



NUNAVUT
INFORMATION
AND PRIVACY
COMMISSIONER

2010/2011
ANNUAL REPORT

**INFORMATION AND PRIVACY
COMMISSIONER OF NUNAVUT**

P.O. Box 262
Yellowknife, NT, X1A 2N2

Phone: 867-669-0976
Toll Free 1-888-521-7088
Fax: 867-920-2511
E-mail: Atippcom@theedge.ca



**NUNAVUT
INFORMATION
AND
PRIVACY
COMMISSIONER**

2015 - 47th Street
P.O. Box 252
Yellowknife, NT
X1A 2N2

August 9, 2011

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

Attention: Honourable Hunter Tootoo
Speaker of the Legislative Assembly

Dear Sir:

I have the honour to submit to the Legislative Assembly my Annual Report as the Information and Privacy Commissioner of Nunavut for the period of April 1st, 2010 to March 31st, 2011.

Yours truly,

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner



INDEX

Commissioner's Message	4
The Act	7
Access to Information	8
Protection of Privacy	10
Year in Review	11
Review Recommendations Made	13
Review Recommendation 10-50	13
Review Recommendation 10-51	15
Looking Ahead	17

I do not think that simply obeying the FOIP Act makes anyone a leader in accessibility and transparency. Obeying the law is simply what we are all supposed to do. You are not a leader just because you stop at a red light. Leadership, to me, is about being out there, ahead of the law, showing by example the way things should be.

- Frank Work, Alberta Information and Privacy Commissioner
Edmonton Journal, July 7, 2011



COMMISSIONER'S MESSAGE

However, I am mindful of the fact that the real strength lies not in the laws themselves but in the people in government who work with this information each day to deliver our programs and services. Privacy is in our hands. Accountability is ours.

Excerpt from September 1, 2010 memorandum from Premier Brad Wall to "All Government of Saskatchewan Employees" regarding Privacy and Security Awareness Month

My message this year mimics that of many of many of my counterparts throughout the country. Since the *Access to Information and Protection of Privacy Act* came into force in the Northwest Territories in 1996, my office has campaigned for open, transparent, accountable government, in keeping with the stated purposes of the Act. In the past, my focus was on promoting a generous application of the access provisions of the Act combined with routine disclosure. Advances in technologies, however, have surpassed these concepts. Proactive disclosure is the future and needs to become the norm.

Spearheaded by the Ontario Information and Privacy Commissioner's office, "Access by Design (AbD)" seeks to establish a fundamental change in the way that government and citizens interact, making public institutions proactive, rather than reactive, in their approach to disclosure. The Ontario Commissioner, in her most recent Annual Report, made the following observations about AbD:

In short, AbD requires governments to recognize that publicly-held information is a public good, and that access should be provided by default – as part of an automatic process. The concept of AbD goes much



The protection of citizens' personal data is vital for any society, on the same level as freedom of the press or freedom of movement. As our societies are increasingly dependent on the use of information technologies, and personal data are collected or generated at a growing scale, it has become more essential than ever that individual liberties and other legitimate interests of citizens are adequately respected.

Joint Communique of Privacy Commissioners issued after the Conference of Data Protection and Information Commissioners, London, 2006

further, however. It also calls for a more responsive and efficient government that forges collaborative relationships with citizens, the private sector, and other public institutions. The ubiquitous nature of the Web, and accompanying technologies, has driven dramatic new increases in public demand for government-held information, giving a new dimension to civic participation and allowing for greater citizen engagement in policy making and service delivery.

In September, 2010, at our annual meeting, the Information and Privacy Commissioners of Canada passed the following resolution encouraging all Canadian governments to take steps to implement Access by Design:

1. The Commissioners endorse and promote open government as a means to enhance transparency and accountability which are essential features of good governance and critical elements of an effective and robust democracy.
2. The Commissioners call on the federal and all provincial and territorial governments to declare the importance of open government, including specific commitments for stronger standards for transparency and participation by the public.
3. Governments should build access mechanisms into the design and implementation stages of all new programs and services to facilitate and enhance proactive disclosure of information.



4. Through ongoing consultations with the public, governments should routinely identify data sources and proactively disclose information in open, accessible and reusable formats. Public access to information should be provided free or at minimal cost.
5. In implementing open government policies, the federal and all provincial and territorial governments should give due consideration to privacy, confidentiality, security, Crown copyright and all relevant laws.

Public institutions require a strategy when it comes to making public data more accessible, and we believe that Access by Design provides the roadmap. The U.S. and the U.K. have made great progress in this area and there is no reason why other jurisdictions, including Ontario, can't do the same .

- Brian Beamish, Assistant Information and Privacy Commissioner of Ontario, March 9, 2011

I take my turn in encouraging the Government of Nunavut to ensure that new programs and services are built with access mechanisms as an integral part of the program so that Nunavumiiut have free and open access to information that interests them. When access is embedded into the design of public programs from the outset, it delivers the maximum ability for the public to obtain access to government-held information by making proactive disclosure the default. Not only can the public then access information more directly, it is cost effective and can limit costs long term by making information available on a routine basis as a default position. Information has been called the lifeblood of the 21st century economy. The information must not only be easily available to the public, it must also be accurate, reliable and up-to date. Quality control and assurance protocols are vital to ensure that public participation in the democratic process remains relevant and meaningful.



THE ACT

The *Access to Information and Protection of Privacy Act (ATIPPA)* of the Northwest Territories came into effect on December 31st, 1996 and became part of the law of Nunavut when the Territory was created in 1999. The Act establishes the rules surrounding the collection, use and disclosure of information about individuals by Nunavut public bodies. It also outlines the rules by which the public can obtain access to public records.

I believe that a guarantee of public access to government information is indispensable in the long run for any democratic society.... if officials make public only what they want citizens to know, then publicity becomes a sham and accountability meaningless.

- Sissela Bok, Swedish philosopher, 1982

The office of the Information and Privacy Commissioner (IPC) is created by the legislation to provide independent advice and review on questions that arise with respect to the implementation and interpretation of the Act. The IPC is an independent officer of the Legislature and is appointed by the Commissioner of Nunavut on the recommendation of the Legislative Assembly. She reports to the Legislative Assembly of Nunavut. As an independent officer, the IPC can only be removed from office "for cause or incapacity" on the recommendation of the Legislature.

The Act provides the public with a process to obtain access to most records in the possession or control of the Government of Nunavut or one of a number of other Nunavut publicly owned organizations. The general rule under the Act is that the public has right to any record which public bodies hold. There are, however, a number of specific and limited exceptions to the right to access. Most of the exceptions function to protect individual privacy rights, to allow



elected representatives to research and develop policy and the government to run the "business" of government. The Supreme Court of Canada has clearly stated that exemptions to disclosure provided for in access to information legislation should be narrowly interpreted so as to allow the greatest possible access to government records.

Every thing secret degenerates,
even the administration of justice;
nothing is safe that does not show
it can bear discussion and publicity.

- Lord Acton

The Access to Information and Protection of Privacy Act also has rules which are focused on protecting individual privacy. By its very nature, government collects and retains significant amounts of information about individuals - from medical and educational records to driving and financial information. Any time an individual interacts with a government agency, information is likely collected and retained. The ATIPP Act provides rules for when and how public bodies can collect personal information, what they can use it for once they have collected it, and when the information can be disclosed to another public body or the general public. It also provides a mechanism which allows individuals the right to see and make corrections to information about themselves in the possession of a government body.

ACCESS TO INFORMATION

Any person, whether they live in Nunavut or any other part of the world, may request access to a government record. Unless the information being requested is for the Applicant's own personal information, there is a \$25.00 fee. In some cases involving a large number of records, additional fees may be applicable.



To obtain a record from a public body, a request must be made in writing and delivered to the public body from whom the information is sought. When an applicant is not certain who his or her request should be sent to, it can be sent to the Manager of Access to Information and Protection of Privacy who works in the office of the Executive and Intergovernmental Affairs and she will make sure that it is delivered to the right person in the appropriate public body.

It is a matter of leadership. It is a matter of those who promise transparency delivering on the promise and it is as simple as sending the instruction down the ranks. It is the difference between a culture of secrecy and a culture of openness. If you are going to promise transparency, then embrace it... Let the public see, let the public judge, let the public find ways to make the information useful and relevant to themselves and others.

- Frank Work, Alberta Information and Privacy Commissioner, 2010 Annual Report

When a request for information is received, the public body has a duty to identify all of the records which are responsive to the request. Once all of the responsive documents are identified, they are reviewed to determine if there are any records or parts of records which are protected from disclosure under the Act. The public body must endeavor to provide the 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. In most cases, the response must be provided within 30 days after it is received.

If a response is not received within the time frame provided under the Act, or if the response received is not satisfactory, the applicant can ask the Information and Privacy Commissioner to review the decision made.

The role of the Information and Privacy Commissioner (IPC) is to provide an independent, non-partisan oversight of decisions made by public bodies in Nunavut in relation to requests made under the Access to Information and Protection of Privacy Act for access to information.



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 as to the reasons for their decisions. In most cases, the Commissioner will receive a copy of the responsive documents from the public body involved and will review the records in dispute. The IPC will consider the responses received and provide the public body and the Applicant with a report and recommendations. The IPC generally does not have any power to make binding orders, but she is required to make recommendations. The head of the public body must then make a final decision as to how the government will deal with the matter. If, in the end, the person seeking the information is not satisfied with the decision made by the head of the public body, they may apply to the Nunavut Court of Justice for a final determination of the matter.

These freedoms of expression and worship -- of access to information and political participation -- we believe are universal rights. They should be available to all people, including ethnic and religious minorities -- whether they are in the United States, China, or any nation. Indeed, it is that respect for universal rights that guides America's openness to other countries; our respect for different cultures; our commitment to international law; and our faith in the future.

President Barack Obama
Shanghai Speech, November 17, 2009

PROTECTION OF PRIVACY

Part II of the Access to Information and Protection of Privacy Act establishes the rules about how public bodies can collect personal information, how they can use it once it has been collected and how and when they can disclose it to others. The Act requires public bodies to ensure that they maintain adequate security measures to ensure that the personal information which they collect cannot be accessed by unauthorized personnel. This Part of the Act also provides the mechanism for individuals to be able to ask the government to make corrections to their own personal information when they believe that an error has been made. Every person has the right to ask



for information about themselves. If an individual finds information about themselves 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 still be made on the file that the individual has requested a correction.

It's very easy to put out information that doesn't have any negative consequences for you. The hard part is putting the stuff out when it doesn't make you look so good, but that's part of transparency, that's part of accountability. And that is where the rubber will meet the road.

- Vincent Gogolek ,
B.C. Freedom of Information
and Privacy Association

In Nunavut, the Information and Privacy Commissioner has no formal legislated authority to receive a complaint about a breach of privacy, or to do an investigation or make recommendations. Notwithstanding the lack of a formal mandate in this regard, this office routinely accepts complaints and undertakes investigations and provides reports and recommendations when a member of the public complains that their personal information has been improperly collected, used or disclosed by a public body. There is no requirement that a public body respond to such recommendations or even that they co-operate with the Information and Privacy Commissioner in her investigation of such complaints.

THE YEAR IN REVIEW

In the 2010/2011 fiscal year, the Information and Privacy Commissioner's Office opened five (5) review files. Four of those were with respect to Access to Information matters and one was a privacy complaint.

The requests involved several government bodies including:



- Nunavut Housing Corporation
- Community and Government Services (2)
- Culture, Language, Elders & Youth
- Human Resources

Public institutions require a strategy when it comes to making public data more accessible, and we believe that Access by Design provides the roadmap. The U.S. and the U.K. have made great progress in this area and there is no reason why other jurisdictions, including Ontario, can't do the same.

- Brian Beamish
Assistant Commissioner for Access for Ontario in commenting on the Access by Design project.



REVIEW RECOMMENDATIONS MADE

There were two Review Recommendation issued in 2010/2011.

Review Recommendation 10-50

Security is a process, not a product. Hackers are innovative, and security practices need to be constantly enhanced to protect confidentiality. Security is also a balance between ease of use and absolute protection. The most secure library in the world -- and the most use-less -- would be one that never loaned out any books.

- John D. Halamka,
(Computerworld), October 5, 2009

In this case, the Applicant was seeking information about the Education Leave granted throughout the Territorial Government. The Applicant was seeking detailed information about which departments had granted long term education leave, what programs leave was granted for, how long the employee who received leave had been employed at the time that leave was granted and the percentage of salary paid to the individual granted leave, among other things. The Applicant received the information requested only from one department and was not satisfied with the amount of information he received. From the public body's perspective, they were concerned about protecting the personal privacy of the individuals who had received educational leave. They were trying to find a way to provide the Applicant with the specifics he required without revealing the names of the individuals who had received the benefit or the studies they had undertaken.



In completing the review, the Information and Privacy Commissioner pointed out that both sections 23(4)(e) and 23(4)(h) of the Act provide specifically that it is NOT an unreasonable invasion of a third party's privacy to disclose the details of a discretionary benefit received by them and that it seemed fairly clear that educational leave was a discretionary benefit . As a result, the disclosure of the fact that an individual received Educational Leave benefits and even the amount of benefit he/she received would not, by itself, constitute an unreasonable invasion of privacy.

First, don't say it unless you mean it. Don't toy with us. Don't toss "open," "accountable," "transparent" at us unless you intend to follow through. Someone might actually remember that you promised it and they might actually call you on it.

- Frank Work, Alberta Information and Privacy Commissioner
Edmonton Journal, July 7, 2011

The most vital piece of information that the Applicant was seeking was the partial allowance in lieu of salary paid to each employee receiving Educational Leave for the term of the leave approved. The IPC concluded that this information could be disclosed without disclosing anything that would constitute an unreasonable invasion of anyone's privacy. Because Educational Leave is a discretionary benefit, and the disclosure of the range of pay for employees is not to be considered an unreasonable invasion of a third party's privacy, the IPC suggested that the following information could be disclosed:

- a) the Department that the application was made to
- b) pay range for the employee at the time the application was made
- c) the length of time for which the Education leave was granted
- d) how long each employee had been an employee when Education leave had been granted (in yearly increments)



- e) the partial allowance in lieu of salary (expressed as a range - eg. between 30 and 40 percent of pay or between \$30,000.00 and \$40,000.00)
- f) the terms of reference for all Departments' Education Leave committees.

The recommendations were accepted.

Review Recommendation 10-51

It's deeply ironic and hypocritical to keep the briefing book for the minister of democratic reform a secret. It just shows the cult and culture of excessive secrecy of this government.

-- Duff Connacher, founder and co-ordinator of Democracy Watch

In this case the Complainant was upset because he felt that his former supervisor within a public body had disclosed information about him to his detriment. In particular, he accused his former supervisor of telling various persons outside of the workplace that his employment had been terminated and that, as a result of this unreasonable breach of his privacy, he suffered not only unnecessary embarrassment, but financial damages as well.

After completing her investigation, the IPC concluded that outside agencies did become aware that the Complainant had been dismissed from his employment. However, she could not conclude one way or the other how that information came to be known -- whether the Complainant did it himself or whether there was an assist in one or more instances from his supervisor. She noted, however, that in very small communities, it is very difficult to keep secrets of any kind and commented that it is, therefore, even more important in these communities that extra care be taken to protect



employee information and to emphasize to supervisors again and again that this kind of information must remain confidential, particularly in terms of casual remarks made outside of the work place, whether in passing or in some other context.

The recommendations were accepted.

The best defence [for a democracy, for the public good] is aggressiveness, the aggressiveness of the involved citizen. We need to reassert that slow, time-consuming, inefficient, boring process that requires our involvement; it is called 'being a citizen.' The public good is not something that you can see. It is not static. It is a process. It is the process by which democratic civilizations build themselves.

- John Ralston Saul



LOOKING AHEAD

Privacy is not just a function of the raw quantity of information available about each of us, but of the control we exercise over that information. To be sure, it may seem that we have less of that as well when any scrap of data that appears on the Internet can so easily be copied and circulated. But for the generation that came of age online, those scraps of data are often part of a very conscious public performance of identity. Not necessarily a performance all of them will be eager to own ten years down the line, but a performance all the same.

- CATO@Liberty, January 11, 2010, No Privacy Please, We're Millennials, Julian Sanchez

Historically, I have used this part of my Annual Report to make recommendations for changes which would improve the administration of the Act and to suggest steps that should be taken to better meet the goals articulated in the *Access to Information and Protection of Privacy Act*. It is frustrating, to say the least, when year after year, these recommendations come to nothing. This year, therefore, I will focus on only one recommendation for change - the one which I consider most critical to ensure that the fundamental purposes of the Act can be met - privacy oversight.

The *Access to Information and Protection of Privacy Act* sets out the rules and regulations with respect to how government can collect, use and disclose personal information. One of the goals of the Act is to ensure that the personal information that public bodies collect is used only for the purposes it is collected and that it is not disclosed except in accordance with the Act. The rules are clear and focused. Unfortunately, however, they are unenforceable. There is absolutely no mechanism provided for in the Act to ensure compliance or allow redress when the rules are not followed. The only provision which deals with the consequences of a breach of the privacy rules under the Act is Section 59 (1) which provides that any person who “knowingly” collects, uses or discloses personal information in contravention of the Act or the regulations is guilty of an offence punishable on summary conviction and liable to a fine not exceeding \$5,000. This does not serve as a deterrent, nor encourage public



bodies to give the privacy protections inherent in the Act the attention they deserve.

The government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears," said his memo to the heads of departments and agencies.

= President Barack Obama,
January 22nd, 2009

Furthermore, most privacy breaches are not intentional but are a result of poor policy or poor enforcement of policies, or a simple lack of attention and focus. These are not issues that can be addressed by section 59(1) which requires a willful act. In virtually all privacy complaints I have received to date, the privacy breach was unintentional or inadvertent or simply done without thought about the privacy implications. This doesn't make the breach any more acceptable or any less harmful to the individual whose privacy has been breached, but the Act provides no redress and no solution.

Secondly, in order for Section 59 to apply, someone must take the step of having a charge laid under the act and prosecuted by someone. That is unlikely to happen except in most egregious of circumstances.

Thirdly, fining someone for intentionally contravening the Act will not focus attention on problems in a way that will encourage review and changes so as to prevent the same kind of breach from happening again.

What is completely missing from the privacy piece is oversight - a way to monitor the way government agencies collect, use and disclose personal information. Independent oversight will allow gaps and problems to be identified and recommended solutions can be



made to address those imperfections with new policies, procedures and education. The technologies of today's world put a premium on the value of personal information. Although it seemed for some years like the public was not terribly concerned about how much of their personal information was available and to whom, evidence is mounting that the public is very much aware of their privacy rights and are seeking to claw back control of how their personal information is used.

Remember, the whole idea of the Freedom of Information and Protection of Privacy Act is to ensure that the public has access to information held by government. This information does not belong to government, it belongs to the people who elected you and they deserve to know what you are doing and how you are doing it.

- Frank Work, Alberta Information and Privacy Commissioner
Edmonton Journal, July 7, 2011

If the privacy rules were thought important enough to put into the legislation, they are important enough to deserve a way in which to monitor and assess whether they are being followed. I therefore, once again, recommend that amendments be made to the Act to allow for a review process where there is a concern that someone's personal information has been improperly collected, used, or disclosed. Although the Government of Nunavut's response to the Standing Committee on Oversight of Government Operations has, in the last two years running, acknowledged the need for privacy oversight, there has been little or no progress on addressing the issue on a practical basis.

The fact that I am focusing on this one recommendation does not change my position on the other recommendations made in years past. They remain active recommendations which I hope, in time, will be addressed in some positive fashion.