and that recommendation was accepted by the head of the public body. One of the requests for review was closed without further action as it did not fall within the mandate given to the Information and Privacy Commissioner under the Act. The remaining requests, all received in the last quarter of the fiscal year, are still under investigation. The Department of Education and the Department of Health and Social Services were the two departments most often involved in Requests for Review.

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

One cannot assume, solely from the nature of the interview itself, that there was an expectation of confidentiality. There must be something more. For example, might there be some consequence to the person giving the opinion if not kept confidential? What is the nature of that possible consequence and how significant might that be to the individual? Would others refuse to give candid and forthright answers to questions posed if the responses are not kept confidential? Were the interviewees in a position of relative strength or weakness insofar as the applicant was concerned. For example, if the applicant actually got the job applied for, would she be in a position of superiority to the interviewee such that it could affect the interviewee's working relationship with the Applicant if the record were released?

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner,
Review Recommendation #02-003

IV. REVIEW RECOMMENDATIONS

Review Recommendation #02-003

This Request for Review came from an individual who had applied for a position with the Government of Nunavut but was, apparently, unsuccessful in her attempts. She felt that one or more of the references that had been given were negative and that that was what was preventing her from being successful in her application. She requested copies of any records which would reflect the opinions of the references consulted. The Department was reluctant to provide the Applicant with the information requested and relied on section 22 of the Act. Section 22 gives the public body discretion in deciding whether or not to release personal information that is evaluative or opinion material compiled solely for the purpose of determining the applicant's suitability, eligibility or qualifications for employment when the information has been provided to the public body, explicitly or implicitly, in confidence.

In reviewing the material in question, the Information and Privacy Commissioner concluded that the records requested did, indeed, contain personal information of both the Applicant and the reference and that the information was compiled solely for the purpose of determining the Applicant's suitability for a position of employment with the Government of Nunavut. However, she pointed out that she was not provided with any significant evidence that the information had been provided to the public body either explicitly or implicitly

in confidence. She indicated that more information was needed before she could come to that conclusion. In the result, the Commissioner recommended that the third parties who gave the opinions be consulted about whether or not they objected to the release of the information in question to the Applicant. If they did object, that would provide the public body with at least some evidence tht the information was given in confidence so as to provide them with good reason to exercise their discretion to refuse access. However, if there was no objection to the release of the information, and consent was given, the public body had no good reason to withhold access to the records.

The Recommendation was accepted.

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

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

V. 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 Standing Committee on Government Operations and Services. However, we have yet to see even the most basic of the recommended actions accomplished. For this reason, many of my recommendations for change are simply repeated from previous years.

As a priority, I continue to point out that the regulations which identify which public bodies are subject to the Act have not been amended since division. Many of the entities listed in the previously existing Northwest Territories Regulations no longer exist (as an example, the regional health boards, which were all listed in the Northwest Territories regulations, no longer exist). New entities have been created in Nunavut which did not exist prior to division and several public bodies have changed their names (Nunavut Housing Corporation would be one example). The number one priority insofar as this legislation is concerned is, to my mind, to list the public bodies which currently exist in Nunavut and to amend the regulations to reflect the reality of Nunavut today.

Another issue that I feel quite 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. Municipalities, particularly tax based mu-

nicipalities, gather and maintain significant information about individuals in their day to day dealing with the business of running communities. More and more often I hear of plans to "integrate" certain information systems so that information can be shared between Territorial and Municipal governments. Quite apart from whether or not information should be shared between levels of government, the concerns are magnified exponentially when the public body receiving the personal information does not have any legislated constraints on how and when the information is used . Such sharing of information without appropriate restrictions on the use of such material is irresponsible use of personal information. I encourage the Government of Nunavut to resist the urge to open up the avenues of data sharing.

I understand that the Department of Health and Social Services has made telehealth one of its priorities. Although the benefits of telehealth are undisputed, particularly in a place like Nunavut where the economies of scale will not justify the retention of full time specialist in all fields, the threat to the privacy of personal health information is significant. I understand that the Department is currently seeking a telehealth provider. I would strongly recommend that any foray into expanding the telehealth system in Nunavut makes privacy protection the number one priority of any such system. Failure to do so will put the health information of the people of Nunavut at serious risk of inadvertent disclosure to the detriment of all.

Still on the issue of health information, information technolo-

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"

gies are 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 businesses in the health sector are 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 consistency in approach and practice. Even if the government does not want to tackle generalized private sector legislation, I would strongly recommend that it does consider health sector legislation.

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 in general, and Nunavut in particular, 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.

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 add "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

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. My office has received a number of these kinds of complaints. 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 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 which must be dealt with in some manner by the public body involved.

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 Nunavut, 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 prop-

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

erty 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 further states, 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 infor-

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

mation gleaned from other sources in order to steal identities

This is not an outlandish or hypothetical threat. It has already happened in the United States where police in Ohio found and confiscated death certificates and social insurance cards for a large number of people, along with two CD-ROMs containing bulk lists that had been legitimately purchased from the Motor Vehicle Registry. The bulk lists were being used to assist the holders of this information in their identity theft business. 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.

Finally, I would take this opportunity to once again encourage the generalized training of all government employees and specialized training of ATIPP Co-Ordinators with respect to how to deal with Requests for Information. Several of the requests for Review received have arisen because the public body involved has not given a Request for Information the thorough and serious attention that the legislation requires. Requests should not be treated as a nuisance to be gotten rid of. They must be given the attention necessary to properly and fully answer the inquiry made. It is my sense that, in at least some cases, Requests for Information are given a very low priority and responses are made without the necessary review of the legislation to ensure that the request is being properly classified and dealt with. Many requests have been

made more difficult and time consuming because they have not been given the respect they should be given at the first instance.

In closing, I return to the one recommendation which I have made in each of my Annual Reports 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. 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. The Standing Committee has supported my recommendation but there appears to be reluctance on the part of government to accept the recommendation, preferring a "deemed rejection" rule. I am strongly against this approach as I believe it will cause far more mischief than the alternative. The best way 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 re-

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

fuses 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 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 re-

All Canadians cherish their "right" to get the facts on any subject and to get the truth when governments are suspected of rewarding friends, punishing enemies, putting self-interest above public interest or simply of using secrecy in paternalistic ways.

Hon. John M. Reid
Information Commissioner for Canada
Response to the Report of the Access to Information Review Task Force
September, 2002

solve the matter in favour of a deemed acceptance rule. This is the practical resolution of the issue as well because most of the recommendations made by this office are accepted in full in any event.

In conclusion, it appears that the people of Nunavut are becoming more aware of the provisions of the *Access to Information and Protection of Privacy Act* and are increasingly using it to seek information from government and to insist on the protection of their private personal information. It is important that the Government of Nunavut keep pace with the population and that some of the recommendations made in this and previous annual reports be addressed as soon as possible.

Respectfully Submitted

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner

Public interest in privacy protection has grown steadily over the past two decades, prompted by social, economic and technological change. The development of a global economy, proliferating computer networks, exponential growth in Internet transactions, satellite-based telecommunications, and sophisticated surveillance technologies all contributed to a general public uneasiness about eroding personal privacy.

Bruce Phillips
Former Privacy Commissioner of Canada
Annual Report
1999/2000