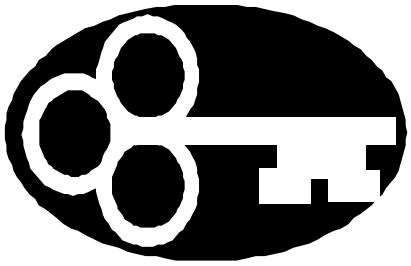

NUNAVUT

INFORMATION AND PRIVACY COMMISSIONER

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

ANNUAL REPORT OF THE INFORMATION AND PRIVACY COMMISSIONER OF NUNAVUT

I. COMMISSIONER'S MESSAGE

As suggested by the name of the Act, the *Access to Information and Protection of Privacy Act* of Nunavut has a dual purpose. The first is to afford access to government information by the general public and the second is to ensure that personal information held by government agencies about individuals is protected from unauthorized use or distribution.

The most visible part of the act is that which relates to the right of the general public to obtain information from the government relating to themselves and to the business of government generally. Openness encourages accountability and accountability is the cornerstone of free and democratic society. The newest government in Canada, that of Nunavut, has started its mandate on a stated commitment to openness in government. This is a lofty goal and, despite its apparent simplicity, is not so easy to follow in practice. It will require the ongoing commitment and encouragement of both elected and non-elected government officials to maintain that lofty goal. I am encouraged, thus far, with the enthusiasm with which this concept has been embraced.

The other aspect of this Act, however, is the protection of personal privacy. With the advent of new communications technologies and the ability to share information world wide without leaving the comfort of your chair, Canadians are becoming more and more aware of the need to protect their personal privacy and this issue will, without a doubt, become one of the more important political issues in the next decade. Government collects and uses a great deal of information about each and every one of us and it is important that all public bodies are vigilant about protecting that information. As

In the last thirty years, the idea that citizens should have a right of access to information held by public institutions has become firmly entrenched in most advanced democracies. This is evidenced by the rapid diffusion of freedom of information (FOI) laws that establish a right of access to information and explain how it may be exercised. In 1976, no Canadian government had an FOI law. By 1996, all but one of Canada's federal, provincial and territorial governments had adopted such laws.

Alasdair Roberts
"Retrenchment and Freedom of Information: Recent Experience Under Federal, Ontario and British Columbia

many larger businesses will tell you, protecting the private information of your clients is simply good business. The more technological advances allow the collection and sharing of information, the more important it will be to good business practices to protect that information. This is no different in the business of government than it is in any other business.

At the national level, the *Personal Information Protection and Electronic Documents Act* has been passed and comes into effect within the next few months. This legislation will provide guidelines and impose regulations with respect to the collection and use of personal information by private sector organizations. It will, in time, apply to any organization which collects personal information, either in printed or electronic form. Although neither the Territorial Government nor the private sector have yet taken much interest in this legislation, it will have significant impact in the way businesses collect and use personal information.

The protection of personal information is bound to be one of the "hot" political issues of the next decade. Many of the provinces are now looking at legislation which will address the protection of personal information in the private sector and I would encourage the Government of Nunavut to study the issue and consider similar legislation as well.

Because I was appointed only in October of 1999, there has not been a lot of activity under the Act as yet in terms of requests for review. However, I did visit Iqaluit in January and met with a number of government officials and the public to make my presence known. I have since developed a "consultative" relationship with a number of government departments and am encouraged to find that I am being

The paternalistic belief by many public officials that they know best, what and when to disclose to citizens, remains strong. At the very highest levels of the bureaucracy, the official line on ethics for public servants stresses their "servant" role (i.e. being unseen, unheard, obedient, unaccountable) rather than their "public" role (being accountable, professional, obedient to the law and the public interest). The notion of ministerial accountability is, too often, taken to mean that the public should not know what public servants do or advise their ministers to do.

Hon. John Reid. PC
Information Commissioner
Canada
1998/99 Annual Report

consulted by many public bodies at the beginning of the request process, rather than waiting to have the decisions referred to me because an applicant for information is unhappy with the result. It is also encouraging that my office is being consulted on a number of policy issues as well. I hope to be able to continue to work co-operatively with all public bodies to ensure that the goals of the Act are attained.

Freedom of information laws have proved to be useful instruments for improving public understanding of the policy-making process and protecting citizens against arbitrary decisions by public bodies. However, governments have often been ambivalent about recognizing a right of access to information. They have been motivated by fears that openness will discourage frankness among ministers and officials, compromise the ability to collect information from other organizations , and undermine regulatory and security functions. There are also less worthy concerns about openness, rooted in a desire to minimize accountability for ill-advised policy decisions and poor management.,

Alasdair Roberts
Retrenchment and Freedom of Information: Recent Experience under Federal, Ontario and British Columbia Law

For the Act to work, however, there must be a commitment to the purposes of the Act on the part of the government. Section one of the Act sets out its purposes:

1. The purposes of this Act are to make public bodies more accountable to the public and to protect personal privacy by

a) giving the public a right of access to records held by public bodies;
b) giving individuals a right of access to, and a right to request correction of, personal information about themselves held by public bodies;
c) specifying limited exceptions to the rights of access;
d) preventing the unauthorized collection, use or disclosure of personal information by public bodies; and
e) providing for an independent review of decisions made under this Act.

The effective working of the Act requires that there be a group of people within each public body who are not only aware of the Act, but who are also knowledgeable about its application. The Act contemplates that each public body will have an Access to Information and Protection of Privacy (ATIPP) co-ordinator. This person would be responsible for receiving and dealing with requests for information and for dealing with the Information and Privacy Commissioner when there is a

Request for Review. These employees would also have some special training to assist them in interpreting and applying the Act. To the best of my knowledge, these individuals have not yet been appointed and no training has yet been provided to them. This should be a priority for the government in the next year. Once the ATIPP co-ordinators have been appointed, I would be happy to provide some training and assistance in providing these people with the information they need to apply the Act.

Both rights —- the right to know and the right to privacy —- shift power in a very real sense from the state to the individual citizen. Each right is enriched through respect for the other.

Hon. John Reid, P.C.
Information Commissioner, Canada
1998/99 Annual Report

The other requirement of the Act is for the Government to produce a "Access to Information and Protection of Privacy Handbook". This, too, should be a priority for the use of the public.

For my part, one of my priorities in the coming year will be to produce a brochure and educational materials , and to develop a web page to help educate the general public of the existence of the Act and its purpose. I look forward to working with the people of Nunavut over the next four and a half years and to doing my part to help ensure that the government's commitment to open and accountable government remains strong.

Elaine Keenan Bengts

Information and Privacy Commissioner
Nunavut

II. INTRODUCTION

A. ACCESS TO INFORMATION

Background

The *Access to Information and Protection of Privacy (ATIPP)* Act was created to promote, uphold and protect access to the information that government creates and receives and to protect the privacy rights of individuals. The Act itself is identical to the *Access to Information and Protection of Privacy Act* of the Northwest Territories, which applied to all public bodies in the Northwest Territories and Nunavut prior to division. The Nunavut Act came into effect upon the creation of Nunavut on April 1st, 2000.

The Act provides the public with a means of gaining access to information in the possession of the Government of the Nunavut and a number of other governmental agencies. This right of access to information is limited by a number of exceptions. These exceptions function to protect individual privacy rights, and enhance the ability of 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.

Under *The Freedom of Information and Protection of Privacy Act*, disclosure is the rule, not the exception. In that the exceptions to access under the Act derogate from the thrust of the Act, they must be strictly and narrowly interpreted. Therefore, unless an access request falls squarely within one of the exceptions, the information must be disclosed. Where a discretionary exception applies, there should be a reason why the public body chooses to withhold, rather than release the record.

Barry E. Tuckett
Manitoba Provincial
Ombudsman
Annual Report

The Process

Each of the public bodies governed by the Act are required 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 ATIPP Co-Ordinator of 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.

A popular Government, without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy; or, perhaps, both. Knowledge will forever govern ignorance; and a people who mean to be their own governors must arm themselves with the power which knowledge gives.

James Madison
1822

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 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 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

As society has become more complex, governments have developed increasingly elaborate bureaucratic structures to deal with social problems. The more governmental power becomes diffused through administrative agencies, however, the less traditional forms of political accountability, such as elections and the principle of ministerial responsibility, are able to ensure that citizens retain effective control over those that govern them. … The over-arching purpose of access to information legislation, then, is to facilitate democracy.

Dagg v. Canada (Minister of Finance) Supreme Court of Canada

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 Minister involved. In the event that the person seeking information does not agree with the Minister's decision, 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 legislative and other government initiatives which effect access to information or the distribution of private personal information in the possession of a government agency.

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;

Control over our privacy in the information age is increasingly a pipe dream, because our information goes everywhere. We kind of shed it like skin wherever we move.

Dr. Roger Magnusson
1999

- 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 can and will receive privacy complaints and make 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 is both unlikely to happen except in extreme cases, and not very instructive. It is the hope of this Privacy Commissioner that the legislature will review these sections of the Act and provide the ATIPP Commissioner with specific authorization to review privacy complaints and to make recommendations where there are problems.

Perhaps the hardest dilemma of privacy is not just how much is optimal, or the ways in which 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

III. REQUESTS FOR REVIEW

Even where the Act is applicable, a public body should consider whether use of the Act is necessary. It is good administrative practice for a public body to have determined what records can be routinely disclosed without the need of the access to information procedure. The determination of that initial question saves time and resources for both the public and the public body in the long run.

Barry Tuckett
Manitoba Ombudsman
1998 Annual Report

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 the decision made by the public body. 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.

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 for Information and a copy of all responsive documents from the appropriate public body. Except where the issue is an extension of time, 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 most cases thus far, 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 may not always be necessary.

Because the ATIPP Commissioner was not appointed until October of 1999, there had, as of March 31, 2000, been no Requests for Review or Recommendations made under the Act. There have, however, been a number of discussions between the Commissioner and members of the public service about the requests which they have received for information and how they should be responded to. Although this office does not receive statistics with respect to when and how many initial request for information are received under the Act, it is clear that those requests are being made. The fact that this office has not yet received any requests to review a decision by a public body suggests that the requests are being handled effectively at the first level.

Canadian jurisprudence is consistent in holding that the general philosophy behind this type of legislation is full disclosure insofar as it relates to government documents. The provisions of the Act must be given a liberal and purposive construction. The legislation recognizes that there are legitimate privacy interests that must be respected but any exceptions to the rule of disclosure must be clearly delineated in the legislation.

Justice John Z. Vertes
Supreme Court, NWT
October 25, 1999
CBC and Selleck v. Commissioner of the NWT

V. OTHER MATTERS OF INTEREST

As ATIPP Commissioner, I traveled to Iqaluit in January and spent three days meeting with government employees and the general public. During this visit, I gave a number of government personnel an overview of the *Access to Information and Protection of Privacy Act*, and its application. I also had several meetings with government officials to discuss specific questions they had with respect to the Act. From this initial contact, I have been able to maintain contact with a number of agencies who deal on a day to day basis with personal information and who now feel comfortable in calling me to discuss concerns they have. It is my hope that any government agency which has a question about the Act

or how it is applied will feel welcome to call me for input.

While I was in Iqaluit, I also had the opportunity to host a public meeting and met and chatted with members of the public and government agencies alike who attended. I was also able to address a weekly meeting of the Rotary Club to talk to them a little bit about protection of personal information in the private sector and the federal *Personal Information Protection and Electronic Documents Act* which has been passed and comes into effect within the next few months.

It is my intention to spend time in Nunavut at least twice a year and during my visits I will be taking steps to educate both the government and the public about the Act and the issues that it raises.

I agree that the circumstances can implicitly give rise to a situation of confidentiality. The evidence on this appeal shows that, even though the department has no written rules as to confidentiality, its personnel operate under the assumption that information received from proposers is to be treated confidentially. Similarly, the proposers operate under the assumption that information conveyed to government in a proposal would be treated confidentially. There is a mutual understanding as to the usual practice.

Justice John Z. Vertes
Supreme Court , NWT
October 25, 1999
CBC and Selleck v. Commissioner of the NWT et al

VI. COMPLAINT TO THE FEDERAL PRIVACY COMMISSIONER

In late 1999, a final report was received from the Federal Privacy Commissioner with respect to a complaint made to the Privacy Commissioner for Canada by the Information and Privacy Commissioner of the Northwest Territories on behalf of a resident of the Northwest Territories (which then included Nunavut) who did not want to make the complaint herself. Although the complaint arose prior to division, the rationale for the resolution applies equally, if not more clearly, to Nunavut. The result of the investigation and complaint is contained in the Annual Report of the Federal Privacy Commissioner as follows:

> The Information and Privacy Commissioner for the Northwest Territories complained that Human Resources Development Canada (HRDC) was making improper disclosures of SINs by printing them on cheques for employment insurance benefits. Her contention was that recipients therefore cannot cash their cheques without revealing personal information to a financial institution or other cheque-cashing establishment.
>
> HRDC still prints the SIN on several kinds of cheques it issues. Of these, employment insurance cheques are the case for which the department offers perhaps its best argument. In this instance, as often in the past, HRDC explained its position as follows:
>
> - Given that the SIN was designed for employment insurance purposes in the first place, its use on employment insurance cheques is entirely appropriate and legitimate. Furthermore, the SIN is the official file number for the employment insurance program, and as such is an important element in establishing the identity of cheque recipients. Since many persons may have the same name, an employment insurance payment is actually issued not to a name, but rather to a SIN.
> - In cases where a cheque was lost or stolen, tracing it would be expensive and laborious without the SIN

Privacy concerns have figured prominently in the debate about SIN since its inception. Public resistance to SIN becoming a universal identifier, fortified by the Praliamentary review committee's recommendations in *Open and Shut* prompted the 1989 Treasury Board directive limiting federal government uses of SIN. Successive Privacy Commissioners have warned of the dangers of establishing any system of universal identification, be it a modified SIN or some other number.

Bruce Phillips
Privacy Commissioner of Canada
1999/2000 Annual Report

- As far as confidentiality is concerned, financial institutions already have responsibility for recording the confidential SIN for certain other transactions. Establishments other than financial institutions may not have similar SIN responsibilities, but on the other hand, people who have their cheques cashed at such alternative establishments do so by their own choice.

- Another good option available to recipients is having their cheques deposited directly to their bank accounts. Direct deposit obviates the need for any others to cast eyes upon the confidential SIN.

Even if it doesn't show through its envelope window, a Social Insurance Number (SIN) printed on a government-issued cheque does not stay hidden forever. Sooner or later the envelope gets opened, and the SIN becomes visible to people who really have no right to see it — notably, the people who cash the cheque.

Bruce Phillips
Privacy Commissioner for Canada
1999/2000 Annual Report

The Office sees some merit in the HRDC argument, particularly as it relates to the options generally available to cheque recipients. Financial institutions do indeed already have routine access to SIN, notably for transactions such as reporting income to Revenue Canada. Presumably, they also have safeguards in place for the protection of this personal information. Likewise, it is true that direct deposit may bring a greater measure of privacy.

However, when the Northwest Territories comes into the picture, the HRDC position weakens. In the many sparsely populated areas of Canada's North, financial institutions may be few and far between. Direct deposit or no direct deposit, its hard enough just to get to the bank. Many northerners have to rely on whatever alternative cheque cashing facilities may be available – the local general store, for example.

Such establishments may have attractions of their own, of course, but they are not known for the kind of anonymity that one often seeks in a financial institution. After all, it is one thing to have your SIN scanned by an unknown and indifferent bank teller, but quite another to be obliged to disclose personal information to a friend, relative, neighbor or local acquaintance.

The Office is please to announce that, as a result of discussion arising directly from this northern complaint, HRDC has softened its line. It has agreed to examine its use of social insurance numbers on the cheques it issues — not just for employment insurance, but for *all* of its programs. More concretely, the department has

already proposed to change its procedures so as to print not the whole SIN but rather only the last six digits on each cheque it issues.

Would six digits be enough for HRDC? Yes. The Department has conceded that six digits are all it really needs for most purposes of identification.

But would merely eliminating three digits of the SIN be enough to address the privacy issue? In good part, it would. For one thing, the six remaining digits would not be identified as part of a SIN, nor would they be recognizable as such. For another, no one, not even HRDC, could guess or recreate the complete SIN from the last six digits.

In short, both the federal commissioner and the territorial commissioner regard this proposal as a reasonable compromise. While acknowledging that the change may not be accomplished overnight, the Privacy Commissioner has assured his northern counterpart that he will monitor the progress of HRDC's undertaking.

Once again, the SIN was on the mind of many inquirers. This year's SIN-related inquiries exceeded even last year's total, which had burgeoned as a result of commentary by the Auditor General. In fact, more than 40 per cent of telephone inquiries in 1999/2000 related to the use of the SIN

Bruce Phillips
Privacy Commissioner
for Canada
1999/2000 Annual Report

VII. LOOKING AHEAD

Two matters, originating at the federal level, will demand the attention of the Government of Nunavut in the near future.

Bill C-6 is very much about protecting the right to be let alone. It is about ensuring a fair balance between the legitimate information needs of the private sector and the essential rights of individuals in a democracy. It is not the objective of the bill to impede business. The objective is to help create a state of mind in which business routinely considers client, customer and employee privacy rights in developing products and administrative practices. This will not happen overnight. But business depends on satisfied clients and customers. Its reputation is any company's most important asset, and no one will want to risk being singled out for willfully flouting the rights of individuals.

Bruce Phillips
Address to the Canadian Bar Association, Ontario

The first of these is the advent of the *Personal Information and Electronic Documents Act*, passed by the federal government this spring. This legislation was spurred by directives made by the European Economic Community with respect to the restriction of trade with jurisdictions which did not have safeguards in place for the protection of personal information.

The *Personal Information Protection and Electronic Documents Act* gives Canadians new legal rights when their personal information is collected, used or disclosed in the course of a commercial transaction. Beginning in one year, the Act will apply to federally regulated companies such as banks, communications companies and transportation companies as well as crown corporations. It will also apply to some interprovincial and international data transactions, particularly the buying, selling and leasing of customer lists and other personal data. In approximately five years, unless the Territorial Government has by that time passed its own legislation to deal with privacy protection in the private sector, it will apply to all organizations regulated by Territorial law. The law will apply to all personal information about an identifiable individual, regardless of the form in which that information exists with a few, very narrow exemptions. The Act will require all businesses and organizations which collect such personal information to comply with the CSA Code, which has nine points.

1. Accountability - organizations will be responsible for personal information in their possession and will have to designate one or more individuals to oversee individual privacy rights and compliance with the Act.

2. Identifying Purposes - the purpose for which

information is being collected must be determined before it is collected and that purpose must be disclosed to the individual from whom it is being collected. Before such information can be used for any other purpose, consent of the individual will be required.

3. Consent - Consent will be required for the collection, use or disclosure of any personal information and the purposes must be clearly stated and there must be a reasonable effort made by the organization to ensure that those purposes are understood. The nature and form of the consent will have to match the sensitivity of the information and the individual's reasonable expectations.

4. Limiting collection - The amount and type of information collected must be limited to what is necessary for the identified purposes.

5. Limiting Use, Disclosure and Retention - Personal information can only be used for the purposes it was originally collected, except with the consent of the individual involved. Personal information is to be retained only as long as necessary to fulfill the purpose identified.

6. Accuracy - There will be an onus on organizations to ensure that personal information is as complete, accurate and up to date as necessary for the required purpose, particularly where the information will be used to make decisions about an individual.

7. Safeguards - All personal information must be protected against loss, theft, unauthorized use or disclosure, copying or modification.

Information privacy is important for a number of reasons. First, it is related to a series of other rights and values such as liberty, freedom of expression and freedom of association. Without some control over our personal information, our ability to enjoy these rights may be hindered

Second, as more information about us becomes available, it is used in a wider variety of situations to make decisions about issues such as the kinds of services we are entitled to, the jobs we are qualified for and the benefits we may be eligible for. It is extremely important to have mechanisms in place to give us control over our own personal information and enable us to ensure that it is both accurate and relevant.

The Protection of Personal Information — Building Canada's Information Economy and Society
Industry Canada
Justice Canada
January, 1998

8. Openness - Organizations will be required to provide the public with general information about their data protection policies and practices.

9. Individual Access - Individuals must have access to personal information about themselves held by an organization and be given the opportunity to correct errors. Organizations will also be required to advise individuals how their information has been used.

The challenge facing Canadians is to find a balance between the needs of business for access to the information necessary for functioning in a knowledge-based economy and the rights of individuals to privacy and security of personal information. Collectively, we must ensure that technological innovations do not become intrusions on these economic needs and fundamental rights.

The Protection of Personal Information — Building Canada's Information Economy and Society
Industry Canada
Justice Canada
January, 1998

This is far reaching and important legislation made more necessary by the advent of new communications technologies and the ever increasing ability in a computerized world to share, link and use information in ways not even contemplated even fifteen years ago. It is an important first step and I would urge the Government of Nunavut to consider its own legislation to parallel the federal law.

The second federal initiative that will undoubtedly affect not only the Government of Nunavut, but also every individual living in Canada, is the proposal for the "Canada Health Infoway". Over the last few years, the federal, provincial and territorial governments have participated in discussions about the development of what will be, in essence, a national database for health information. There is much to be said for such a database in terms of reaching new heights of administrative efficiency, the sharing of knowledge and the effectiveness of the Health Care System. The biggest drawback to such a project is the unprecedented threat to the protection of the most personal and intimate of personal information. Those heading the discussions have recognized the concerns and have therefore met with all of the Information and Privacy Commissioners on two occasions to

discuss the issues and are working quite closely with the ATIPP Commissioners from some of the larger jurisdictions, some who have already dealt with the privacy implications of large health database systems (some successfully, others not so successfully). It is encouraging to note the importance that appears to be being put on the protection of personal privacy. The ATIPP Commissioner will continue to monitor this project and would be pleased to provide her comments to the Government of Nunavut as the project progresses.

Each federal, provincial and territorial jurisdiction now takes a different approach to privacy, with the result that the level of protection varies greatly across the country. At the same time, the level of security in hospital record offices and in physician's offices can leave much to be desired. Most people do not know how to obtain access to their records, while the rules governing how much of a person's file a health care professional or provider needs to see are often vague. A key foundation of the Canada Health Infoway will be the harmonization upward of provincial, territorial and federal privacy legislation for privacy protection in the health sector. Another will be the implementation of fair information practices and privacy-enhancing technologies throughout the health sector. "

Canada Health Infoway
Paths to Better Health
Final Report
February 1999

VIII. RECOMMENDATIONS FOR LEGISLATIVE IMPROVEMENTS

In the course of working with a new piece of legislation, such as the Access to Information and Protection of Privacy Act, certain deficiencies and problems come to light. Although I have just begun to work with the Nunavut Act, I have the benefit of having been the Information and Privacy Commissioner of the Northwest Territories for the last three

years and have therefore been able to observe some areas of the Act which could be improved with legislative amendments.

Because the Nunavut Act has not yet been extensively used, the amendments suggested today are very general suggestions which I believe would improve the effectiveness of the Act generally, rather than changes which I believe will make the Act more sensitive to the uniqueness of Nunavut. The latter kinds of changes will, undoubtedly, present themselves in time. For the present, however, I do feel that there are some changes which can and should be made to help make the Act more effective.

The Commission took this opportunity to remind government that it cannot treat the citizen's personal information as if it were its own. "This information characterizes and differentiates each of us; it is the property of individuals in the strictest sense of the word. Citizens entrust their personal information in good faith. They expect, and have right to expect, that it will be dealt with respectfully and only for the purpose for which it was collected.

Paul Andre Comeau
Commission d'access a l'information
Annual Report
1998/99

1. <u>Appointment of ATIPP Co-Ordinators and the Publication of an ATIPP Handbook.</u> In order for the Act to work effectively, there must be at lease one individual in each government department who has more than a mere passing knowledge of the ATIPP Act and its workings. The Act contemplates the appointment of ATIPP Co-ordinators for each department and this appointment process should be undertaken as soon as possible. Once these people are identified, appropriate training should be provided into the Act and how it should be applied. I would be happy to help with such training if it would be of assistance.

   In order for the general public to be able to use the Act, they must be aware of how to make a complaint. Section 70 of the Act also requires the Minister to

produce and update as required a directory containing a list of all public bodies which fall under the Act and the title and name of the person in each public body to whom requests for information should be sent or delivered. I would suggest that, in addition to this information, the directory should have a copy of the Act and the Regulations under the Act. The publication of this directory should be a priority.

2. <u>The acceptance of recommendations made.</u> One problem which has arisen many times in the Northwest Territories is that the recommendations made by the Information and Privacy Commissioner are languishing on the desks of the heads of the public bodies which are supposed to be dealing with them. The Act provides that the head of the public body is to deal with a recommendation of the ATIPP Commissioner within thirty days of it being made. That deadline has rarely been met in the Northwest Territories and, in one case, it was nearly a year from the date that the recommendation was made before the Applicant received a decision. This delay was the subject of a feature news report on the local CBC news show “North Beat” earlier this year. I would strongly recommend that an amendment be made to the legislation which would create a presumption that recommendations made by the ATIPP Commissioner be deemed to be accepted thirty days after the recommendation is made, unless, prior to that, the head of the public body issues a different decision. This puts the onus on

Opinion polls have repeatedly shown that, for a variety of reasons, public cynicism is rampant and faith in various levels of government is low. Yet those of us who have the opportunity to work closely with government organizations often see a different picture -one of hard-working people who do their best to live up to the meaning of "public service."
By releasing the information on which tough choices are based, government organizations can open a window on the decision-making process. Some people may well disagree with what government has done, but at least they will have a better understanding of why government has done it.

Dr. Ann Cavoukian
Information and Privacy Commissioner for Ontario

the head of the public body to meet the legislated deadline with consequences for failure to do so.

3. The "service" of documents. Many of the provisions in the Act provide for a thirty day notice period. Unfortunately, thirty days will not always give a party sufficient time to respond. For instance, in one recent incident , a document was sent to my office from Iqaluit by mail and date stamped the 2nd day of the month. It was received in my office in Yellowknife on the 28th of the month. That would have given the individual only 5 days to meet the 30 day deadline, rather than the 30 days contemplated. To ensure fairness, I would recommend that the legislation be changed to provide that all notices required under the act be delivered personally to the person, or be "served" in some other fashion which allows verification of the date of delivery, and that the thirty day reply periods begin only after "service" has been so effected. I believe that this is essential to fair process under the Act and would respectfully suggest that, whether or not the legislation is changed, that all government agencies covered by the Act should take steps to ensure that documents are actually received by the addressee before they begin to calculate the 30 days.

4. Privacy Complaints. Across Canada, Information and Privacy Commissioners are reporting that more and more of the complaints and inquiries being received are about privacy issues rather than access

Parliamentarians and Canadians instinctively know the truth of the position recently articulated by the Supreme Court of Canada: the access law is an indispensable tool for ensuring an accountable government and a healthy democracy. Parliamentarians and Canadians instinctively know that governments distrust openness and the tools which force openness upon them. Parliamentarians and Canadians instinctively know that they, not governments, bear the burden of keeping the right of access strong and up-to-date.

John Ried
Information Commissioner

to information. Although the Act provides that it is an offence for anyone to make use of personal information in a manner not consistent with the Act, it also provides protection from prosecution for government employees who release information "in good faith". There is no complaint mechanism which allows the ATIPP Commissioner to review a complaint of invasion of privacy or to make recommendations as a result. This ATIPP Commissioner has chosen to accept complaints of this nature and make recommendations, but there is no legislated authority for me to do so under the Act, nor would any public body be required to co-operate in such an investigation if they chose not to. As noted earlier, the protection of personal privacy is becoming a larger and larger issue and there really should be a mechanism in place to deal with such complaints other than prosecution, particularly where there has to be "bad will" involved in order to justify a prosecution.

....when it comes to response deadlines, the law needs teeth. There is a need for legal consequences when the right of access is undermined by means of delay. Delay is as grave a threat to the right of access as is document tampering or record destruction.

Hon. John M. Reid
Information Commissioner
Canada
Annual Report 1998/99

5. ATIPP Commissioner's Powers. The nature of this legislation and the subject matter of some requests for information, and human nature being what it is, there are bound to be some instances in which I will meet with some resistance from some public bodies in undertaking my investigations under the Act. Because of the manner in which the Act is drafted, the Information and Privacy Commissioner must rely on the good faith and co-operation of government agencies. This may not always

forthcoming and, because of the way that the Act is drafted, a public body would have no difficulty in being able to delay dealing with an application for significant periods of time. We have seen this happen in the Northwest Territories, where in at least one case, the reluctance of a public body to co-operate has resulted in delays of over a year. The ATIPP Commissioner is relatively powerless to compel compliance with requests in such circumstances. I recommend that the Act should be amended:

- to provide the ATIPP Commissioner with the power to subpoena documents and witnesses;
- to impose penalties for failure to comply with the time limits outlined in the Act or imposed by the Commissioner including the right to disallow fees otherwise payable by an applicant, and removing the right to invoke discretionary exemptions in the event of late responses;
- to withhold performance bonuses from heads and deputy heads of departments which consistently fail to meet deadlines.

Certain comments made by Justice J.Z. Vertes in CBC and Selleck v. Commissioner of the Northwest Territories et al referred to above bear some consideration as well. In that case, Justice Vertes stated:

Yet the Commissioner, while empowered to review,

Grounded in a 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, 1988
R. v. Dyment

can only make recommendations. The government is free to ignore those recommendations. The head of the public body may "make any other decision the head considers appropriate": s. 36(a). So, could it be that the legislature intended to create a position that performs inconsequential functions (irrespective of the expertise that the Commissioner may develop in analyzing and applying the Act)? I think a broader question to ask is whether an independent review can be at all meaningful if there is no enforcement power or where the results of that review bind no one.

....some children are spending hours online in "chat rooms," unaware of who they are talking to and the potential dangers to their safety and privacy. Some of these chat rooms ask children to provide personal information about themselves, such as their age, sex, telephone number, address, grade level, personal preferences, and a picture or physical description of themselves.

KIDSONLINE
Ontario Information and Privacy Commissioner's Office

This observation is one which has merit. If the Information and Privacy Commissioner is to demand the respect of a reluctant bureaucracy, the position must be given more significant powers. That does not necessarily mean that the ATIPP Commissioner needs the power to make binding orders. There must, however, be some authority given to the Office in order to encourage compliance with the Act and recommendations made under the Act and some real consequences for failing to do so.

6. Municipal Governments. In most jurisdictions, municipalities are included in the Act or have legislation which provides municipalities with rules with respect to both access to information and protection of privacy. In light of what appears to be a commitment in the Government of Nunavut to encourage open government, it would seem both appropriate and logical to include municipalities under the Act.

In Genesis, the Bible records that Adam and Eve were expelled from Eden because they had disobeyed God's instruction not to eat the fruit of the tree of knowledge of good and evil. They were made mortal and forced to provide for themselves, prevented by a flaming sword from ever returning to Eden

Whether we interpret Genesis literally or not, it describes the reality of our existence: that innocence, once lost, cannot be regained; that knowledge, once acquired, is never unlearned. Despite our efforts over the centuries, we cannot renounce that taste of the fruit of the tree of knowledge and return to Eden. We must make our own way in the larger world.

How we do so remains very much in our own hands

Hon. Perrin Beatty
President and CEO
Canadian Broadcasting Corp.
Lecture to the University of Western Ontario

7. Review of Public Bodies Subject to the Act. With the advent of Nunavut, many changes have been made to the way government is run and the different government agencies which exist. For example, the Regional Health Boards no longer exist. Furthermore, there is at least one instance in the Northwest Territories in which a government agency which really should fall under the Act (the Public Utilities Board) is not listed in the regulations so as to include it. It is my recommendation, therefore, that the Government of Nunavut should consider the regulations and and amendments made to reflect the realities of the Government of Nunavut as it has been established and all of the new agencies which have been established. This should be a priority to ensure that the public is able to access information and be satisfied that their personal privacy will be protected within these agencies.

8. Legislation with respect to Private Sector Privacy Standards. With the passage of the *Personal Information Protection and Electronic Documents Act* at the federal level, the Government of Nunavut will have to put its mind to the question of legislation at the Territorial level to ensure protection of privacy in the private sector. This is a golden opportunity to take the time necessary to create a "made in Nunavut" solution to the privacy issues that will inevitably be front and centre as a political issue over the next decade. I would strongly encourage the Government of Nunavut to look at passing its own legislation to deal with this issue.

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
Privacy Commissioner
Canada
1999/2000 Annual Report