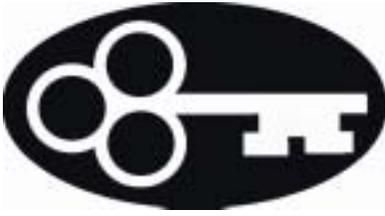




2003-2004 Annual
Report of the
Information & Privacy
Commissioner of
Nunavut



November 2004

Honourable Jobie Nutarak, MLA
Speaker of the Legislative Assembly of Nunavut
Legislative Assembly Building
Iqaluit, NU
X0A 0H0

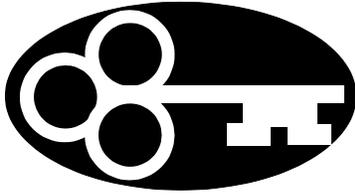
Dear Sir:

I have the honour to submit the Annual Report of the Information and Privacy Commissioner of Nunavut to the Legislative Assembly for the period April 1, 2003 to March 31, 2004.

Yours truly,

A handwritten signature in black ink, appearing to read 'E. Keenan Bengts', with a long horizontal line extending to the right.

Elaine Keenan Bengts
Information and Privacy Commissioner of Nunavut



The natural progress of things is for liberty to yield and government to gain ground. This is so because those who gain positions of power tend always to extend the bounds of it.

Thomas Jefferson

1. COMMISSIONER'S MESSAGE

Every year, new and interesting issues arise in my work as the Information and Privacy Commissioner for Nunavut. Fiscal 2003/2004 was no different. It was somewhat quieter in terms of the numbers of files opened but there were a number of issues that arose which invited inquiry and research and which drew me into discussions with government employees and with my counterparts throughout the country. The fact that there were fewer requests for me to review decisions made by public bodies was, I think, a function of two factors. The first was the filling of the position of Manager, Access to Information, which had been vacant for almost a year. The second factor was that one individual who made significant use of the Act in 2002/2003 did not make as many inquiries under the Act in the 2003/2004 fiscal year. With a small jurisdiction, one persistent individual can skew the "statistics" significantly. The large number of requests last year was a function of this phenomenon and I believe that this year's numbers are more indicative of the normal or expected number of inquiries.

The number of new files opened was down to 10 in 2003/2004 from 32 in the previous fiscal year. These included one request from the Legislative Assembly to provide comments on a legislative initiative, five Requests for Review, three requests that the Information and Privacy Commissioner lay a charge pursuant Section 59 of the *Access to Information and Protection of Privacy Act*, and one general file.

E

very citizen has the right to observe the operation of his or her government closely and personally. That right is the cornerstone of our great democracy. We can have no real freedom without openness in government.

Henry McMaster
Attorney General
South Carolina.

In addition to dealing with these files, I joined my fellow Information and Privacy Commissioners discussing issues of national import, such as the federal government's exploration of a mandatory National ID Card, the effect of the Patriot Act in the United States on the privacy of Canadians (particularly insofar as it relates to the contracting out of government initiatives to private sector companies with American affiliation), the Federal/Provincial Territorial Health Privacy Framework and video surveillance issues.

I have had the pleasure of being able to meet with Ms. Unger, the new Manager of Information and Privacy with the Government of Nunavut, when visiting in Iqaluit as well as when she was in Yellowknife on other business. I am pleased to report that we maintain a very good working relationship. I have also had the opportunity to meet with a number of the ATIPP Co-Ordinators and will continue to take whatever opportunities are presented to me to do so as I believe that the enforcement of the *Access to Information and Protection of Privacy Act* should, where possible, be involve open discussion and consultation. I was also able to meet with a number of the elected members of the Legislative Assembly of Nunavut while they were in Yellowknife last winter shortly after the election, to discuss issues about access to information and privacy.

I have been impressed with the increased level of training and education which appears to have been offered to the employees of the public service since Ms. Unger took up her

Striking a balance between the protection of privacy and the promotion of national security is one of the single most important issues facing our society today. This is an issue to be addressed by all jurisdictions across Canada.

Jennifer Stoddart
Information
Commissioner of
Canada

position. She has worked hard to ensure that each department has an ATIPP Co-Ordinator as well as a “back up” person who have all been trained with respect to the interpretation of the Act and this is a significant improvement from previous years. I know from my discussions with Ms. Ungar that access requests are being made by the public on a fairly regular basis. The fact that I am getting fewer Requests for Review suggests to me that the departments are doing a good job in answering the requests they receive for information at the first instance. When individuals get the information they seek from the department at the first instance, the work of the Information and Privacy Commissioner becomes much easier.

Although the more visible role of the Information and Privacy Commissioner is as an independent referee on access to information issues, it is also her role to be a watchdog with respect to personal privacy issues as well. I continue to be intrigued by and increasingly aware of the privacy aspects of the Information and Privacy Commissioner’s role. The concept of personal privacy is one that is increasingly difficult to preserve. Many things are contributing to the whirlwind of activity surrounding privacy issues. The fallout from September 11, 2001 continues to challenge governments to balance privacy rights with safety and security. Many initiatives which begin with good intentions either as government initiatives or as private sector initiatives have huge potential to burrow deeply into our privacy. One of the things currently being discussed on a national level is the implementation of standards for drivers licenses

We live in an age of technological miracles. The challenge we share is to use this incredible technology to serve us and our society without enslaving us.

Frank Work
Information and Privacy Commissioner of Alberta
2002/2003 Annual Report

throughout the country which might include the use of Radio Frequency Identification Devices (RFIDs). RFIDs are silicon chips about the size of a piece of rice with an antenna that can transmit data to a wireless receiver so that it can be read remotely. These RFIDs can contain a large amount of personal information, including names, addresses, dates of birth and perhaps other identifiers such as fingerprints or other biometric information. The desire of governments to make drivers licenses more uniform throughout the country is driven by security concerns and the need of law enforcement agencies to be able to verify identities. The privacy concerns, however, are numerous. For example, in a world where identity theft is the fastest growing criminal activity, once RFID's are fitted into a driver's license, anyone with a "reader" would be able to simply scan a crowd to obtain whatever information is contained on the individual's driver's licensee. Identity theft would become so much easier than it is even now. And just because a fingerprint is needed to obtain a drivers license does not mean that terrorists will be stopped at the counter. All of the terrorists involved in the September 11th bombings had legitimate US identification documents. In Spain, where residents are required to hold a National ID card, that requirement did not prevent terrorists from bombing a commuter train in that country. Although such technology may well succeed in more accurately identifying the law abiding public, whether or not these technologies will help in any way to prevent further terrorist activities bears careful consideration.



One of the key challenges for all governments in these turbulent times is the delicate balance of showing leadership on real issues of national importance while avoiding invoking major policies or initiatives without due consideration of the long term impact of these changes.

Ann Cavoukian
Information and
Privacy Commissioner
of Ontario

Annual Report
2002

Several Canadian provinces are also grappling with the wide reaching implications of the US Patriot Act, which was passed in response to 9/11. One of the provisions of this Act gives the American Government the right to demand any American company to hand over the records they hold containing the personal information in their possession, without warrant and with the specter of serious consequences for either failure to hand over the records or for advising the individuals involved that their information has been shared. This issue came to the forefront in Canada when the British Columbia government decided to contract out the responsibility for maintaining the medical records of British Columbians to the Canadian Branch of a wholly owned American company. The British Columbia Government Employee's Union raised an alarm, arguing that this put the personal medical records of Canadian Citizens at risk for mandatory disclosure to American officials. As a result of this concern, my counterpart in British Columbia is doing a major research project to determine how and when the Patriot Act will apply to American owned Canadian companies which will likely create a blueprint for all Canadian jurisdictions, including Nunavut.

Ever evolving and improving technology makes possible today what was considered pure science fiction less than ten years ago. From microchips the size of a piece of rice which can carry more information than first generation personal computers did twenty years ago, to cell phones capable of taking and transmitting digital pictures from almost anywhere,

To permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society....We must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy

Justice Gerald La Forest
Supreme Court of Canada

to GPS systems in vehicles which track you every where you go, technology continues to evolve. Most technology is aimed at making our lives easier. But for every positive use of such technology, more sinister uses can be, and often are, discovered. How much we will tolerate in terms of how our personal information is used. How much surveillance are we prepared to accept? Should the government or an employer be able to monitor our Internet use? Should foreign governments be able to demand our personal information in the name of their own security concerns and to keep and use that information without our knowledge and consent for any number of purposes? Should businesses be able to buy and sell our personal information to willing buyers without our permission? Is the right to market our product greater than the right to be free of e-mail spam or tele-marketing calls? Technology can undoubtedly make our lives easier, but we must be aware of what we are giving up in exchange for that convenience and government must keep up with changing technologies.

In Canada, the federal government and three provinces (British Columbia, Alberta and Quebec) have all passed legislation to regulate the protection of personal privacy in the private sector. At least two other provinces have legislation that specifically deals with the protection of privacy in the health sector, private and public. Three other provinces are considering private sector privacy information. This is an issue that will become more and more important as technologies continue to expand. Although we, in the North,

But privacy is not simply a frill or a selfish extravagance that can be tossed away the moment someone claims that it inhibits some other valuable social goal — regardless of whether the goal is security or public health or even individual life or death. Privacy is a cornerstone of individual freedom. It exists in a dynamic balance with our other social needs. The key to preserving privacy is careful analysis of any measure that purports to bring us some other social benefit, to ensure that the balance is maintained.

Robert Marleau
Interim Privacy
Commissioner of
Canada
Annual Report
2002-2003

are somewhat sheltered from some of the worst abuses of these technologies, we won't be sheltered forever. The North is, therefore, in the enviable position of having the luxury of time to examine what needs to be done to protect the public from identity thieves and overreaching surveillance. Private sector legislation is necessary and I encourage the Government to begin the process of drafting and implementing legislation to deal with these issues.

The erosion of privacy, particularly since 9/11 has been pronounced. At first, a concerned public encouraged harsh security measures, even with their tendencies to erode privacy. As the public begins to reflect on those erosions of their right to privacy, however, they become less willing to accept those kinds of measures without some concrete assurances that they are necessary to protect them from terrorism. This has become a hot political issue in the United States, for instance, where the Patriot Act has become an issue in the federal election. It is also becoming more and more of an issue with the Canadian public. It is estimated that one in every 100 Canadians will be the victim of identity theft of some description over the next two years. Identity theft is the fastest growing criminal activity in the world, costing both individuals and businesses hundreds of millions of dollars. These are not "southern" issues. They are very real issues for the people of Nunavut and it is important that the government take what steps it can to protect its citizens. How do we ensure that companies do not improperly share their customer's personal information? What can we do to

For the system to function most effectively, the consumer must be informed of their rights and empowered to use them. Every corporation that collects personal information is required to publicly disclose the contact information for their privacy officer. You can ask that person what information that company is collecting on you. The information integrity gauntlet has been thrown down - now the power is in the hands of the consumer.

And the responsibility.

John Wunderlich and
Carolyn L Burke
Globe and Mail

June 22, 2004

remind companies that they have to erase all data from their computers when disposing of old equipment? How do we impress upon the private sector that it is important to have appropriate security in place to ensure that only those who need to know will have access to their client's information? It is hoped that the federal government's answer to private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) can start to address the problem. I believe, however, that leaving this role to Ottawa will leave Nunavummiut exposed. Although the Federal Privacy Commissioner has jurisdiction to receive complaints from Nunavut, her office is far removed and not in touch with the people. I will continue to encourage the government of Nunavut to act as quickly as possible to address these issues.

I have been occasionally criticized over my tenure as Information and Privacy Commissioner for Nunavut for my lack of visibility and I acknowledge that I have found this to be a bit of a challenge. I have, however, taken steps to improve this situation and there are plans in the works to bring more attention to the office. I have a proposal before the Clerk of the Legislative Assembly for the creation of a web site in both English and Inuktitut. I would very much like to obtain approval for this project before the end of my term so that it can be up and running before the end of the year. This site will give the public more immediate contact with the Office of the Information and Privacy Commissioner. It will also help to more widely publish the Recommendations I make to public bodies so that both the public and the government can have

Is a passport any more "robust" than a driver's license as a confirmation of identity? The answer, unfortunately, is "not much".

There is a huge effort expended on designing and implementing a self-protecting identity token (driver's license, passport etc) and far too little effort on the validity of the actual identity, or on checking the legitimacy of the token.

It might also seem amusing that we regard the passport as the ultimate identity document, yet we're permitted to submit our application by mail.

What about biometrics, the catch-cry of the current decade? Biometrics is a very robust tool particularly in the case of fingerprint and iris recognition. Biometrics, however, won't identify anyone (despite the strident cries of the privacy police); it merely allows a strong link between a person and a previously established identity

David Heath
The Sydney Morning Herald
April 14, 2004

the guidance contained in those recommendations. It will also provide information about how to make a request for information or a request for review. It will contain information, as well, about national issues, and give guidance on protection of privacy in the public sector. I realize that the internet does not reach everyone, but it is a first and rather large step in the process of making the office more visible.

In addition to this initiative, I have invited a senior advisor in the Federal Privacy Commissioner's office to come to Nunavut to speak to the business sector about PIPEDA and privacy issues. She and I will be guest speakers at next spring's annual Meeting and Trade Show sponsored by the Nunavut Chamber of Commerce.

I have also invited my colleagues from across the country to come to Iqaluit for their annual meeting in the early summer of 2006 and that invitation has been accepted with enthusiasm. I would expect a lively exchange of information with some of the sessions being open to the public and I would hope to be able to prevail on my fellow Information and Privacy Commissioners to impart some of their wisdom in a public forum while they are there.

Finally, Ms. Unger and I have discussed the possibility of a joint effort to visit some of the smaller communities of Nunavut with general information sessions and public meetings. This initiative will depend largely on budgetary constraints, but I would hope that it could become a goal to visit one or two communities each year.

H

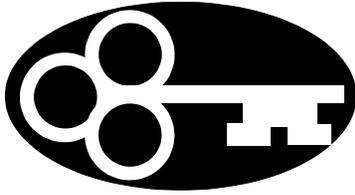
owever, at this point in our history, it is not clear how reducing the freedoms of all individuals in society will prevent further threats to public safety whether by terrorists on a political mission or for that matter, sex offenders acting on uncontrolled impulses.

But I can tell you that as we collect more information about more individuals we are increasing that possibility that people will be subjected to unnecessary scrutiny, that more people will be singled out, and that more people will be treated unfairly.

Jennifer Stoddart
Privacy Commissioner for
Canada
Address to Standing
Committee on Transport
and Communications

March 18, 2004

October, 2004 will mark the end of my five year appointment as Nunavut's first Information and Privacy Commissioner. I would be honoured to continue in the role, if that is the will of the Legislative Assembly. I would, however, like to take this opportunity to thank the people of Nunavut for allowing me the opportunity to play a small role in the development of this new territory. It has been entirely my pleasure and I hope that I have acquitted myself in a fashion that has helped to develop Nunavut's unique role in Canada.



An attitude of service to access requesters is the frame of mind the Access Act requires public servants to take in answering access requests. Parliament has made it an express obligation to create records from electronic databases if it is reasonably possible to do so. It is not open to public servants to dictate to access requesters the format in which they will receive access to government records.

Hon. John Reid
Information
Commissioner for
Canada
Annual Report 2003/2004

II. INTRODUCTION

A. ACCESS TO INFORMATION Background

The stated purpose of the *Access to Information and Protection of Privacy Act* as set out in section 1 of the Act, is to make public bodies more accountable to the public and to protect personal privacy. This can be a difficult task, because the Government, as a business, must be able to keep certain things to itself or it risks being taken advantage of in negotiating contracts and securing the best deal possible. The Act recognizes that the government does operate in a business world and tries to balance the right of the public to know with the ability of the government to compete fairly in the business aspects of its mandate. The general rule which has been applied to Access to Information legislation across the country is that openness is the rule and only narrow and specific exceptions apply and, where those exceptions do apply, they must be applied in the manner that provides the greatest amount of public access and scrutiny. The legislation also recognizes that government agencies hold considerable amounts of personal, private information about individuals which needs to be protected from improper use or disclosure. There is sometimes a fine balancing to be done in dealing with requests for information to weigh which records should be disclosed to the public against which records should be subject to the Act's exemptions. The spirit of openness suggested by the Act is clear. However, it is not always easy to apply the law to individual records. Simple common sense is an important and valuable resource in the interpretation of the Act. Each request for information

Distributed intelligence is everywhere, from the black boxes that record how we drive, to medical devices that log our tests for audit purposes. Increasingly, our movements are recorded in everything that we do, everything that we buy, everywhere that we go.

A century from now, will people consider privacy and other liberties enjoyed by their grandparents to be a curiosity, a museum exhibit? Have we lost sight of the right to be left alone? Or will we choose to design a world safe from those who want to wield the power of prying electronic devices?

Ian Kerr
Globe and Mail
January 12, 2004

must be dealt with on its own terms and the facts surrounding the particular information in question may well dictate when and in what circumstances records are protected from disclosure.

In Nunavut, the *Access to Information and Protection of Privacy Act* predated division. It came into effect in the Northwest Territories on December 31st, 1996 and became part of the law of Nunavut on division day.

The Act provides the public with a means of gaining access to records and information in the possession of the Government of Nunavut and a number of other governmental agencies, subject to the exceptions which are spelled out in the Act.

The exceptions function to protect individual privacy rights, and allow elected representatives to research and develop policy and the government to run the “business” of government. The Act also gives individuals the right to see and make corrections to information about themselves in the possession of a government body.

As at the end of fiscal 2004, no new regulations had been passed to designate which public bodies were subject to the Act. As at the date of the writing of this report, however, that deficiency appears to have been corrected as new regulations were published in the Gazette in June of this year, naming 15 public bodies subject to the Act.

The Department of the Executive and Intergovernmental Affairs’ web page now also lists names and contact numbers for, I believe, each of the public bodies subject to the Act so

Good records management is an essential pillar that supports the FOI process in Ontario. The public's statutory right to access government-held information cannot be fulfilled unless public servants properly document government programs and activities and maintain records in a well-organized manner.

A good records management system should enable a government institution to quickly locate and retrieve any requested records.

Excerpt from: Electronic Records and Document Management Systems: A New Tool for Enhancing the Public's Right to Access Government-Held Information?

Ontario Information and Privacy Commissioner's Office

July, 2003

that individuals requesting information can know who they should direct their inquiries to. It is also to be noted that there has been a marked improvement in the number of departments and other public bodies with ATIPP Co-ordinators appointed. Last year, I believe that there were only four Co-Ordinators in place. It now appears that each of the public bodies named in the new regulations have an ATIPP Co-Ordinator who is responsible for co-ordinating requests for information received. It does not appear, however, that the Government has yet published an Access Directory as required by section 70 of the Act. The information on the web page is a start, but not everyone has access to a computer or the Internet. There must still be a paper copy of this publication available to the public.

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 in both English and Inuktitut to facilitate such requests). Requests are submitted, along with the \$25.00 fee, to the appropriate public body. There is no fee if an individual is requesting his or her own personal information.

Once a request for information is received, the public body should identify all of the records which are responsive to the request and vet them with a view to disclosure. In vetting the records, the public body must endeavour to provide the

T

he 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
Dagg v. Minister of Finance
[1997] 148 DLR (4th) 385

applicant with as much of the requested information as possible, while at the same time respecting the limited exceptions to disclosure specified in the Act. Some of the exemptions from disclosure are mandatory and some of them 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 answering requests. The Public bodies must exercise their discretion to ensure a correct balance is struck between the applicant's general right of access to information and the possible exceptions to its disclosure under the Act.

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

The Role of the Information and Privacy Commissioner

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 Information and Privacy Commissioner is appointed by the Legislative Assembly but is otherwise independent of the government.

At times, being open and transparent may cause some discomfort for the government of the day – so be it. The need to allow for government decisions and actions to be publicly evaluated and openly assessed remains one of the keys to responsible government. We should have no less.

A successful access to information regime also opens the door to effective public participation in the democratic process. We often hear talk of the so-called “democratic deficit,” reflected in such things as decreasing voter turnouts for general elections. Providing the public with access to the information required to assess government actions is a means to reduce this deficit.

Ann Cavoukian
Ontario Information and
Privacy Commissioner

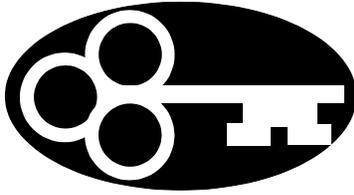
Annual Access and
Privacy Conference

October 7, 2004

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 powers given to the ATIPP Commissioner under the Act to resolve disputes are in the nature of those of an ombudsman. The Commissioner is mandated to conduct reviews of decisions of public bodies and to make recommendations to the “head” of the public body involved. In the case of a Department, the “head” is the minister. For other public bodies, the head will be determined in accordance with the regulations. The Information and Privacy 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 who must respond to a recommendation made by the Information and Privacy Commissioner within thirty (30) days of receipt of a recommendation. The head of the public body may chose to follow the recommendations made, reject them, or take some other steps based on the information in the recommendation. The decision must be in writing and must be provided to both the person who requested the review and the Information and Privacy Commissioner.

In the event that the person seeking information does not agree with the decision made by the head of the public body, that party has the right to appeal that decision to the Nunavut Court of Justice.



Society's willingness to accept diminished privacy for public safety purposes should not be misinterpreted. It doesn't mean people are any more willing than before to accept businesses misusing their personal information. Surveys have consistently shown high levels of consumer concern about privacy issues, which have thus far impeded the growth of electronic commerce. The need for business to respect customer privacy will not be diminished by this tragedy. Do not make the mistake of confusing one with the other.

Excerpt from: Public Safety is Paramount - But Balanced Against Privacy

Ann Cavoukian
Ontario Information and Privacy Commissioner

September 21, 2001

B. PROTECTION OF PRIVACY

The *Access to Information and Protection of Privacy Act* also provides rules with respect to the collection, use and disclosure of personal information by government 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.

The closer the information is to one's "biographical core" such as information about one's health, genetic characteristics, sexual orientation, employment, social or religious views, friendships and associations — the greater is the obligation on government to respect and protect the individual's privacy

David Loukedelis
British Columbia
Information and Privacy
Commissioner
"Privacy and the USA
Patriot Act"
October 2004

- 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 clearly reserved for extreme cases, and is not very instructive in terms of how to deal with the day to day handling of the masses of personal information which the government has in its possession. 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 co-operate with the Information and Privacy Commissioner. The ever increasing amounts of information collected and retained by government, the amount of outsourcing which governments now do, and the evolution of technologies which allow easy data matching and sharing

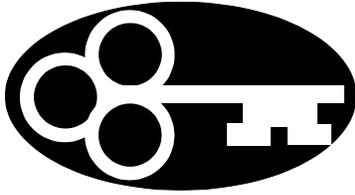
W

hen records documenting the actions, decisions and considerations of public officials are not created; when such records are created but are not included in an indexed institutional system of records or when the disposition or archiving of records is left to the unguided whim of the records creator, then there can no longer be an effective right of access to information no matter how strong the words of the law may be.

**Hon. John Reid
Information
Commissioner of
Canada**

**Excerpt from Address to
the Second International
Conference of
Information
Commissioners —
Mechanisms of
Accountability and the
Democratic Deficit
Cape Town, South Africa**

make it all the more important that there be an independent review process. I renew my recommendation that the privacy provisions of the *Access to Information and Protection of Privacy Act* be amended to allow for the Information and Privacy Commissioner, or some other oversight body to review processes, assess privacy practices and make recommendations on how to avoid unintentional and inadvertent disclosures of personal information.



Overall, most studies indicate that CCTV's (Closed Circuit Televisions) are not an effective means for reducing crime. CCTVs are effective at reducing incidents of burglary and property crime, but they are not effective against personal crime, violent crime or public disorder. A report released by NARCO (National Association for the Care and Resettlement of Offenders) states that CCTVs result in a 5% reduction in crime whereas better street lighting results in a 20% reduction in crime. These figures are fairly consistent throughout most CCTV studies

Literature Review on Issues of Privacy and Surveillance Affecting Social Behaviour

Stephen Greenhalgh, MA, MLIS
August, 2003

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 personal information by a public body, may apply to the Information and Privacy Commissioner for a review of that decision. This includes decisions about the disclosure of records, corrections to personal information, time extensions and fees. The purpose of this process is to ensure an impartial avenue for review and independent oversight of discretionary and other decisions made under the Act.

A Request for Review must be made in writing to the Information and Privacy Commissioner's Office. This request must be made within 30 days of a decision by a public body in respect to a request for information. There is no fee for a Request for Review.

When the Information and Privacy Commissioner receives a Request for Review, she will take steps to determine what records are involved and obtain an explanation from the public body. In most cases, the Commissioner will obtain a copy of the Applicant's original request for information and a copy of all responsive documents from the public body involved and will review the records in dispute. In some cases, it may be necessary for the Information and Privacy Commissioner to attend the government office to physically examine the public body's file. Generally, an attempt will first be made by the Commissioner's Office to mediate a solution

The right to remain anonymous (leaving no trace to one's identity) is something we have sought to maintain as a fundamental element in defending our private space. At best, we should only have to identify ourselves to government or business when knowledge of our identity is essential to concluding a particular transaction. It would not normally be essential when we are merely seeking information. Otherwise, we should be able to choose whether or not to reveal our identity. This is true as much in the electronic world as in the physical world.

John Woulds
Former UK Deputy Data Protection Commissioner as quoted in David H. Flaherty, "Defending the Right to Anonymity", a paper delivered at "Frontiers of Privacy", Victoria, BC (Feb 13, 2003)

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

The Information and Privacy Commissioner's Office received five (5) new requests for review in fiscal 2003/2004. This is down considerably from the 23 requests received in /2003. It is to be noted that almost all of the requests received in 2002/2003 were received from the same individual, which makes comparison somewhat academic.

Four review recommendation were made in fiscal 2003/2004, the same number as were made in the previous year. The Information and Privacy Commissioner was also able to resolve another request without having to make recommendations after discussion with the parties involved.

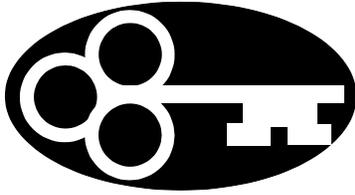
Of the new requests received in 2003/2004, one was with the Department of Health and Social Services, one involved the Department of Sustainable Development. The Departments of Education, Justice and Finance were also each involved in one Request for Review application.

In my last Annual Report, there was some concern expressed about the fact that several of the Requests for Review arose out of the public body's failure to respond to a request within the time provided for in the Act. This has not been a factor

in 2004 and not one of the requests received by the Information and Privacy Commissioner's Office was as a result of delay on the part of the public body.

The ability to manage and effectively use information is a core skill that needs to be at the centre of any public sector education and training strategy.

Hon. John Reid
Information Commissioner of Canada
Annual Report 2002/2003



The topic of information management may not seem – at first – to have much sex appeal. But we all should be passionate about it, because on it hinges our very ability as democratic societies to have good and accountable government. It is one of the first steps to dealing with the "democratic deficit" in any jurisdiction.

**Hon. John Reid
Information Commissioner
of Canada**

**Excerpt from Address to
the Second International
Conference of Information
Commissioners —
Mechanisms of
Accountability and the
Democratic Deficit
Cape Town, South Africa**

IV. REVIEW RECOMMENDATIONS

Review Recommendations #03-08

In this request, a company who had unsuccessfully bid on a proposal to the Department of Health and Social Services for the provision of Air Ambulance Medivac Services in the Baffin Region requested copies of the contracts which were eventually entered into with the successful bidders. The Department refused to disclose the contracts. One of the third parties was also involved in the review process, and they objected to the disclosure of the contracts.

The Applicant argued that he was not asking for information regarding any Third Party's costs of doing business or trade secrets. He did, however, feel that he was entitled to know what the government, and ultimately the taxpayer, was paying for the services provided under the contract.

Both the public body and the Third Party relied on section 24(2) of the Act which prohibits the disclosure of records where that disclosure would reveal a third party's trade secrets, financial or commercial information or where the disclosure might interfere with the third party's competitive position.

The Information and Privacy Commissioner reviewed the contracts in detail and determined that much of the body of each of the contracts was the "standard form" which most government agencies use in contracting with private parties. Some of the information in each contract was drawn directly

U

nfortunately, the Department has not made any real effort in this case to explain why they have taken the position they have with respect to this Application for Information. They have simply stated as a given that the disclosure of the contracts in question would put the Applicant, who is a direct competitor of the Third Parties who currently hold the contracts which are the subject of this Application for Information, in an advantageous position in future competitions "by knowing their competitor's operational and pricing structure". I would simply comment at this juncture that very little about the application and interpretation of the *Access to Information and Protection of Privacy Act* is that obvious. Application of the Act and, in particular, section 24, requires a careful review of the provisions of the Act and a knowledgeable application of the concepts articulated in the legislation. If a public body refuses to provide records requested, they must be prepared to defend their decision and to provide a detailed explanation as to the reasoning behind their thinking.

Elaine Keenan Bengts
Nunavut Information and
Privacy Commissioner
Review Recommendation #03-08

from the Request for Proposals which each of the proponents would have received before making their proposals and so was public information in any event. In fact, the only sensitive information in any of the contracts was contained in the appendices. The Privacy Commissioner recommended that the contracts be disclosed, subject to the severance of certain information which was exempted from disclosure pursuant to section 24 of the Act. The public body accepted the recommendations made.

Review Recommendation #03-09

In this case, the Applicant sought from an individual employed with the Government of the Northwest Territories, a copy of all correspondence that existed between the employee and each of :

the Department of Education
the Department of Human Resources
the Federation of Nunavut Teachers, and
Risk Management

The request was responded to by the Department of Human Resources and forty one pages of records were provided, some of which had some sections severed before they were provided to the Applicant. The Applicant asked that I review the Department's refusal to provide unedited copies of the records in question. The Department took the position that those parts of the records which were severed were not responsive to the Applicant's request for information and did not relate to him personally.

Specifically, the record requested is the names only, without other personal information relating to the petitioners. In this case, however, the names do not appear alone but in the context of having signed a petition requesting a review of municipal practices. Disclosure of the names would reveal the fact that identifiable individuals signed the petition, which is other personal information about the petitioners.

Ontario Information and Privacy Commissioner's Office.
Order 171 (Appeal 890023) concerning the Ministry of Municipal Affairs

The Information and Privacy Commissioner reviewed the records in question and agreed with the department. She recommended that no further steps need be taken by the public body. The recommendation was accepted.

Review Recommendations 03-10

This matter arose out of a request made to the Department of Sustainable Development for access to specific information relating to complaints made to the department against a corporate entity and a specified individual. The company and the individual were both from a fairly small community and apparently had received some government contract in the community. Complaints had apparently been made to the department about the way in which the contracts were being undertaken and the company and the individual and the company wanted to know what the complaints were and who had made them. The public body identified 43 pages of records responsive to the request, but withheld the production of some of them and severed portions of others before disclosing them to the Applicant. The only issue that the Applicants really wanted to have addressed was whether they were entitled to know who had made the complaints.

The public body took the position that the names of the third parties was personal information, the disclosure of which would be an unreasonable invasion of the third parties. The Applicant, on the other hand, argued that in order for the presumption of unreasonable invasion of privacy to arise, the

Section 3(1) provides that the Act applies to “all records in the custody **or under the control** of a public body” (emphasis added). The Department of Sustainable Development is a public body and it has some control over the records held by KPID, at least insofar as those records relate to monies disbursed on behalf of the Government of Nunavut. Reading the policy as a whole, it is clear that the Department felt that it was necessary to retain a degree of control over how public monies were spent through the vehicle of KPID, to the extent that a designated official from the Department was given a position on the Board and Executive of KPID. KPID has the contractual obligation to the Department to be accountable and to report to the Department. The Department has some role in the decisions made by KPID.

Elaine Keenan Bengts
Nunavut Information and
Privacy Commissioner
Review Recommendation
#03-11

name of the individual had to appear in conjunction with other personal information about the individual in order to be protected from disclosure and that the disclosure of the names alone could not be considered to be unreasonable.

The Information and Privacy Commissioner found that the disclosure of the names of the third parties who made the complaints would, in fact, be an unreasonable invasion of the third party’s privacy because it revealed not only their name, but the fact that they had made a complaint about the Applicants. She recommended that the names not be disclosed. This recommendation was accepted.

Review Recommendation #03-11

This Request for Review came from two individuals who were in a dispute with the Department of Sustainable Development and were attempting to obtain access to information held by that department about them personally and about their company. They were unhappy with the information received because they knew of other records in which they or their company had been mentioned. Those records, however, were apparently in the possession of a third party company known as Kivalliq Partners in Development (KPD). This is not a public body, but the Applicants argued that the partnership between the government of Nunavut and the KPD was such that the government could require KPD to disclose the documents requested. The public body’s failure to even ask KPD to provide the requested disclosure, they said, was in contravention of the Act because KPD’s records were “in the

It is imperative that institutions keep a record of the use and disclosure of personal information under their control. Except in limited circumstances, individuals have the right to know which documents containing their personal information are set to whom and when they are disclosed.

Robert Marleau
Interim Privacy
Commissioner of
Canada
Annual Report 2002/2003

possession or control” of the public body by virtue of the agency relationship between KPD and the public body. The Information and Privacy Commissioner explored the relationship between KPD and the public body and concluded that KPD was not a public body as defined in the *Access to Information and Protection of Privacy Act*. She went on to observe, however, that the Act applied to all records in the custody of or under the control of the public body and that the accountability provisions of the agreement between KPD and the public body provided the public body with the right to demand that KPD produce a good number of records. In those circumstances, the Information and Privacy Commissioner made two recommendations:

1. That the public body in this case should work with the Applicants to assist them in getting the information they were seeking from KPD
2. That the public body include in its partnership policy and in its contribution agreements the contractual obligation on the private partners to be subject to the provisions of the *Access to Information and Protection of Privacy Act* in order to ensure that the public’s personal information is afforded the protection of the Act.

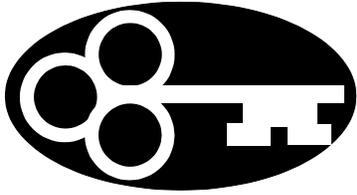
The first of the two recommendations was accepted and the Department agreed to work with the Applicant to obtain the requested information. The head of the public body, however, reserved a final decision with respect to including a

More broadly, excessive surveillance in the name of national security and public safety can threaten the freedoms on which every successful democracy depends. Awareness of widespread surveillance makes people nervous about speaking their minds, engaging in political activities, or doing anything that might arouse ill-founded or vague suspicion. Excessive surveillance herds people toward conformity and discourages the diversity of ideas and beliefs that are indispensable to the flourishing of our communities.

David Loukedelis
BC Information and
Privacy Commissioner

Excerpt from : Privacy
and the USA Patriot Act:
Implications for British
Columbia Public Sector
Outsourcing

provision in contracts with non-governmental partners with respect to access and privacy. The Minister responsible for the Department of Sustainable Development undertook to make every effort to ensure that future contribution agreements relating to the delivery of government program dollars by third parties include a provision to bind the third parties to the provisions of the Access to Information and Protection of Privacy Act. However, the Minister was reluctant to change its current policies to also require that such a provision must be included in every such contract. He felt, instead that the issue should be dealt with on a case by case basis.



In a democracy, the people are vested with ultimate decision-making authority, which they delegate to elected representatives and other public servants. Except in very limited and specific circumstances, public officials should conduct their business in open, not in secret, and ensure that the people to whom they are accountable - the public - are given proper notice of all meetings.

Making Municipal Government More Accountable - The Need for an Open Meetings Law in Ontario
Office of the Ontario Information and Privacy Commissioner
Oct 2003

VIII. RECOMMENDATIONS

Clearly, accountable government depends on the ability of the public to know what goes on in government. 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. There has been some progress this year in implementing some of those recommendations. Most of them, however, have not been acted upon. For the most part, therefore, my recommendations will follow along the same lines as those of previous years.

1. I recommend that the Government of Nunavut immediately direct the preparation and publication of an "Access and Privacy Directory" as required by section 70 of the Act . Once published, the Directory should be made available, either at no cost or for a nominal fee, to the public. Further, the Directory should be available for review by the public at government offices throughout the Territory. The Directory should also be made available on line on the Government's web page in such a manner as to be easily found and visible.
2. It appears that a list of the public bodies subject to the Act has now been created by regulation. This is a very positive step and I commend the government for its action in this regard. I would recommend that this list be reviewed on an ongoing basis to ensure that it

Change must come from the ranks of the most senior public servants and from the political level itself. The best guarantee of that change is greater access by the public, the media, non-government organizations, and others to information that enables them to scrutinize the workings of government and hold public servants and politicians accountable.

Hon. John Reid
Information
Commissioner of
Canada
Annual Report
2002/2003

remains relevant as the Government continues to mature and expand.

3. I would continue to encourage the Government to support ongoing training for those individuals who are responsible for Access to Information matters within their own departments and to ensure that all government employees are aware of their basic responsibilities to the public when dealing with personal information and access requests. All employees should know who the ATIPP Co-Ordinator for their department is and where they should turn if they have any questions. Much progress has been made in this regard with the hiring of Linda Unger in the position of Manager of Information and Privacy and I would encourage the government to continue to support her efforts in this regard. I would like to see a component dealing with Information and Privacy issues as a mandatory part of the initiation process with all new employees.
4. It is important that those who are given the responsibility to deal with Access to Information Requests in each public body are given the time to do their jobs properly. While I appreciate that it would be impractical to hire someone in each department to do only ATIPP work on a full time basis, it is important to give those who are assigned the work of the ATIPP Co-Ordinator sufficient time to undertake the task. That will likely be more time in some departments which are

Ten centuries ago, at the previous millennium, a Viking lord commanded the rising tide to retreat. No deluded fool, King Canute aimed in this way to teach flatterers a lesson -- that even sovereign rulers cannot halt inexorable change.

A thousand years later, we face tides of technology-driven transformation that seem bound only to accelerate. Waves of innovation may liberate human civilization, or disrupt it, more than anything since glass lenses and movable type. Critical decisions during the next few years -- about research, investment, law and lifestyle -- may determine what kind of civilization our children inherit. Especially problematic are many information-related technologies that loom on the near horizon -- technologies that may foster tyranny, or else empower citizenship in a true global village.

David Brin
Aug. 3, 2004

likely, by their nature, to get more requests for information, such as Human Resources, Health and Social Services and Education, than in other departments. It is important, however, that there be consideration given to this issue when determining manpower needs. It is a matter of recognizing, as part of the government's "corporate culture" that ATIPP issues are important and have some priority.

5. As noted in previous Annual Reports and in my report to the Standing Committee I have long been a proponent of including municipalities as "public bodies" under the Act or that new legislation be created to make rules and regulations for municipalities with respect to both access to information and protection of personal privacy. Not only is it important that municipal authorities be accountable to the public, it is also clear that municipalities, particularly tax based municipalities, gather and maintain significant information about individuals in their day to day dealing with the business of running communities. In the last year, I have received several inquiries from or on behalf of Nunavut municipalities about how certain issues should be dealt with. This leads me to believe that they are concerned about the issues and are looking for guidance. I would again encourage the government to consider including municipalities under access to information and protection of privacy legislation in some form.



However, many of the disclosures [of publicly available records] were practices developed at a time when the predominance of paper records provided a practical protection for personal information. It was just too difficult for any but the most determined to locate and copy personal information, which was held in many different locations. The value of “practical obscurity” has been eroded by computerization, and so disclosure now takes place in an entirely new context. This new context, in my view, necessitates a review of government practices in the sale of personal information.

Excerpt from: *Balancing Access and Privacy: How Publicly Available Personal Information in Handled in Ontario, Canada*

Ann Cavoukian
Information and Privacy
Commissioner for
Ontario

October, 2000

6. On the same theme, several issues have come up this year which involved private entities who administer or undertake public functions on contract with the Government of Nunavut. There does not appear to be any recognition, at least in the contracts which I have had the opportunity to review, that those private companies have any obligation either to allow the public access to their records or to adhere to the privacy provision of the *Access to Information and Protection of Privacy Act*. As more and more “public” functions are contracted to private industry, it is important that provisions be inserted into contractual documents that require the private organizations to comply with requests for information and to ensure that personal information is properly gathered, used and disclosed in accordance with the principles set out in the Act. Access and privacy clauses should be standard fare in outsourcing contracts.
7. I continue to feel that Nunavut should be taking steps to create “made in the north” legislation to deal with the protection of personal information in the private sector, rather than leaving this field to the federal government and the federal Privacy Commissioner’s office. This is particularly a concern in the health sector. Health care is not only a public sector service. There are many private sector businesses (and I stress the word “businesses”) which receive and hold very sensitive personal information, from dentists and chiropractors, to pharmacists and private laboratories.

The public's demand for greater accountability is getting stronger and "trust me" is just not good enough; either for shareholders who demand accountability from their corporate directors, or for citizens who expect good governance at all levels.

For government, transparency is a key requirement to achieve accountability.

Integrity will always be an issue unless we have rules for transparency that are clearly understood and consistently adhered to.

Dr. Ann Cavoukian and
Tom Mitchinson
Oct. 14, 2003.

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.

8. I repeat my assertion that this government should consider generalized privacy legislation over private sector businesses. As noted at the beginning of this report, technological advancements, easy access to databases, the free wheeling and unrestricted ability of companies to buy and sell personal information, and the increasing reliance of both businesses and the public on computers means that our personal information is at greater risk than ever. Businesses need information and guidelines and, in some cases, the rule of law, to regulate the use they make of personal information. The public needs legislation it can rely on to help them avoid the escalating costs of identity theft. Although the *Personal Information*

Governments make skeptics of Information Commissioners. Time after time, regime after regime, scandal after scandal, government leaders raise expectations by promising to be more accountable and transparent. Just as routinely, governments maintain their deep addiction to secrecy, spin, foot-dragging and decision making by nods and winks. When it comes to honouring the public's "right to know", governments have found it profoundly challenging to "walk the walk".

John Reid
Information Commissioner
of Canada
Annual Report 2003/2004

Protection and Electronic Documents Act applies to the private sector throughout Canada effective January 1st, 2004, it is legislation administered by the Privacy Commissioner in Ottawa and is quite limited in its ability to deal with some of the smaller, more localized issues. Private sector privacy legislation is absolutely necessary for Nunavut to be able to continue to do business with the world. I believe that legitimate and ethical business would welcome such guidance and I would encourage the Government of Nunavut to make private sector privacy legislation a priority.

9. More emphasis must be placed on the "protection of privacy" provisions of the *Access to Information and Protection of Privacy Act*. 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 Information and Privacy Commissioner to investigate or provide recommendations when there is a complaint that an individual's privacy rights have been breached. From time to time I do receive these kinds of complaints and I have reviewed them the best I can, but without any specific authority in the Act to do so. There is 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

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.

Benjamin Franklin

breaches of privacy under the Act and I would recommend, once again, that the specific authority be given to the Information and Privacy 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.

When I made my last report to the Standing Committee on Government Operations and Services, I emphasized the need for a “corporate culture” which respects the goals of the Act. I see in Nunavut a commitment to openness. I see in Nunavut’s leadership and elected officials a belief in the principles embodied by the Act. I see in Nunavut’s public service a sincerity in their desire to ensure that the objectives of the Act are met. This is the corporate culture which I referred to. As Information and Privacy Commissioner, I am encouraged by this attitude. My strongest recommendation would be to continue to foster this corporate culture. It is sometimes difficult to do. The balance between openness and the protection of personal privacy is difficult to maintain and the line is sometimes difficult to discern. However, as long as the leadership at both the political and the bureaucratic levels remain committed to the principles of the Act, its long term objectives will be achieved.

Respectfully submitted

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner