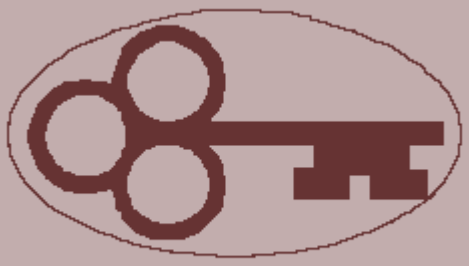
Information and Privacy Commissioner of Nunavut

ANNUAL REPORT

2011/2012



NUNAVUT
INFORMATION
AND
PRIVACY
COMMISSIONER
[illegible]
P.O. Box 382
Yellowknife, NT
X1A 2N3

October 4, 2012

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, 2011 to March 31st, 2012.

Yours truly,

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner

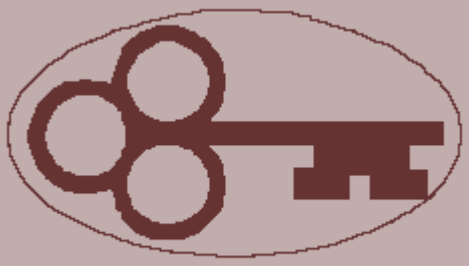
In Yellowknife: 867-669-0976 ♦ Toll free: 888-521-7088 ♦ Fax: 867-920-2511 ♦ E-mail: AtippComm@theedge.ca

INDEX

COMMISSIONER'S MESSAGE

The Access to Information and Protection of Privacy Act is an important component of the balance which is democratic government. In Sweden, the Freedom of the Press Act of 1766 granted public access to government documents. It thus became an integral part of the Swedish Constitution, and the first ever piece of freedom of information legislation in the modern sense. That act created the "Principle of Public Access" which remains the basic principle of all access to information legislation to this day. That principal provides that the general public are to be guaranteed an unimpeded view of activities pursued by government and local authorities; all documents handled by the authorities are public unless legislation explicitly and specifically states otherwise, and even then each request for potentially sensitive information must be handled individually, and a refusal is subject to appeal. In Canada the first ATIPP legislation was implemented in 1983 at the federal level, closely followed by each of the provinces and territories. Our act came into force in 1996, prior to division and was carried over from the Northwest Territories in 1999 at the time of division.

So much has changed since 1766. Eighteenth century Swedes could never have imagined today's world of electronic information, email, the internet, social networking or the ability to gather and manipulate data the way that is commonplace today. Even when our *Access to Information and Protection of Privacy Act* was passed in



Any man who would exchange liberty
for security deserves neither.

Benjamin Franklin

1994, we lived in a very different world. Today, modern technology has made information one of the most valuable resources there is and, as noted by Suzanne Legeault, Information Commissioner of Canada in her 2009/2010 Annual Report, "In a knowledge-based economy, public sector information is essential to foster collaboration and innovation among public sector organizations, individuals and businesses."

While the world has changed, those important first principals remain relevant and, in fact, essential to maintaining democratic government today.

The purposes of the Act, as stated in its very first section, reflect the Principles of Public Access as established by the Swedes in 1766. Section 1 states:

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

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

While access to information is the life blood of democracy, in today's information age, perhaps even more important is the protection of personal information held by government agencies. As noted by the Supreme Court of Canada in *R. v. Duarte* [1990] 1 S.C.R. 30 at 46, Canadians have a right to informational privacy - "the right of the individual to determine for himself when, how and to what extent he will release personal information about himself."

After my last Annual Report, the Government of Nunavut committed to making changes to the Act so as to finally include independent oversight of privacy breaches and privacy complaints as part of my mandate. I was very happy to see these changes proposed and expect that I will be able to report in my next Annual Report that Nunavut has joined the rest of the country in providing a means for the public to challenge public bodies who fail to abide by the privacy provisions in the Act. The next step, I hope, will be to establish new legislation to deal with the special challenges which arise in connection with personal health information.

When Parliament explicitly sets forth the purpose of an enactment, it is intended to assist the court in the interpretation of the Act. The purpose of the Act is to provide greater access to government records. To achieve the purpose of the Act, one must choose the interpretation that least infringes on the public's right of access.

Canada (Information Commissioner) v. *Canada (Immigration & Refugee Board)* (1998), 140 F.T.R. 140 (Fed. T.D.) at 150,

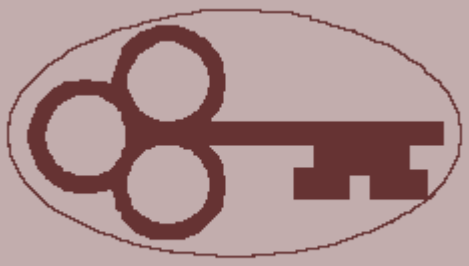
THE ACT

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 rules about 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.

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 application 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 Information and Privacy Commissioner can be only be removed from office "for cause or incapacity" on the recommendation of the Legislature.

ACCESS TO INFORMATION

The Act provides the public with a process to obtain access to most records in the possession or control of the various departments of the Government of Nunavut or



Terrorism isn't about identity; it's about motivation.

Lembit Opik, Northern Ireland

one of a number of other public organizations. Generally, 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.

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.

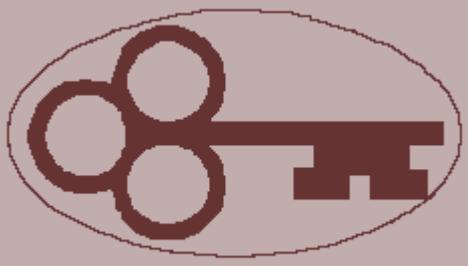
When a request for information is received, the public body has a duty to identify all of the records which are responsive to the request. Once all of the responsive documents are identified, they are reviewed to determine if there are any records or parts of records which are protected from disclosure 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 over decisions made by public bodies in Nunavut in relation to requests for information made under the *Access to Information and Protection of Privacy Act* .

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.



> Once a government is committed to the principle of silencing the voice of opposition, it has only one way to go, and that is down the path of increasingly repressive measures, until it becomes a source of terror to all its citizens and creates a country where everyone lives in fear.
> --Harry S. Truman

PROTECTION OF PRIVACY

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.

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 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 mis-

leading 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.

In Nunavut, the Information and Privacy Commissioner has had 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 has routinely accepted complaints and undertaken investigations when complaints have been made about breaches or perceived breaches of privacy. These complaints are investigated and recommendations have been provided. Amendments to the legislation introduced in 2012 will soon give the IPC the formal legislative power to undertake such reviews.

Freedom of Information is also part of the constitutional settlement. It's a reminder that Governments serve the people, and not the other way around. It's a reminder that what Government does in our name, on our behalf, and with our money, is a matter of public interest.

Richard Thomas, UK Information Commissioner, 2005

THE YEAR IN REVIEW

The 2011/2012 fiscal year was a much busier one for the Information and Privacy Commissioner's Office than the last number of years. We opened 22 new files during the year, compared with only 5 the previous year. The files can be divided into a number of categories:

Requests for Review - Access to Information	14
Requests for Comment	4
Requests for Review - Privacy Issues	2
Request for Correction to Personal Information	1
Administrative	1

A significant number of the Access to Information review matters resulted from an initial failure on the part of the public body to respond to the request for information within the required 30 days. Most of those were either eventually withdrawn by the Applicant when the public body did respond, or were resolved without any order or recommendation being made.

No one public body was over represented in the access to information review requests. Community and Government Services, Economic Development and Transportation and Qvlliq were each involved in two matters which came before me.

REVIEW RECOMMENDATIONS MADE

There were six Review Recommendation issued in 2011/2012, up four from the previous year.

Review Recommendation 11-52

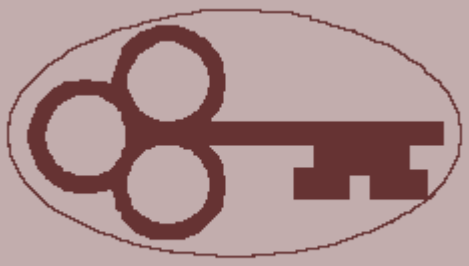
This matter arose as a result of a request for information made to the Nunavut Housing Corporation by a member of the press, who was seeking those sections of the briefing binder given to Tagak Curley upon his take over of ministerial responsibility of the Nunavut Housing Corporation pertaining to four program areas.

The public body refused access to any of the responsive records on the basis of section 14 (1)(a) and (b) which provides public bodies with the discretion to refuse to disclose records which constitute advice to officials, specifically,

(a) advice, proposals, recommendations, analyses or policy options developed by or for a public body or a member of the Executive Council;

(b) consultations or deliberations involving a member of the Executive Council, or the staff of a member of the Executive Council.

The public body in this case applied a blanket exemption to all of the responsive documents (a total of 15 Briefing Notes and 78 pages). They acknowledged that they had made no effort to review the records to see if there was any portion of



Privacy is the right to be alone - the most comprehensive of rights, and the right most valued by civilized man.

Louis D. Brandeis

them which did not fall under the exemptions. Neither did they really exercise any discretion. They simply concluded that because these records were titled “briefing notes” they fell under section 14 and would not be disclosed.

I reviewed each record, page by page, and analyzed them in accordance with the principles set out in Order F2004-026 made by the Alberta Information and Privacy Commissioner in discussing Alberta’s equivalent to our section 14. In that case, the Information and Privacy Commissioner of Alberta noted:

> Earlier decisions of this office have considered the circumstances under which the criteria in these provisions apply. Order 96-006 said that to determine if section 24(1)(a) [then section 23(1)(a)] will apply to information, the advice, proposals, recommendations, analyses or policy options ("advice"), should:
>
> 1. be sought or expected, or be part of the responsibility of a person by virtue of that person's position,
> 2. be directed toward taking an action,
> 3. be made to someone who can take or implement the action.

In the same Order, the Information and Privacy Commissioner accepted that the purpose of this exemption was to "allow persons having the responsibility to make decisions to freely discuss the issues before them in order to arrive at well-reasoned decisions" and that ‘the Head should exercise the discretion to withhold documents where disclosure would defeat the purpose of this section.

Having reviewed all of the responsive records, I concluded that most, if not all of the responsive records met the first and the third requirements of section 14 as set out above. Very little contained in the records, however, was "directed toward taking an action". The contents of the records were factual and informative in nature only. They contained, for the most part, facts and figures, and in some cases an explanation for choices and decisions already made and some projections and forecasts. There was no suggestion that any actions or even discussions were expected or intended to arise out of the Briefing Notes.

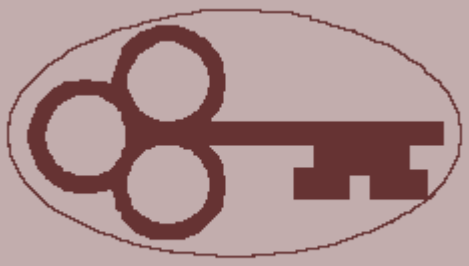
As a result, I recommended that the records be disclosed to the Applicant, with only very limited sections edited where those sections contained discussion on possible options for moving forward.

The recommendations were accepted.

Review Recommendation 11-53

In this case, an Applicant made a request for records from the Department of Community and Government Services (CGS) for records relating to contracts awarded and amendments made to existing contracts for Arctic Resupply, including the metric volume of cargo transported for a five year period.

Access to a number of the responsive records was denied based on several sections of the Act, but primarily section 24 (information the disclosure of which could



When government organizations use the services of individuals or companies in the private sector, the public should not lose its right to access this information.

Ann Cavoukian, Ontario IPC

reasonably be expected to affect the financial or competitive position of third parties). The public body argued that, in order to ensure that the RFP process is fair and that contracts are awarded to those best able to provide the services required, CGS requires that companies divulge a lot of proprietary information in their proposals such as pricing discounts and the use of Inuit Labour and Training programs. They argued that this information is provided in confidence and that the disclosure of this information to other companies or the public may harm the business interests of the contractors. .

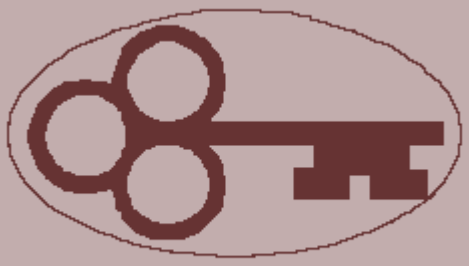
The Applicant argued that the "blanket" application of section 24 to deny access to entire contracts is not in accordance with the Act. Further, he pointed out that no evidence was provided to support the assertion that the information requested was commercially confidential or that the competitive positions of the Third Parties would be compromised by its disclosure. The Applicant emphasized the need for public bodies to be accountable to the public with respect to the granting of large contracts and argued that most Canadian jurisdictions disclose contracts such as these as a matter of routine practice.

I concluded firstly, that the public body had not properly identified all of the responsive records. In particular, rather than provide the relevant records related to the extension of the contracts in question to the Applicant as requested, the public body simply provided the Applicant with confirmation that extensions had been granted. It seems to me that an extension of a contract would require something in writing and most likely some correspondence back and forth between the Third Party com-

panies and the public body. It was not sufficient merely to provide confirmation that there had been an extension. Furthermore, based on the documents provided by the Applicant which he received from another public body in response to a separate Request for Information, it was clear that there were records which originated with CGS which were not identified or disclosed.

I further concluded that it was not appropriate to apply a blanket exemption to any one record. There must be a line by line review of every record and, insofar as it is possible to sever those parts of the record that are subject to an exception to disclosure, those parts should be severed and the remainder of the record disclosed. In most cases, there is not a lot of proprietary information in contracts involving the government and a Third Party. Proprietary information is information which originates from the Third Party, such as unit prices, technical requirements, labour information and the like. To the extent that this information is contained in government contracts, it is usually included as an appendix and does not form any part of the main body of the contract.

In order to determine whether or not the disclosure of certain information might negatively impact on the financial or competitive position of a third party, I concluded that in most cases, it would be necessary to consult the third parties who might be affected. In this case, therefore, I contacted the three Third Parties involved to advise them of the request and to ask them for their input. Two of the three Third Parties responded and indicated that they had no real objection to the disclosure of the information requested, except for certain, specific information. The third Third



Party did not respond at all, which suggests that they had no significant objections to the disclosure.

I therefore recommended:

a) that the public body begin its search again and that it identify ALL records responsive to all parts of the Applicant's request, including not only paper records, but electronic records and e-mail records as well.

b) that once ALL responsive records have been identified, the public body should compile a list or index of all such records and to the extent that the search identifies records not previously identified, I recommended that these records be fully vetted in accordance with the Act and that there should be a further disclosure to the Applicant, including a detailed explanation as to the reasons for any records not disclosed, either in whole or in part.

c) I recommend that the contracts which are the subject of this Request for Information be reviewed on a line by line basis and that they be disclosed to the Applicant, subject only to severing any information that is proprietary in nature.

The recommendations were accepted in part. They also chose to do a further consultation with third parties before disclosing the records requested.

Data protection is crucial to the upholding of fundamental democratic values: a surveillance society risks infringing this basic right.

Thomas Hammarberg, Council of Europe's Commissioner for Human Rights

Review Recommendation 11-54

This review involved a request for a report which had been prepared by the Department of Executive and Intergovernmental Affairs (E.I.A.) in response to a grievance filed by the Applicant (an employee of the GN) under the Public Service Act. The pubic body disclosed part of the record, but chose to redact certain portions of the report, relying on several sections of the Act, specifically, sections 14(1)(a) (the disclosure could be reasonably expected to reveal advice, proposals, recommendations, analysis or policy options developed by or for a public body or a member of the Executive Council) and 23 (unreasonable invasion of a third party's personal privacy).

After doing a line by line review of the report, I recommended that some of the redacted portions of the report be disclosed.

My recommendations were accepted

Review Recommendation 12-55

In this case, the Nunavut Employees Union (NEU) requested information in relation to the terms and conditions of the resignation of one of its members. In making the request, the union provided a letter from it's member consenting to the disclosure of the information requested. The request resulted in the disclosure of one piece of paper, which appears to be a copy of a hand written letter from the Union Member

in which he asks the employer to accept his resignation as of 5:00 pm on the date of the letter. Access to a number of "related records" was denied on the basis that the disclosure would constitute an unreasonable invasion of A.B.'s privacy.

In dealing with the review, the public body explained that the circumstances surrounding the employee's resignation were such that criminal proceedings were being contemplated against him. They were concerned that, although the employee had provided a consent to the disclosure, in the circumstances they had concerns about whether it was an informed consent because of the criminal implications. The public body's motive was to protect the integrity of the employee, not to circumvent the ATIPP process.

There was no indication that the public body had followed up with the employee to confirm the nature and extent of the consent given. Nor did they follow up with the union to ask them to provide evidence that the employee's consent was fully informed. Rather, the public body simply decided that they didn't think that the employee really wanted the information disclosed and refused to disclose it to the union. I suggested that, in such circumstances, the appropriate thing for the public body to do would have been to contact the employee to make sure that he understood the nature and extent of his consent and the possible consequences of such disclosure or to require a more specific consent from the Applicant union. I made the following recommendations:

a) that the public body follow up directly with the employee to ensure that his consent to the disclosure of his information to the union was fully informed;

b) in the alternative, that the public body require the Applicant (NEU) to provide a more specific consent which would satisfy a reasonable person that the employee was aware of his right to refuse his consent and that the records requested may reveal information that could have a negative impact on him;

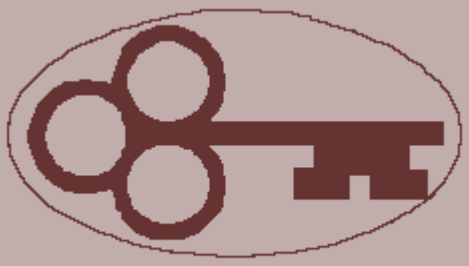
c) that upon receipt of a new consent, the responsive records be disclosed to the Applicant;

d) if not already done, that the Government of Nunavut develop a form of consent that can be used (on a non-mandatory basis) by third parties to provide their consent to the disclosure of their personal information to an Applicant which includes the necessary cautions about the possibility of further disclosure.

The recommendations made were accepted.

Review Recommendation 12-56

This review recommendation resulted from a complaint about a perceived breach of privacy. The Complainant was a former employee of a public body who had recent-

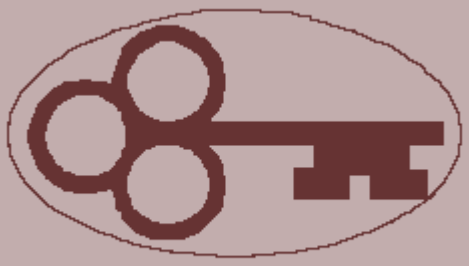


ly been laid off or fired, Some weeks later, when he was having a conversation with an acquaintance, the acquaintance pointed to a man standing some distance away and asked if the Complainant knew him. The reason for the inquiry was that the individual noted had been talking to the acquaintance about the Complainant and the fact that he had been fired from his job with the public body. The Complainant had not told anyone he had been fired and came to the conclusion that the stranger had some kind of relationship with his former manager and surmised that the manager must have improperly disclosed his personal information.

The public body investigated but could find no direct evidence that the supervisor or anyone else had disclosed the Complainant's information. They specifically asked the Complainant's supervisor about the matter, who denied ever having discussed the Complainant with anyone outside of the workplace. The Department also outlined the policies and safeguards in place to ensure that personal (and other) information obtained in the course of employment is not improperly used or disclosed. In particular, they pointed to the following safeguards:

a) the Government of Nunavut Code of Conduct which prohibits employees from taking advantage of, or benefit from, confidential information gained as a result of their official duties, which binds all GN employees;

b) the Oath of Office and Secrecy which every GN employee is required to take upon being employed and to abide by



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.

President Barrack Obama, January 22nd, 2009

c) the division itself also has its own additional Code of Ethics, posted at all work sites, which requires employees to properly safeguard all documents, reports, directives, manuals and other information.

d) the Department of Human Resources holds regular orientation sessions for new GN employees, which include an introduction to the *Access to Information and Protection of Privacy Act.*

While there were some circumstantial indications that the supervisor and the stranger were acquainted, I concluded that there really was no way to confirm with any degree of certainty that he had been the source of the disclosure about the Complainant's job situation. I could not find, therefore, that the complaint was well founded.

Notwithstanding that, however, I took the opportunity to remind all pubic bodies that, while policies and codes of conduct are good, they are not sufficient to ensure that all employees will comply. What is needed in order to ensure ongoing respect for those policies and oaths is consistent messaging and positive reinforcement. While most GN employees appreciate and understand the requirement not to disclose the personal information of third parties, people gossip. The communities in Nunavut are small places. Once the information gets out, it won't take long for it to be widely known. It is human nature to talk about things that happen to us, around us and about people around us. It is important, therefore, that all public bodies are vigilant in reminding employees, again and again, that privacy rules and policies apply not only to third parties who use government services, but also to fellow employees.

REVIEW RECOMMENDATION 12-57

The Applicant in this case made a Request for Information from the Department of Education for all email correspondence between certain named individuals within a specific time frame. The Department responded to the Applicant indicating that they were unable to locate any e-mail correspondence that was responsive to the Applicant's request. The Applicant was not satisfied with the response received and asked me to review the matter.

I asked the public body to explain how they searched for responsive records. They advised me that only one of the individuals named in the request was their employee, so they limited their search to that individual's email records. The search was then done by keyword searches, using each of the other names in the list individually. Although they did find some email correspondence between the individuals noted in the Request for Information, all such email was outside of the time period noted in the Request for Information. As a result, they responded to the Applicant by advising that there were no responsive records.

I was satisfied that the public body's search was adequate and that there simply were no records which were within the parameter's of the Applicant's Request for Information. I therefore recommended that no further action be taken with respect to this request.

My recommendation was accepted.

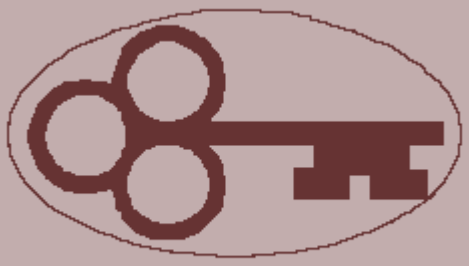
LOOKING AHEAD

I am very pleased that my major recommendation for 2010/2011 has resulted in the passage of an amendment to the *Access to Information and Protection of Privacy Act* to provide the Information and Privacy Commissioner with a formal oversight function in relation to complaints about breaches of privacy. This is a huge step forward, bringing Nunavut into line with the rest of the country.

There is, however, still a need to address the special circumstances surrounding personal health information. This spring I was surprised to learn, through the press, about a health surveillance system in which all babies born in Nunavut and all mothers will be "followed" from gestation to up to five years through a program described as a maternal–child health information system. I completely understand and applaud the goals of this project, and understand the need to gather the information necessary to have healthier children in Nunavut. I was, however, surprised that, despite the fact that this program has the potential to be highly invasive of personal privacy, there was no attempt to involve my office in the consultation process leading up to the implementation of the program, to address the those privacy issues. It appears from what I have read about the program since learning about it, that the plan is to collect the information locally then to remove personal identifiers from the data when it is transferred from the community health centre to the data centre collating the information. That said, a unique identifier will be attached to the data to allow "accurate longitudinal collection of information". It would, therefore, be

a fairly simply process to trace the information back to the individual. There are no real controls over how this information is utilized or how the use of the information might change in the future. Nor is there any indication that there is any intention to inform mothers about the fact that their personal information is being collected or used for a purpose outside the scope of that for which it was provided or to obtain the mother's consent to this use of her own and her child's personal health information. Finally, because the communities are so small, even without personal identifiers, it will often be able to identify the individuals merely from the facts and community.

This is only one small example of why health privacy issues are far more complicated than when dealing with other kinds of personal information. I have heard, anecdotally, about a number of troubling situations in which the health information of Nunavut residents has been improperly used or disclosed. Furthermore, within the strict reading of the *Access to Information and Protection of Privacy Act* personal health information can only be used "for the purpose it was collected" and there are some real questions about what that means and how far that can be stretched in terms of it's use. With the advent of electronic health records, this is going to become more and more of an issue. Most other Canadian jurisdictions have or are working on health privacy legislation to address the unique challenges presented by health information. As noted in my opening comments, the Supreme Court of Canada, way back in 1990 recognized the importance of "informational privacy" which it defined as "the right of the individual to determine for himself when, how and to what extent he will release personal information about himself". (*R. v. Duarte*

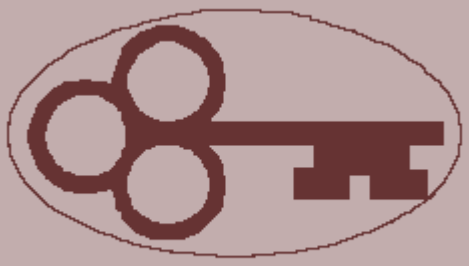


Public bodies need to show they recognize the imperative of accountability (and make lives easier for themselves) by identifying what absolutely has to be kept secret and then proactively publishing other official information as a matter of routine.

Richard Thomas, UK Information and Privacy Commissioner, 2009

[1990] 1 S.C.R. 30 at 46). This is never so true as when we are talking about personal health information. Health privacy legislation needs to be on the legislative agenda as soon as possible.

Once again, I would also encourage the Government of Nunavut to find a way to provide municipalities with some rules and policies on access and privacy matters. While I have, in the past, advocated that municipalities be included as public bodies under the Act, that may be something to aspire to rather than something that is possible today. In the spring I had the opportunity to meet with and discuss access and privacy issues with a number of officials from the City of Iqaluit. All of them were keen on establishing an access and privacy regime within the municipality. They were, however, candid in admitting that their information management system would not be up to the task of responding to a historical access request. Nor were they confident that their current practices, even, would stand up to the requirements. Perhaps, then, a start, is to provide municipalities with some assistance in creating appropriate policies and guidelines with respect to both access to information and privacy matters and help in establishing adequate information management systems so as to allow an eventual inclusion under the *Access to Information and Protection of Privacy Act*. The primary requirement to be able to adequately respond to access to information requests is an information management system that allows easy review of historical records. It is important for municipalities to start working toward proper record keeping so that, in time, they can be called upon to provide public records to the public in an efficient and effective way. While they may not currently be up to that task, the process has to start somewhere. I would



encourage the appropriate government department to work with the municipalities in a formal way to move toward the day that they can be included under the ATIPP Act.

> "In a government of responsibility like ours where the agents of the public must be responsible for their conduct there can be but a few secrets. The people of this country have a right to know every public act, everything that is done in a public way by their public functionaries. They are entitled to know the particulars of every public transaction in all its bearings."
>
> *State of UP vs Raj Narain*, Supreme Court of India, 1975