

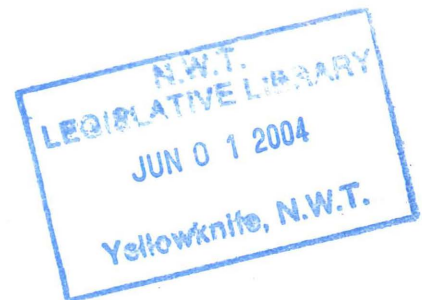


**NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER**

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

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

ANNUAL REPORT 2002/2003





**NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER**

April 26, 2004

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

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

Attention: Tim Mercer
Clerk of the Legislative Assembly

Dear Sir:

I have the honour to submit my annual report to the Legislative Assembly of the Northwest Territories for the period from April 1st, 2002 to March 31st, 2003.

Yours very truly

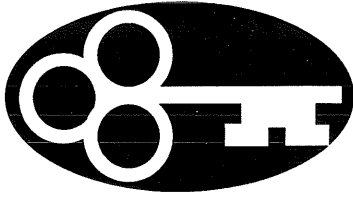
Elaine Keenan Bengts
Information and Privacy Commissioner
Northwest Territories



**NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER**

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

Commissioner's Message



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.

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

I. COMMISSIONER'S MESSAGE

As Information and Privacy Commissioner for the Northwest Territories, I continue to face new challenges every year and this fiscal year was no different. The number of files opened remained fairly consistent with previous years with fifteen new files opened, including eight Requests for Review, one privacy complaint, two requests for comment with respect to legislative proposals, one request to participate in an educational conference, two administrative files with respect to national issues and one general administrative file. In addition, 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 Non-Insured Health Benefits Consent issue and the National Birth Mother Survey proposed by Statistics Canada, as well as general issues surrounding privacy in the health sector.

The issue that continues to focus my attention more and more, however, is personal privacy and how difficult it is becoming to preserve it. All levels of government maintain significant amounts of information about every individual citizen. We put a lot of trust in public bodies to maintain that personal information in a manner that does not threaten our larger right to privacy and, for the most part, that trust is well founded. The intentions are clearly good. But there are also a lot of pressures to share information and use it for purposes it was not originally intended. And government is not the only place where our privacy is at risk. We also give our personal information to any number of private entities for various purposes on a daily basis and trust them, as well, to use the

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

information provided only for the purpose it is given. This trust is often not so well founded and in many cases, the good intentions are clearly missing as well.

The right to privacy is a concept that is changing almost daily because of new technologies. What we have to accept in terms of incursions into our privacy continues to expand almost daily. Often, we give up personal privacy without even thinking a lot about where our information might end up or what it might be used for. The right to privacy is becoming an major political issue in many places around the world. A prime example of this is the backlash in the United States to many provisions of the Patriot Act, which was passed in the wake of the events of September 11, 2001. In fact, the fallout from "9/11" continues to challenge governments to find that very thin line between security and privacy and to balance on that line. It is a precarious balance indeed. Almost daily I become aware of another government initiative somewhere which threatens to change forever our ability to control how our personal information is used. With global technologies, legislation passed in another country can now begin to affect the way we live in Canada. For example, American legislation now requires all airlines who wish to land in the United States to provide detailed customer information data, including telephone numbers, credit card details, dietary requests, passport numbers, the names of the people you are travelling with, place of origin, and place of destination. The legislation allows the use of this information for various purposes and will be kept for many years, ostensibly to help in the "war on terrorism" but it is also available for use for any number of

The evolution of the computer from background record-keeper to interactive, networked transaction manager has increased dramatically the volume and variety of personally identifiable information collected and held by organizations. This capability for high speed, high volume processing and dissemination creates the potential for substantial risks, as well as large-scale opportunities, associated with information security and privacy protection.

The Security-Privacy Paradox: Issues, Misconceptions, and Strategies
A Joint Report by the Information and Privacy Commissioner/Ontario and Deloitte & Touche
August 2003

other, as yet unspecified, purposes. If Canadian airlines want to fly into the United States, they will have to provide this information to the American government or face stiff fines and the possibility of being refused landing privileges.

Quite apart from changes spurred by security issues which have become much more of a priority since 9/11, ever evolving and improving technology makes possible today what was considered pure science fiction less than ten years ago.

From microchips smaller than 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 GPS systems in vehicles which track you everywhere you go, the technology surrounds us, sometimes without our even knowing it. Most technology is aimed at making our lives easier. But it very often comes at the expense of our ability to keep personal matters private. It becomes ever more important for us, as citizens, to determine 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 your 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 your personal information to willing buyers without your permission? Is the right to market your product greater than the right to be free of e-mail spam or telemarketing calls?

The Better Business Bureau estimates that it takes about 600 hours for a victim to clean up the mess caused by identify fraud. They need to contact police and credit reporting agencies, stop payments, close any compromised accounts, acquire new documentation and closely monitor their accounts for months to come.

Throughout the process they may be treated more like a fraud perpetrator rather than a victim.

Michael Kane
CanWest News Service

Governments throughout the world are attempting to deal with these issues, some more successfully than others. In Canada, that attempt began with the passage of the *Personal Information Protection and Electronic Documents Act* (PIPEDA) which has been coming into force in stages over the last three years and comes into full force for all private sector commercial activity in Canada on January 1st, 2004. Two provinces, Alberta and British Columbia, will have their own private sector privacy legislation before January 1st, 2004. Ontario, although not as far ahead, is also planning to pass private sector legislation. Alberta, Saskatchewan and Manitoba each have legislation to deal with the privacy of health information. Quebec has had private sector legislation for a number of years and has been far ahead of the rest of the country.

But legislation will not, in itself, be enough. There has to be a public realization that the world is changing and each of us has to take ownership of our privacy which, until now, we have pretty much taken for granted. Individuals have to educate themselves and be more aware of how they use their own personal information. When a clerk at a clothing store requests our telephone number when we purchase an item, do we give it to them? Do we question why they would require our telephone number? Do we give our personal information, including credit card numbers and banking information, to strangers over the phone or over the Internet? Do we throw out paperwork with our name, address, banking or credit card information without ensuring that vital information

As we move toward a more fully digital world, the cost of manipulating information approaches zero, and the hazards therein multiply. Even our privacy is in peril. The "clickstream" pouring into Web merchants — the information that you provide with clicks of your mouse ... what music you listen to and where you like to eat — lets those merchants personalize their marketing, but it may be more information than you want to share widely. And some Web entrepreneurs collect this information and sell it. Supermarket scan cards may be more convenient than coupons, but ... they, too, "put a price on privacy." The activities in these examples are perfectly legal, of course, but they increase the potential for electronic malfeasance.

Marshall Jon Fisher,
"moldovascam.com,"
September 1997, p. 22.

is unreadable? Every person must do his or her share. Identity theft is the fastest growing criminal activity in the world. The Federal Trade Commission in the United States estimates that identity theft cost consumers and businesses 53 billion dollars in the United States in 2002 alone. One recent report suggests that privacy theft in Canada is up 60% from 2002. Dollar losses in Canada were \$14.1 million in the first three quarters of 2002. Identity theft is one of the results of the wired world.

Identity thieves commit fraud and other crimes by impersonating their victims, usually by stealing personal information or aggregating publicly available data about them. Crime groups or those acting alone can use the information to open bank accounts, make credit-card purchases, obtain loans and harm reputations.

But individuals do not always have complete control over their personal information. Even where one would expect personal information to be secure, there is no guarantee of privacy. Recently, two Bank of Montreal computers containing detailed customer financial data were sold to a university student without being properly erased. The student almost resold the machines on eBay before discovering the bank's error. Even Canada Customs and Revenue has recently lost computers containing the personal information, including social insurance numbers and bank account information for thousands of individuals and businesses in the construction industry. Experts in the field warn that this isn't just a problem that can be rectified by individuals being more careful

The technologies of surveillance are developing at the speed of light, but the body of law that protects us is stuck back in the Stone Ages. In the past, new technologies that threatened our privacy, such as telephone wiretapping, were assimilated over time into our society. The legal system had time to adapt and reinterpret existing laws, the political system had time to consider and enact new laws or regulations, and the culture had time to absorb the implications of the new technology for daily life. Today, however, change is happening so fast that none of this adaptation has time to take place - a problem that is being intensified by the scramble to enact unexamined anti-terrorism measures. The result is a significant danger that surveillance practices will become entrenched in American life that would never be accepted if we had more time to digest them.

Jay Stanley and Barry Steinhardt
Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society
January 2003

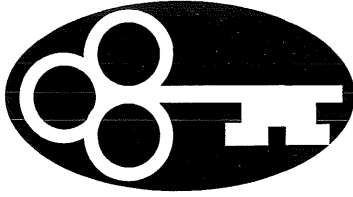
with their personal information, although that is one vital cog in the wheel. A large part of the problem results from failures in the business and governments sectors, such as lax security, and sharing of personal information between businesses in the marketplace. It is hoped that PIPEDA can start to address these problems. However, I would, once again, urge the Government of the Northwest Territories to take steps to protect the personal information of its citizens by introducing legislation to set out rules and regulations to ensure that law, rather than convention, governs the way that the private sector collects, uses and discloses our personal information. The speed of advancing technology demands that governments at all levels keep pace. Unless we sit up and take notice, Orwell's "Big Brother" will be upon us before we realize what has happened.



**NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER**

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

Introduction



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 why they are disclosed.

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

II. INTRODUCTION

A. ACCESS TO INFORMATION

Background

In an increasingly complex world, access to information legislation helps to ensure that governments are open and accountable to the public. Although it recognizes that in some instances government needs to be able to keep some information confidential in order to ensure that it can do the business of government in the most effective and efficient manner, the exceptions to open access to government records are limited. 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 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 the Northwest Territories, the *Access to Information and Protection of Privacy Act* came into effect on December 31st, 1996.

The e-government information environment requires a new breed of information professionals. A common complaint of deputy ministers and other senior managers is that people who understand and can support this new environment are not available. Records managers, file clerks and other traditional positions common in the paper world have long been disappearing. Reasons include budget cuts and the naive assumption that new technology would make "records management" unnecessary. Managers subsequently realized that managing complex electronic data systems was an even more challenging task than dealing with "paper mountains".

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

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

Regulations passed pursuant to the Act designate the public bodies other than government departments that are subject to the Act. There are currently thirty two (32) public bodies listed in the Regulations.

The Department of Justice web page at one point listed the names and contact numbers for a number of public bodies but that information no longer seems to be available. In order to meet the stated purposes of the Act, to give the public a right of access to records held by government bodies and to personal information held about themselves, the tools to allow that to happen must also be in place. If a citizen can't find out who they have to direct their inquiries to, or if it requires four or five phone calls to find the right person, the effectiveness of the act is diluted and the purposes are not met. The Act requires that each department have an Access To Information Co-Ordinator and each of those individual's names and contact information should be easily accessible, both on line and in printed form. I note as well that the Gov-

Invariably there will be situations where equally valuable goals in a free and democratic society will collide. Thus, the right to individual privacy must be balance against the public's right to disclosure. As well, there will be situations where a public body will find it necessary to refuse to disclose a document where the result would be to prejudice the competitive position of, or interfere with or prejudice contractual or other negotiations of either the third party or the public body. The Act is an attempt to balance those competing objectives.

Madam Justice Steel
Kattenburg v. The Minister of Industry, Trade and Tourism
Court of Queens Bench,
November 19, 1999

ernment has not updated the Access Directory required by section 70 of the Act since the Act first came into force.

These are things which must be done in order to make the Act fully functional. I would encourage the Government to ensure that these steps are taken as soon as possible.

The Process

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

The role of the public body is to apply the specific requirements of the *Access to Information and Protection of Privacy Act* to each request received while at the same time 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 various ways.. The ATIPP Co-ordinators must exercise their discretion to ensure a correct balance is struck between the applicant's general right of access to information and the possible exceptions to its disclosure under the Act.

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

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

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

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

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. The independence of the office is essential for it to maintain its credibility and ability to provide an impartial review of the government's compliance with the Act. Under the Act, a Commissioner is appointed for a five (5) year term.

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

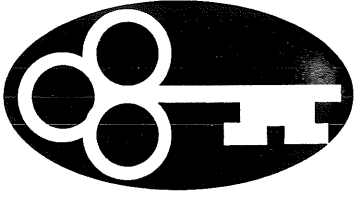
The Information and Privacy Commissioners, the Auditor General, Parliamentary Committees and others have repeatedly called attention to poor information management and its impacts. Most recently, poor record keeping was cited as a key factor of concern in the management of the gun registry program, in concerns over GST fraud, in the improper tendering of government contracts, in the inability to locate costly commissioned reports, and the lack of security for sensitive information placed on government websites. The Auditor General has said that some programs were so poorly documented that an audit could not even be completed. The records were simply unavailable, incomplete or unreliable.

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

tions 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 Northwest Territories Supreme Court.

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 affect access to information or the distribution of private personal information in the possession of a government agency.



At stake is whether society is able and willing to maintain its trust and confidence in government. Without these qualities, democracy itself is in serious jeopardy.

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

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 must advise the individual exactly the uses for which the information is being collected and how it will be utilized and, if it is to be used for other purposes, obtain the consent of the individual prior to such other use;
- 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 [applicant's] motive is irrelevant. There is no need to justify a request for information. A citizen is prima facie entitled to access information from his government unless there are sufficiently compelling reasons to exempt the information from disclosure. Those reasons are identified in the legislation and constitute exemptions to the general principle of disclosure. The refusal to disclose is mandatory with respect to some of the exceptions while others are only discretionary.

Madam Justice Steel
Kattenburg v. The Minister of Industry, Trade and Tourism
Man. Court of Queen's Bench
November 19, 1999

- 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.

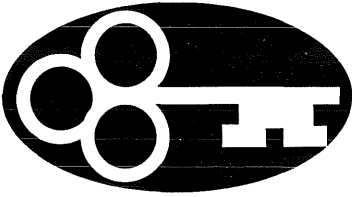
The ever increasing amounts of information collected and retained by government, the amount of outsourcing which governments now do, and the evolution of technologies which allow easy data matching and sharing make it all the more important that there be an independent review process for privacy issues. I acknowledge the steps taken by the Government of the Northwest Territories to address this deficiency in the Act and look forward to seeing that legislation passed and implemented in the next fiscal year.



**NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER**

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

Requests for Review



We are seeing a general recognition that respecting privacy is not as onerous as some people thought, and in fact is simply good business practice.

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

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

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.

When the 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 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

The impact of poor records management goes far beyond the government's access and privacy regime. Within government, the lack of accurate and authoritative information results in poor decisions, failed programs and lost opportunities. Time wasted finding information and the storage of records no longer needed increase government operating costs. The failure to maintain and protect records with high legal and intellectual property value results in increased liability and financial loss. The premature destruction of records with long-term archival value contributes to our collective historical amnesia and the loss of valuable knowledge.

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

solution satisfactory to all of the parties. In several cases, this has been sufficient to satisfy the parties. If, however, a mediated resolution does not appear to be possible, the Information and Privacy Commissioner will do a more thorough review, giving all of the parties involved, including the Public Body, the opportunity to express their positions on the matter in writing. After reviewing all of the submissions and the records in question, the Information and Privacy Commissioner will then make a recommendation to the head of the public body. The head of the public body then determines whether or not he or she will accept the recommendations made, reject them, or substitute his or her own resolution to the question.

The Information and Privacy Commissioner's Office received eight (8) new requests for review in fiscal 2002/2003 as well as one privacy complaint. This is approximately the same number as were received in previous years.

Six recommendations were made.

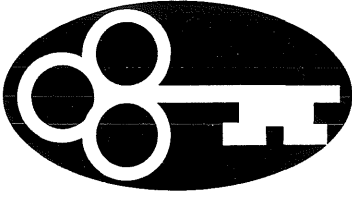
This year, the Information and Privacy Commissioner was asked to review decisions from six different departments. Three requests involved the Department of Justice and one each involved the Department of Health and Social Services, the Workers Compensation Board, the Department of Resources Wildlife and Economic Development, the Department of Sustainable Development and the Department of the Executive. The privacy complaint involved the Department of Health and Social Services.



**NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER**

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

Review Recommendations



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, Ph.D.
Ontario Information and
Privacy Commissioner
Annual Report 2002

IV. REVIEW RECOMMENDATIONS

Review Recommendation #02-025

This Request for Review came from an individual who was seeking to obtain a copy of a tape recording of a court proceeding which had taken place in the Supreme Court of the Northwest Territories. The request was made of the Department of Justice. The Applicant was provided with a transcript of a "limited in content" tape recording made by the Court Reporter during the trial, as well as an explanation that the tape recording was not continuous and was made for back-up purposes only. He was also advised that the Clerk of the Court had made the tape recording. The Department of Justice took the position that this particular tape recording was information in a court record and, therefore, outside the scope of the Access to Information and Protection of Privacy Act pursuant to section 3 of the Act. The Applicant was, however, advised that the tape recording would be made available for him to listen to. In order to listen to it, however, it was the Court's policy that either the Applicant or his agent would have to attend at the Court House in Yellowknife to listen to the tape in the presence of the Clerk of the Court. This clearly proved impossible for the Applicant to do in light of the fact that he was incarcerated in a southern security institution.

The issue was whether the Access to Information and Protection of Privacy Act applied to the record in question or whether it was outside the scope of the Act pursuant to Sec-

The Department has clear responsibilities under the ATIPP Act and under the Child Day Care Act. Their responsibility under the Child Day Care Act is to regulate and set rules for day home operators. Their responsibility under the ATIPP Act is to respond to requests for information. There is nothing in either of these two pieces of legislation which says that the Department's role is to in any way "protect" day home licensees from controversy or complaint. Nor should it be involving itself in disagreements between the day home business and its customers, unless that disagreement arises out of a breach of the provisions of the Child Day Care Act or its regulations. There is certainly nothing in the Access to Information and Protection of Privacy Act which suggests that access to information can be refused because the public body does not like the Applicant or what they think he is going to do with the information, which appears to be the reason the Department is asking me for permission to disregard the request for information in this case.

Elaine Keenan Bengts
Information and Privacy
Commissioner
Review Recommendation
02-026

tion 3 of the Act which defines what is included in the term "record" . That section provides that the Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to record made from information in a court file, a record of a judge of the Court of Appeal, the Supreme Court or the Territorial Court or a record of a justice of the peace.

The Information and Privacy Commissioner was of the opinion that Section 3 did not exclude information on a court file and recommended that a copy of the tape be made and provided to the Applicant.

The Department rejected the recommendation of the Information and Privacy Commissioner.

Review Recommendation 02-026

This request came from the Department of Education, Culture and Employment and was a request pursuant to section 53 of the Act for authorization to disregard a request for information. The request for information in question came from a parent whose child had been placed in a licensed day care. The request was for information about the day care, whose license was granted by the Department of Education, Culture and Employment. The Department was asking that they be allowed to disregard the request as they felt that the request was being made "in bad faith". In making that assertion, they relied on a set of background facts which they say amounted to harassment of the owner of the day care facility in question.

If the purpose of such legislation is to protect the public from those who would hold themselves out as professionals without the necessary qualifications or skills, then that individual must also know that disciplinary matters might well be subject to public scrutiny. The integrity of the disciplinary system would quickly be impugned if the findings of investigations, such as the one in question today, were hidden from public eyes.

Elaine Keenan Bengts
Information and Privacy
Commissioner
Review Recommendation
#02-027

The Information and Privacy Commissioner declined to give the authorization requested, noting that what the Department was really asking was for the Information and Privacy Commissioner to intervene in the private dispute between the Day Care provider and the parent. The Commissioner pointed out that the Act provided a tool for parties to obtain information from government agencies and it was not for the public body to question why the information was being sought or to refuse access, or refuse to respond, because they did not condone the actions of the applicant. Furthermore, the Information and Privacy Commissioner commented on the fact that the alleged "bad faith" allegation was based only on statements received from the day home provider who did not want the information released and was not supported by any extrinsic evidence. The onus was still on the public body to show that the information in question should not be released.

Recommendation #02-027

This review recommendation involved the Department of Health and Social Services. In this case, the Applicant was seeking a copy of a report of a preliminary ethics investigation which had been conducted in response to a complaint made to the department about the conduct of a professional within the health care system. The public body used their discretion to refuse access to the report on the grounds that it was personal information about the party complained of, the disclosure of which would be an unusual invasion of that person's privacy.

The Access to Information and Protection of Privacy Act deals only rights of access to existing records. There may be other legislation which deals with the creation and management of public records. The ATIPP Act, however, does not and nothing in the Act gives this office any jurisdiction to comment on or deal with the accuracy or completeness of the records made. If there is no record, there is simply nothing to correct.

Elaine Keenan Bengts
Information and Privacy
Commissioner
Review Recommendation
#02-028

After reviewing all of the facts and circumstances and the report itself, the Information and Privacy Commissioner recommended that the report be edited so as to sever sensitive parts of the report which, if revealed, might result in an unreasonable invasion of the privacy of third parties, and that the edited report should be disclosed.

The Commissioner's recommendation was accepted.

Review Recommendation 02-28

In this case, the Applicant was a third party who sought to have certain personal information corrected before certain records were provided to an Applicant. In this case, an applicant sought records from the department with respect to the granting of a day home license. The holder of the license was consulted as a third party under the act before the records were released. In the process of that consultation, the Third Party was given a copy of the records that the Department intended to disclose to the Applicant. The Third Party claimed that there was information missing from the file in that there had been a telephone discussion between herself and the department for which there did not appear to be any notations on her file. She sought to have the department correct the record by creating a record of the telephone discussion in accordance with her own recollection of it. The telephone discussion had occurred many months before the request for information had been received by the department.

In making her recommendation, the Information and Privacy

This document itself does not constitute communication between a solicitor and his/her client.... It has never been communicated to the lawyer by the client or by the client to the lawyer. The only information it contains that would also appear on the lawyer's statement of account are the date of the account, the invoice number and the total amount paid. In the similar circumstances of Order PO-1922, the Ontario Information and Privacy Commissioner made the following remarks:

It is not a communication between a solicitor and a client, nor does its content reveal any prior communication of this nature. Rather, the record contains the type of information identified by the Court in as an exception to solicitor-client privilege - a "statement of fact". Specifically, the record is a factual statement of the amount of public funds paid by the Ministry to Lawyers 1 and 2 in consideration for the legal services provided to Persons A and B during the prosecution of the accused.

I agree with this assessment.

Elaine Keenan Bengts
Information and Privacy
Commissioner
Review Recommendation
#03-029

Commissioner pointed out that there can be no correction of a non-existent record. Furthermore, she noted that the provisions of the Act which provide for correction to public records relate only to the personal information of the the individual seeking to have the record corrected. In this case, it was her opinion that, even if a record of a telephone discussion did exist, it would not necessarily be personal information which was subject to correction. More likely, it would have been the writer's interpretation of what was said during the discussion and, although bits of that might have constituted personal information, it is unlikely that the whole of the notes could have been categorized as such.

Perhaps more to the point, the Information and Privacy Commissioner pointed out that the nature of the Access to Information and Protection of Privacy Act is such that if there is no record, there is nothing to be corrected.

The recommendations made by the Commissioner were accepted.

Review Recommendation 03-029

This request for review involved the Department of Resources, Wildlife and Economic Development (RWED) and a request from a member of the public for information relating to fees paid by the Government of the Northwest Territories and RWED since January 1999 to a specified law firm in connection with the filing, prosecuting and opposing polar bear trade-mark applications and in connection with all Federal

In reviewing the matter, the Information and Privacy Commissioner [of Ontario] distinguished between a lawyer's statement of account, which he agreed was subject to the solicitor/client privilege, and a separately created document which contained only the total amount paid with respect to the matter in question:

The record here is a one-page document prepared by the Ministry which reflects the total funding paid to Lawyers 1 and 2 in representing their clients in the criminal proceedings involving the accused. The records at issue in Orders PO-1714, PO-1822 and in were all actual statements of account, which were characterized as confidential written communications between solicitors and clients.

That is exactly the kind of document we are dealing with in this case. The record in question is one generated through the government's accounting system. The record has never been the lawyers office and was not generated by the lawyer's office.

Elaine Keenan Bengts
Information and Privacy
Commissioner
Review Recommendation
#03-029

Court matters against a particular company. RWED responded by providing a computer printout which listed a series of invoice numbers, invoice amounts and other general information. The response also indicated, however, that the list was a list of all amounts paid to the law firm over the specified period of time and that not all of the amounts were necessarily paid with respect to the particular issue identified. The Applicant asked that those amounts be delineated. The department refused, citing solicitor/client privilege. The Applicant then asked the Information and Privacy Commissioner to review that decision.

The department relied on a Supreme Court of Canada case in which the Court upheld a public body's decision to sever certain information from a legal account before releasing it to a member of the public. The Information and Privacy Commissioner distinguished the facts of this case from those in the Supreme Court case and pointed out that in this case, all that was being asked for was a total amount, not any of the information that went with that amount. Instead, the Commissioner followed a very similar case decided by the Ontario Information and Privacy Commissioner's Office where the record in question is one generated through the government's accounting system. The record had never been the lawyer's office and was not generated by the lawyer's office.

The Information and Privacy Commissioner recommended that the Applicant be provided with the amount that had been spent on legal fees in defending the particular action.

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

The recommendation of the Information and Privacy Commissioner was not accepted and the Applicant did not receive the information requested.

Review Recommendation 03-030

An application was received by the Department of Justice for copies of all documentation surrounding the granting of what is commonly referred to as "Overtime Averaging" permits, issued by the Labour Standards Board to employers who work in camp situations. These permits will allow employers to deviate from the otherwise legislated limits to hours of work and overtime pay. Two of the employers who had been granted such permits objected to the disclosure of the information requested, claiming that the release of the information in question could be reasonably expected to prejudice their competitive position. They also relied on the provisions which deal with unreasonable invasion of third party privacy.

The Department of Justice had reviewed the request for information and had determined that the permits themselves and the letters that accompanied those permits were not subject to any of the exemptions provided for in the *Access to Information and Protection of Privacy Act* and should be disclosed. However, they relied on Section 24(1)(b) of the Act which provides that the public body shall refuse to disclose information where that information is commercial information provided in confidence by a third party and is of a confidential nature. In particular, they felt that the application forms contained proprietary information belonging to the third party em-

Government institutions bear the burden of proof that information held in government files relating to private companies should be kept secret. It is not sufficient for government institutions to blindly follow the wishes of private firms or to shift the burden of proof to the third parties. In order for government institutions to discharge the burden of proof in such cases, simple assertions that harm will result from disclosure, or speculation as to the potential harm from disclosure, will not suffice. Concrete evidence is required which demonstrates, at the level of a probability, that competitive harm to the private company is likely to result from disclosure of the information.

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

employers, the disclosure of which might reasonably be expected to affect the ability of the companies to hire qualified staff if the information fell into a competitor's hands. The permits, themselves, however, were quasi public documents in any event, in that they were required to be posted at the job site, and they did not contain any proprietary information. The Department, therefore, determined that they would release the permits and the letters which accompanied those permits, but would not release the application forms.

After reviewing the matter, the Information and Privacy Commissioner agreed with the department and recommended that they follow the proposed course of action.

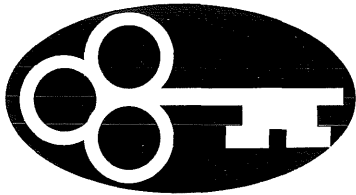
The Information and Privacy Commissioner's recommendations were accepted.



**NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER**

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

Recommendations



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

V. RECOMMENDATIONS

Clearly, accountable government depends to a large degree on the ability of the public to know what goes on in government. To that end, I have made a number of recommendations in my Annual Reports over the years which I feel would help to accomplish that goal. Many of my recommendations have also been aimed at helping the public to maintain their right to privacy in the digital world. Many of the recommendations made in the Information and Privacy Commissioner's Annual Report in the last few years have been made several times. I understand that there is legislation currently wending its way to the Legislative Assembly which will address some of the comments made in previous Annual Reports. I am pleased to see some progress being made and look forward to providing my comments on the proposed legislation as it comes forward.

I believe that the government should be doing a better job of ensuring that the public knows that it has the right to ask for and receive government records. The stated goal of the Act is to make government more accountable to the public by allowing access to information. However, the existence of the Act itself seems to be a closely held secret such that only people in the media and savvy businessmen know of its existence. There is very little information about the act on any government web site. The Department of Justice does have mention of the Act, but does not provide specific information about who, in each department is responsible for receiving and dealing with requests for information. The Access to In-

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

formation Directory, mandated by section 70 of the Act, has not been updated since the Act was implemented and, as far as I know, is not readily available to the public in any event.

I therefore **recommend** that the Government of the Northwest Territories direct the preparation of an updated Information and Privacy Directory and that the directory be updated annually to reflect changes in the Act and in the contact information for the ATIPP Co-Ordinator for each department . I further **recommend** that the Directory be made available to the public at no cost or for a nominal fee, and that it be available at all government offices generally open to the public throughout the Territories. In today's electronic age, where the internet is becoming an increasingly important tool for communications, the names and contact numbers for the ATIPP Co-Ordinators for each public body subject to the Act should be posted on both the Government's web page and on the Legislative Assembly web page in such a way that the public can find it easily and without having to dig through layers of unlikely links before coming up with the information they need.

I would again **recommend** that the Government continue to support and encourage 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 with 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. *The Access to Information and*

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

George Radwanski
Privacy Commissioner for
Canada
Annual Report 2000-2001

Protection of Privacy Act is one of those pieces of legislation that requires widespread general knowledge of its terms in order to be fully functional and effective in the way that it was intended to be. Educated government employees is a vital part of the system.

It is important that those who are given the primary responsibility to deal with Access to Information Requests in each public body are given the time to do their jobs properly. It appears that in almost every case, the duties and responsibilities of ATIPP Co-Ordinators are simply added to someone's job description, without any consideration of the time needed to undertake those added responsibilities. Particularly in those public bodies which often receive Requests for Information, dealing with those applications can be a time consuming undertaking. It is important that the head of each public body recognize this needed time commitment and make that time available for the ATIPP Co-Ordinators involved. It is a matter of recognizing, as part of the "corporate culture" that ATIPP issues are important and have some priority.

One of the recommendations that I have made in several of my Annual Reports is that municipal governments must be brought under legislation which regulates them in terms of their responsibilities to maintain individual privacy and their obligations to provide the public with access to public documents. I repeat this **recommendation** and would encourage the Government of the Northwest Territories to either include municipal governments under the Act or that new legislation

The evolution of the computer from background record-keeper to interactive, networked transaction manager has increased dramatically the volume and variety of personally identifiable information collected and held by organizations. This capability for high speed, high volume processing and dissemination crates the potential for substantial risks, as well as large-scale opportunities, associated with information security and privacy protection.

The Security-Privacy Paradox: Issues, Misconceptions, and Strategies
A Joint Report by the Information and Privacy Commissioner/Ontario and Deloitte & Touche
August 2003

be created to make rules and regulations with respect to both access to information and protection of personal privacy within the municipal public sector. Not only is it important that municipal authorities also 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. More and more often I hear of plans to “integrate” certain information systems so that information can be shared between Territorial and Municipal governments. Quite apart from whether or not information should be shared between levels of government, the concerns are magnified exponentially when the public body receiving the personal information does not have any legislated constraints on how and when the information is used . Such sharing of information without appropriate restrictions on the use of such material is irresponsible use of personal information. I encourage the Government of the Northwest Territories to resist the urge to open up the avenues of data sharing and encourage them to consider legislation which will require municipal governments to comply with both the need for access to information and to the privacy code found in the *Access to Information and Protection of Privacy Act*. I would also strongly **recommend** that access and privacy issues be kept at the top of the agenda when discussing and negotiating devolution and self government. Aboriginal people should be able to test the accountability of their elected officials. Likewise, and perhaps more importantly, they are entitled to be confident that their personal information will not be used without their knowledge or consent or for purposes which they

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.

never intended it to be used for.

On the same theme, I would continue to caution government to ensure that when public functions are delegated to the private sector, the private business be contractually obligated to comply with the provisions of the *Access to Information and Protection of Privacy Act*. There does not appear to be any recognition, at least in the contracts which I have recently 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. I **recommend** that access and privacy clauses should be standard fare in outsourcing contracts.

It has become almost a mantra with me that the North needs its own private sector privacy legislation. I **recommend** that the Northwest Territories take the lead of British Columbia and Alberta and 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

Information about a consumer's behaviour and interests is invaluable for marketing purposes. Collecting this type of information on the Internet has been facilitated by online tracking tools that allow the information to be collected automatically and, in some cases, without the knowledge of the Internet user. In general, the information collected is benign, consisting of a user's IP address; the type of computer and software; the linking Web site; any files which were accessed, and the amount of time spent on each page. However, through the use of cookies, server logs, Web bugs and data matching algorithms, it is possible for businesses to combine data collected from various Web sites and produce detailed profiles on how a particular computer has been used to access content or services through the Internet. When these profiles are combined with information that allows individuals to be identified, detailed personal profiles on consumers can be created.

An Internet Privacy Primer: Assume Nothing
Ontario Information and Privacy Commissioner's Office

businesses (and I stress the word "businesses") which receive and hold very sensitive personal information, from dentists and chiropractors, to pharmacists and private laboratories. It is important that the people of the the North have an effective mechanism to address privacy concerns in the public sector. Quite apart from the benefits to the public that such legislation would provide, good privacy practices are simply good business and such legislation can only serve to enhance the image of the Northwest Territories as a good place to do business.

Technology is growing at an incredible pace and the frightening prospect that George Orwell predicted in his famous novel "1984" is truly reality. We live in an era of super computers, mini chips, radio frequency identity devices, closed circuit cameras, cell phones that take and transmit pictures and satellite positioning. To rely exclusively on volunteer adherence to basic privacy principles in the private sector is, I would suggest, short sighted and overly optimistic. Furthermore, legislated guidelines can provide consistency in approach and practice. This is not something that can be left either to a federal agency or to the good faith of private business.

Although the *Personal Information Protection and Electronic Documents Act* comes into full force throughout Canada on January 1st, 2004, it is legislation administered by the Privacy Commissioner in Ottawa and by necessity, that office will have to concentrate on the "big" issues of wider import, leaving problems in small business and of only local impor-

Technology is offering formidable tools for surveillance of individuals by the state or even by each other, weakening traditional community ties. May have observed that these changes undermine citizens' interest and confidence in the usual channels of democratic expression, essentially the mechanisms of electoral representation. Consequently, in Western societies, we see an increasing interest in strengthening the direct expression of democracy.

Excerpt from "Report on the Implementation of the Access Act and the Private Sector Act - Summary
Jennifer Stoddart
Quebec Information and Privacy Commissioner
November 2002

tance without real regulation. I believe that legitimate and ethical business would welcome such guidance and I would encourage the Government of the Northwest Territories to make private sector privacy legislation a priority.

Finally, I would take this opportunity to voice my disappointment with the Department of Resources, Wildlife and Economic Development and the position which that department took in connection with the request they received in which they were asked to identify how much public money was spent on legal fees to defend the government's position on the polar bear trade mark. (Review Recommendation 03-029). They had the ability to answer that question in a straight forward and concise manner. This was an "accountability" issue.....how is the government spending our tax dollars. Why the department was so reluctant to provide the information that they would blatantly ignore the recommendation of this office is left for us to guess. The impression left, however, is that the government was embarrassed by its spending in this regard and was anxious, therefore, not to reveal the extent of public funds that were devoted to this issue. Embarrassing or not, the public has the right to know.

This office made a recommendation that the amount expended on this particular litigation be disclosed. The recommendation was based on solid precedent set by the Ontario Information and Privacy Commissioner under an almost identical set of circumstances with almost identical legislative wording. The Department, however, chose to refuse access despite both my recommendation and strong precedent from

With the advent of high speed computers, local area networks, powerful software techniques, massive information storage and analysis capabilities, neural networks, parallel processing, and the explosive use of the Internet, a new world is emerging. Change is now the norm, not the exception, and in the quickly evolving field of information technology, information practices must also keep pace, or run the risk of facing extinction. Take, for example, the new directions being taken intending to replace the information "silos" of old, with new concepts such as "data integration" and "data clustering." If privacy advocates do not keep pace with these new developments, it will become increasingly difficult to advance options and solutions that can effectively balance privacy interests new technology applications. Keeping pace will enable us to continue as players in this important arena, allowing us to engage in a meaningful dialogue on privacy and future information practices.

Data Mining: Staking a Claim on Your Privacy
January 1998

another jurisdiction. The *Access to Information and Protection of Privacy Act* is nothing more than window dressing and political expedience if government agencies can ignore recommendations made by the commissioner without fear of consequences. Consequences, however, do attach, even if they are not direct. In this case, the refusal of the public body to provide the information fosters an atmosphere of suspicion and mistrust. What are they hiding? Why is the department so worried about this information being released to the public? If this kind of response to the recommendations of the Information and Privacy Commissioner happens regularly, the public will react and even more difficult questions will be asked.

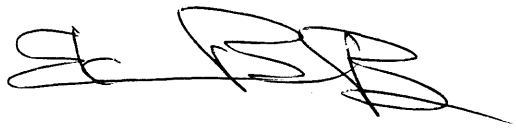
The longer I remain involved in the administration of the *Access to Information and Protection of Privacy Act*, the more convinced I become that it is increasingly important legislation in today's digital world and that it is fundamental to our ability to continue to improve the democratic process. Governments, of course, have operated democratically and openly for hundreds and even thousands of years without such laws to ensure this openness and accountability. However, governments in decades past have not had to deal with the technological age in which information is power and the collection, combining, sharing and storage of personal information data is not only easy and inexpensive, but expedient. Although the advent of technology makes storage of information easier, access to that information is often more difficult, especially for those who do not have every day contact with the government. World events have served to crystallize the

The problem of identity theft must be fought on several fronts. Applying fair information practices is a good place to start. Moreover, as computers and networks make it easier and easier to gather your personal information, technological methods of protecting privacy will become increasingly important. Organizations that can offer their clients greater informational privacy may well obtain a competitive advantage over those who fail to do so. If enough people demand it, we may find that in the future, anonymous transactions (which authenticate identity in a blind manner), will become the standard, as opposed to the identifiable transactions of the present day. De-identifying information may well pave the way to a future which includes privacy.

Identity Theft: Who's Using Your Name?
Dr. Ann Cavoukian
June 1997

apparent need for government to know more about the people it serves. How far should government's be allowed to go? How much intrusion into our private lives do we accept and for what purposes? Where does the line between need for security or the need for efficiency cross over the line that provides us the right to our own personal privacy? We need to start asking ourselves, as governments, as businesses and as individuals what we want our futures to look like. Government is where this questioning must begin.

Respectfully submitted



Elaine Keenan Bengts
Information and Privacy Commissioner

