NUNAVUT

19/20

OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER
OF NUNAVUT

Annual Report

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF NUNAVUT

July 26, 2020

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

Attention: Hon. Paul A. Quassa
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, 2019 to March 31st, 2020.

Yours truly,

Elaine Keenan Bengts
Nunavut Information and Privacy Commissioner
/kb

Table of Contents

COMMISSIONER'S MESSAGE

As I sit down to write this, my last Annual Report as the Information and Privacy Commissioner for Nunavut after 21 years in the position, I can think of only one word to describe the year -- interesting. Not interesting in a good way, but interesting in the way contemplated by the old Chinese curse, "May you live in interesting times".

The highlight - or rather the lowlight - of the year was without any doubt the ransomware attack in early November which shut down pretty much the entire GN computer system - not for a few hours or even a few days, but for almost two months. Even today, 9 months later, the GN has not been able to fully restore its systems. Email records, in particular are still not fully recovered or at least the ransomware attack is still being blamed for an inability to produce records for access to information requests.

This attack, and its aftermath, has huge implications for both access to information and for the privacy of Nunavummiut - implications as yet not entirely understood or even recognized. My review of the issues arising out of the attack is proceeding very slowly, in part because those who could answer my questions about the event have been otherwise occupied trying to restore the system.

At the moment, my formal review under the ATIPP Act is focussed on the implications for "access to information". In this regard I have been advised by GN officials with Community and Government Services that everything that was on the servers at the time of the attack had been backed up and could, therefore, be restored. We are, however, still waiting for full restoration of historical emails (emails sent or received prior to the attack). As recently as a week ago I was advised by one department that they were having difficulty recovering some historical emails even with the assistance of IT staff. The number of IT experts within the GN is limited and most of them appear to be pre-occupied with the bigger issues with respect to attack, and then with the requirements to allow employees to work from home during the pandemic. They have had little time to devote to requests for recovery documents to respond to access to information requests. I suppose it was inevitable that the ransomware would be blamed for the inability to find records responsive to access requests and this is playing out now. How prevalent it becomes as an excuse for non-production of records remains to be seen.

The difficulties in accessing historical emails may be close to being resolved but this is not the only access to information issue arising out of the attack. When the ransomware hit, the only way to address it effectively was to wipe every desktop, laptop, jump drive or other device connected to the system. Nothing saved

on a local device was backed up. This means that all records which had been saved on a local device have been irretrievably lost. While policy requires all final documents to be saved on the servers, this leaves a lot of room for missing records, including drafts, and incomplete documents. It would be naïve to think that all employees of all public bodies unfailingly saved all of their work to a server. Anything saved to a local device is still a GN record, subject to an access to information request. These records, however, are no longer available to the public. The *Access to Information and Protection of Privacy Act* applies to ALL records in the custody or under the control of a public body, not just those properly saved on the servers. As my review proceeds, it is my hope that, at the very least, an inventory of lost records can be created for future reference.

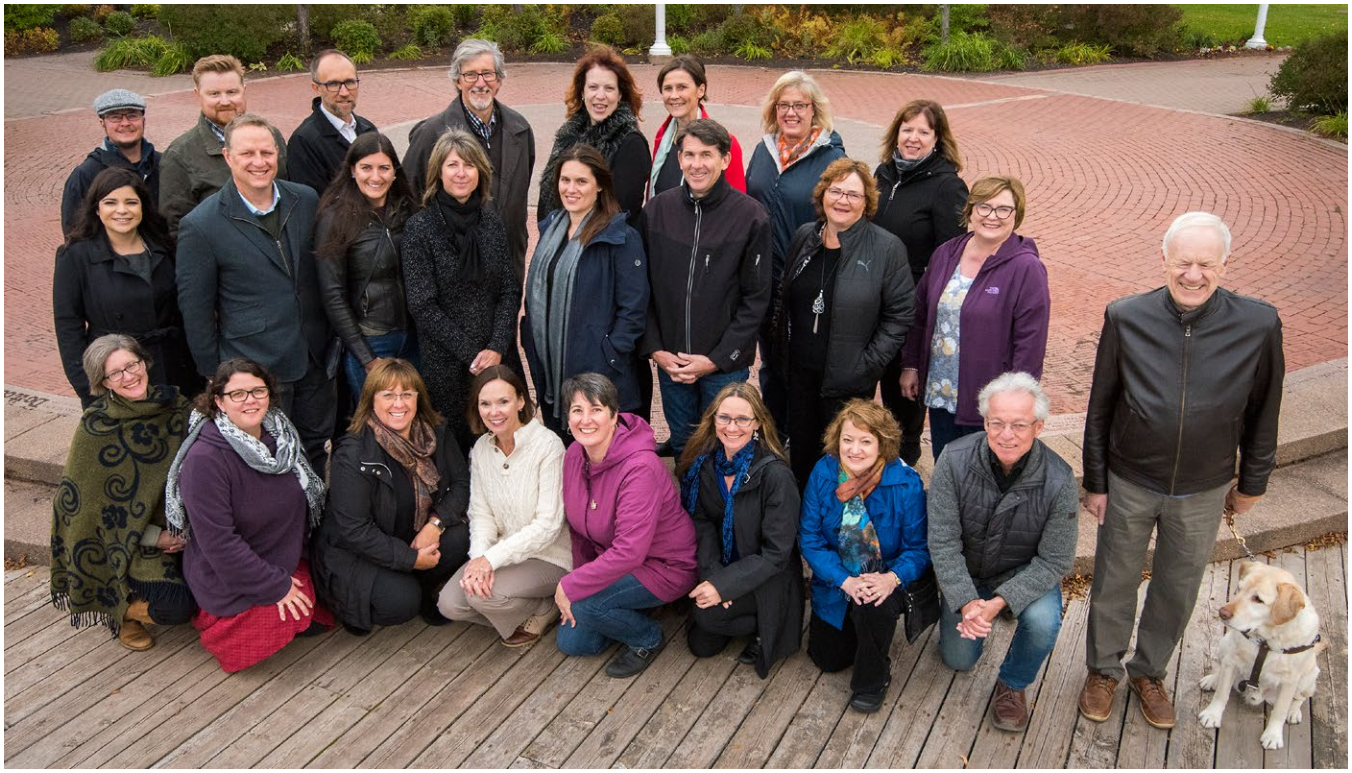
But as if a massive ransomware attack was not enough, a world-wide pandemic fell upon us in the first three months of 2020 and it remains with us today as I write this message in early August. The pandemic sent most GN employees home to work raising a host of new concerns with respect to both access and privacy. These concerns will undoubtedly show themselves over the next months as employees return to the workplace and everyone gets back to our "new normal". Like all other governments in Canada, the GN reacted by instituting new procedures to control the number of visitors to Nunavut (which entails the collection of considerable amounts of personal information), using new technologies for virtual meetings, and providing at least some students with the ability to study virtually. Not all of these processes and procedures or technologies have been fully vetted in terms of their privacy impacts. Privacy rights have not been totally ignored, but have definitely been relegated to being of secondary importance in the response to the challenges of the pandemic. It will be important for governments, including the Government of Nunavut, to pull back on some of these processes and technologies implemented on an "emergency basis" and to fully assess them if the intention is to continue their use in the future. It will also be essential to guard against "function creep" with the use of these new technologies so that we do not find ourselves living in an Orwellian world of constant and ubiquitous surveillance.

As if these events were not challenging enough, the very public death of George Floyd at the hands of police officers in Minneapolis and the huge demonstrations which followed, not only in the United States but also here in Canada, have focussed attention on police transparency and accountability and sounded a renewed call for police officers to wear body cameras. The issue of body worn cameras for law enforcement officers was a live one in Nunavut even before these events, as perceptions have mounted over the last years that the RCMP consistently use more force than necessary to address criminal behaviour. This has led to a call from the public and from politicians to require the use of body worn cameras by RCMP officers in Nunavut. While I completely understand the sentiments behind these calls and agree with the need for greater police accountability, body worn cameras are not the panacea that will fix law enforcement overreach. The use of body cameras raises complex policy issues and huge privacy risks for the public as a whole, including victims and bystanders, without necessarily addressing the issue of police violence. In fact, research

suggests that police worn body cameras do not change police behaviour and footage is more often used against the public than to keep officers honest. I urge caution and careful consideration before Nunavut plunges into a requirement for RCMP in the communities to wear body cams.

In the midst of all this, my term as the Information and Privacy Commissioner for Nunavut officially came to an end on March 31st. The Legislative Assembly has, in my opinion quite rightly, decided that it is time for a full time resident Information and Privacy Commissioner and the search is on. However, the pandemic has slowed the process and I have, therefore agreed to stay in the position on a part time basis until the new Commissioner can be found. As part of this, I have been given the opportunity to write this one last Annual Report and I would like to take the opportunity to acknowledge the dedicated individuals I have worked with over the years, particularly in the Legislative Assembly offices and those who have held the position of Manager of ATIPP in the Department of Executive and Intergovernmental Affairs. It has been my absolute pleasure to work with all of you, even when we have not always seen eye to eye. And, of course, I would be remiss if I did not acknowledge, once again, my assistant, Lee Phypers, whose cheerful demeanor and eye for detail has kept me out of a lot of trouble over the years.

Finally, I would like to welcome the new Information and Privacy Commissioner, whoever that might be, and wish them all the best as they continue the important work of this office.



Annual Federal/Provincial/Territorial Meeting of Canada's Information and Privacy Commissioners, Charlottetown, PEI, August, 2019

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY IN BRIEF

The *Access to Information and Protection of Privacy Act* (ATIPPA) confirms two fundamental rights:

1. the **right** of the public to have access to public records; and
2. the **right** of the public to have the personal information that the Government of Nunavut collects about them individually to be protected from unauthorized use or disclosure.

Of importance here is that the legislation creates not just rules, but **rights** to access public records and to have personal information protected. This legislation outlines how the public can obtain access to public records and establishes limits to how and when public bodies can collect, use and disclose personal information collected and maintained by Nunavut public bodies. It applies to 43 departments, crown corporations, local housing organizations and other agencies in Nunavut.

Access to Information

Part I of the Act gives the public the right to request and receive public records and outlines a process for obtaining such records. This right of access is so important to the maintenance of open and accountable government that access to information laws have been deemed to be quasi-constitutional in Canada. This means that the rights it creates can only be taken away with the clearest of intent and that a conflict between the rights granted by this legislation and rights granted by other legislation will always be resolved in favour of the right to access. When the public can see and test how government is functioning and how it is doing its work, they are better able to participate in government and to hold government and governmental agencies to account. The right of access to government records is not, however, absolute. There are some exceptions to the right of access but these are limited and specific exceptions as set out in the legislation. Most of the exceptions function to protect individual privacy rights and proprietary business information of the companies that do business with the Government of Nunavut. The exceptions also function so as to allow Ministers and their staff to have free and open discussions as they develop policies and deal with issues.

Requests for Information must be in writing and delivered to the public body from which the information is sought. When a Request for Information is received, the public body must first identify all of the records which respond to the request, then assess each record and determine what portion of that record should be disclosed and what might be subject to either a discretionary or a mandatory exception. This is a balancing act which is sometimes difficult to achieve. The response must be provided to the Applicant within 25 business days.

If an Applicant is not satisfied with the response provided by the public body, a request can be made to the Information and Privacy Commissioner to review the response given.

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

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

The over-arching purpose of access to information legislation, then, is to facilitate democracy.

Protection of Privacy

Part II of the Act provides rules for when and how public bodies can collect personal information, what they can use such information for once it has been collected and in what circumstances that information can be disclosed to another public body or the general public. It requires that all government bodies maintain adequate security for the personal information they hold and ensure that only enough personal information is made available only to those who need that information to do their jobs.

This part of the Act also gives individuals the right to ask that the public body correct personal information that is in error.

Part II of the Act also requires public bodies which know or have reason to believe that there has been a material breach of privacy with respect to personal information under its control to report that breach of privacy to the individual whose information has been wrongfully disclosed and to the Information and Privacy Commissioner.

The Role of the Information and Privacy Commissioner

The Office of the Information and Privacy Commissioner (OIPC) was established under the *Access to Information and Protection of Privacy Act* of the Northwest Territories in 1997, prior to division. This legislation was continued in Nunavut on Division Day in 1999. The Information and Privacy Commissioner (IPC) is appointed by the Commissioner of Nunavut on the recommendation of the Legislative Assembly and holds that appointment for a five-year renewable term. This role has been held by Elaine Keenan Bengts since March 2000.

The role of the Information and Privacy Commissioner (IPC) is to provide independent oversight over public bodies as they apply the Access to Information and Protection of Privacy Act. The independence of the role is vital to the work of the IPC as it allows her to openly criticize government, when necessary, without fear of being removed from office.

When someone has asked for information from a public body and is not satisfied with the response received, that person may request a review by the Information and Privacy Commissioner. The IPC is able to see all responsive records and, based on the input of both the Applicant and the public body, will prepare a written report and make recommendations. The Information and

Privacy Commissioner does not have any power to compel public bodies to either disclose records or to protect information from disclosure but she is required to provide the Minister of a department or the CEO of a public corporation with recommendations. The Minister or CEO must decide to either accept the recommendations made or to take such other steps as they deem appropriate, within 30 days. The Applicant has the right to appeal the Minister's or CEO's decision to the Nunavut Court of Justice if there continues to be a dispute as to the proper application of the Act to the records in question.

The Information and Privacy Commissioner is also authorized to investigate privacy complaints, including complaints about the failure or refusal of a public body to make a correction to an individual's personal information. Any person may file a complaint about a privacy issue with the Information and Privacy Commissioner. The IPC will investigate and prepare a report and make recommendations for the Minister or CEO.

The Information and Privacy Commissioner is also authorized to initiate an investigation of a privacy issue of her own accord when information comes to her attention which suggests that a breach of privacy may have occurred.

As in the case of an Access to Information review, the Minister or CEO of the public agency involved must respond to the recommendations made by the Information and Privacy Commissioner in privacy breach matters. In these cases, however, the Minister or CEO has 90 days to respond, and there is no right of appeal from the decision made.

The Protection of Personal Information

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

Building Canada's Information Economy and Society Industry Canada, Justice Canada

January, 1998

THE YEAR IN REVIEW

It was another busy year for the Office of the Information and Privacy Commissioner. We opened a total of 46 new files, up about 35% from 2018-2019. The office issued 18 Review Reports, significantly more than last year's 8 reports. In addition to Review files, we also received 12 requests for our office to provide comment on the privacy impacts of a number of pieces of legislation, policy options and other privacy related issues.

The files opened fell within the following general categories:

Access to Information Matters

- General Requests for Review 1
- Deemed Refusal 1
- Fees 1
- Out of Scope (City of Iqaluit) 1

Privacy Related Matters

- Breach Notifications from Public Bodies (section 49.9(1)) 18
- Privacy Breach Complaints 9

Request for Comment/Consultations 12

Administrative..... 2

Miscellaneous 1

This represents a significant drop in the number of access to information matters reaching my office. I suspect that this has something to do with the ransomware attack in November which virtually shut down the GN's ability to respond to an access to information request for at least two months and which is still affecting the ability to access historical email records. This disaster was followed in quick succession by the COVID-19 pandemic response which sent most GN employees home to work, seriously affecting their ability to access public records to respond to access requests. Nunavummiut have been very patient for many months but that patience has begun to wane in the last few months. I suspect that we will see a huge uptick in the number of files related to access to information matters in fiscal 2020-2021 as we begin to see people returning to work.

Almost all of the breach notifications received pursuant to section 49.9(1) originated in the Department of Health. This is not surprising as the Department of Health is likely one of the only sectors of the GN which readily recognizes a privacy breach, or a contravention of the privacy provisions of the Act, even when those breaches are relatively small, as, for example, when a document containing personal health information is faxed to the wrong place. I would like to commend the Department of Health for its efforts to recognize and report these breaches to my office. Every recognized breach allows us to learn more about what needs to be changed so as to prevent future breaches.
I continue to be concerned about the very few number of breach notifications I receive from other public bodies. It would be naïve to think that other departments do not experience privacy breaches on a regular basis or that these privacy breaches are all so small as to be below the threshold of a "material" breach which must be reported to the Information and Privacy Commissioner. In today's digital world, it takes very little to make a breach "material" as defined in the legislation. All public servants, in my opinion, should be trained on how to recognize a privacy breach and on how to respond to a privacy breach so that we can start to address the causes and create solutions to prevent them in the future. As I noted in last year's Annual

Report, privacy breaches, if not acknowledged and addressed, will result in the erosion of trust in government. Understanding weaknesses in policies and procedures that contribute to privacy breaches allows for the identification of the means and ways to address those weaknesses proactively, so they don't continue to weigh down and distract from the important work of providing services to the public, while giving the public confidence that they can share their personal information and personal health information with public bodies safely.

REVIEW REPORTS

The Office of the Information and Privacy Commissioner issued 18 Review Reports in 2019-2020

Review Report 19-149

Category of Review: Access to Information

Public Body Involved: Department of Health

Sections Applied: Section 1, Section 14(1)(a), Section 14(1)(b)(i), Section 15(a) Section 23

Outcome: Recommendations fully accepted

The Applicant requested copies of his own personal information in relation to his employment with the Department of Health. The Department provided responsive records but withheld information from many of those records pursuant to sections 14, 15 and 23 of the Act. The Applicant sought a review.

The Information and Privacy Commissioner (IPC) reviewed the principles behind each of the exceptions relied on by the Department and applied that analysis to those portions of the responsive records withheld. She recommended the disclosure of additional information, particularly information withheld pursuant to section 23 (presumed unreasonable invasion of privacy), and that discretion be properly exercised with respect to information withheld in reliance on discretionary exceptions.

Review Report 19-150

Category of Review:

Access to Information - Deemed Refusal

Public Body Involved:

Department of Family Services

Sections Applied: Section 1, Section 7, Section 8, Section 11, Regulation 13(1)

Outcome: Recommendations Accepted

The Applicant requested his own personal information from the Department of Family Services on May 7th, 2018. The public body wrote to the Applicant on May 11th, within days of receiving the Request for Information, requesting clarification from the Applicant and indicating that the request would be "put on hold" until that clarification was received. The Applicant responded to this correspondence on May 22nd, re-iterating his request. On May 25th, the Department provided the Applicant with two options:

a) provide clarity or narrow the scope of the request with specific keywords;

b)reduce duplicate copies to reduce the total number of pages

This letter also contained a fee estimate of $2500.00 based on an estimate that there would be 10,000 pages of responsive records and extended the time for their response to July 18 pursuant to section 11 of the Act. At some point it appears that the fee assessment was either withdrawn or forgotten about. The Department provided the Applicant with 3,172

pages of responsive records on July 30th, after the Applicant had already requested a review. The IPC proceeded with the review in relation to the delay issue only.

The IPC found that, had the extension of time been properly handled, the extension to July 30th would not have been unreasonable. The Department, however, had not followed the appropriate steps set out in section 11 of the Act. She further found that the Department had failed to meet its "duty to assist" as set out in section 7 of the Act and, in fact, that the Department's attempts to have the Applicant narrow the scope of the request "teetered on the verge of inappropriate". She further confirmed that the Act does not allow a public body to put a request "on hold" while they clarify a request. As well, the fee estimate, though eventually abandoned, was grossly overestimated to the point that it was a fairly transparent attempt to force the Applicant to withdraw or narrow his request for information.

The IPC recommended that the Department ensure that its ATIPP Co-Ordinator has the necessary resources and training to respond fully and appropriately to access to information requests, and, when needed, that additional help be available within the department to help respond to large or frequent requests for information.

> I point out that the Act provides a right of access to government records. This is a quasi-constitutional right, subject only to the narrow and specific exceptions set out in the Act. The fact that an Applicant requests a very large number of records does not change his or her right to receive those records in a timely fashion.
>
> Review Report 19-150

Review Report 19-151

Category of Review:
Access to Information - Deemed Refusal

Public Body Involved: Department of Finance

Sections Applied: Section 7, Section 8, Section 11, Section 25

Outcome: Some recommendations accepted

The Applicant had made a Request for Information to the Department of Finance for his own personal information in July, 2015. Despite frequent follow-ups by the Applicant asking for updates and status reports, no response had been received by the time he finally asked for a review by the Office of the Information and Privacy Commissioner in April, 2018, almost 3 years after the request had been made.

The OIPC initiated an official review but despite repeated requests to produce responsive documents and clarify the circumstances under review, few details were clarified by the Department and there was never any explanation provided as to how the records could have gone missing or what efforts had been made to find them.

The missing records were eventually located in one of Nunavut's smaller communities and were sent to the Applicant in October 2018, but the response was not complete. The IPC found that the Department had failed to comply with multiple sections of the Act, including non-adherence to legislated time frames and failure to respond in a timely, open and accurate manner. In addition to the Department's failure

to comply with the Request for Information other issues were identified in relation to the Applicant's privacy.

The IPC recommended that the Department take a number of steps to mitigate the damages caused to the Applicant as a result of the failure to respond to the Access to Information request in a timely manner. She also recommended that the Department take a number of specified steps to determine how the information in question became lost, to review both its record management policies and to ensure its ATIPP staff has the resources needed to fulfill their roles in a timely manner.

Review Report 19 -152

Category of Review: Access to Information

Public Body Involved:
Department of Family Services

Sections Applied: Section 1, Section 13, Section 14(1)(a), Section 14(1)(b), Section 15, Section 23(1)

Outcome: Recommendations accepted

The Applicant made a request for his own personal information from the Department of Family Services. The Department identified and produced approximately 1780 pages of responsive records, but withheld some information from many of them. The IPC reviewed the law concerning each of the exceptions applied and recommended the disclosure of additional information.

> ... in the submissions made by the public body in this case, one of the reasons given for the Department's refusal to disclose this paragraph is that its disclosure "could affect the integrity of the Department of Family Services". This statement is concerning because one of the purposes contained in Section 1 of the Act is to make public bodies more accountable. The fact that a disclosure might "affect the integrity" of a pubic body should, therefore, weigh in favour of disclosure and not the opposite. Information should never be withheld simply because it makes a public body feel uncomfortable.
>
> Review Report 19-152

Review Report 19-153

Category of Review:
Breach of Privacy Complaint

Public Body Involved: Department of Justice

Sections Applied: Section 23, Section 42, Section 43, Section 48, Section 49.1

Outcome:
Recommendations partially accepted

The Applicant asked the Office of the Information and Privacy Commissioner to consider whether there was a breach of privacy as a result of the way his government issued email account had been handled after the end of his employment and, in particular was concerned about the confidentiality of communications from third parties. The Information and

Privacy Commissioner considered a number of issues, including

- what, if any, expectation of privacy employees have in relation to the records in their email accounts,
- what, if any, expectation of privacy/ confidentiality the public has in dealing with GN employees,
- the GN's obligation to protect information and prevent unauthorized access and use; and
- whether the nature of the responsibilities of the Complainant's position affected the way in which the email account should have been managed.

She found that there is a limited expectation of privacy for employees in the content of their government issued email accounts but that the public body was also required to ensure that when an employee departed, critical work was attended to. She found that the Department failed to fully follow their own processes and protocols and made recommendations to better manage email accounts upon an employee's departure. She further recommended that the Department consider amendments to the legislation governing the Complainant's position to clarify privacy and confidentiality issues.

Review Report 19-154

Category of Review:
Third Party Privacy Breach Complaint

Public Body Involved: Department of Justice

Sections Applied: Section 1, Section 3, Section 42, Section 43, Section 48, Section 49.8, Section 59

Outcome: Recommendations not accepted

The Complainant had previously done work for the Department of Justice on a contract basis in the area of Securities Regulation. In that capacity, he was given access to the database of a national organization of security regulators. At the end of his employment, the Department of Justice failed to rescind his access to the database. While they had revoked his access to the files the Complainant had been working on, they did not realize that they also had to request deletion of the Complainant's account. As a result, the Complainant continued to have access to the database and simply by updating his password was able to gain access to significant amounts of personal information about thousands of individuals listed in the database. He chose to actively change his password and then trolled the database downloading hundreds of pages of records for his own purposes, thereby breaching the privacy of those listed in the database. He then asked this office to investigate and review the Department's failure to cancel his account.

The IPC found that the Department of Justice had facilitated the Complainant's unauthorized access to the database almost two years after he was no longer contracted to them as their agent. She also found, however, that the Applicant had purposely accessed the records while fully aware that he was not authorized to do so. She recommended that the Complainant be reported to the disciplinary division of his professional governing body and that the Department of Justice take the necessary steps to have the Complainant prosecuted pursuant to section 59(1) of the *Access to Information and Protection of Privacy Act.*

Review Report 19-155

Category of Review: Breach Notification

Public Body Involved:
Department of Family Services

Sections Applied:
Section 42, Section 49.8, Section 49.9

Outcome: Recommendations acknowledged but not accepted

The Department of Family Services reported that they had lost certain child welfare records of one of their former clients when only two of three boxes of records sent from one community to another were received. Despite considerable efforts to find the third box, it could not be found and the matter was reported as a breach pursuant to section 49.9. As a result of the review process and questions asked by the IPC, it was eventually determined that there had never been a third box and that there was, therefore, no actual breach of privacy.

The IPC provided comments with respect to policies and processes and recommended that the Department take immediate steps to create and implement a formal policy or procedure to be followed by all staff when transporting paper records from one place to another. She further recommended the creation and implementation of a privacy breach protocol so that it is clear what steps need to be taken in the event of a breach and that the protocol include notification to the Information and Privacy Commissioner whenever child protection records about an individual are involved.

> By any measure, any record originating with child protective services about a client or former client of the Department is not only a material breach of privacy, but a serious one. It matters not whether the information is about one individual or twenty. These records are easily as sensitive as health records.
>
> Review Report 19-155

Review Report 19-156

Category of Review:
Access to Information - Duty to Assist

Public Body Involved:
Legal Services Board of Nunavut

Sections Applied: Section 1, Section 7, Section 69

Outcome: Recommendations accepted

The Applicant contacted the public body requesting some basic information about how to make an access to information request, including to whom the request should be directed. Despite making a number of inquiries, no response was received and, as a result the Applicant submitted his request to the Manager of ATIPP in the Department of Executive and Intergovernmental Affairs, who forwarded the request to the Legal Services Board (LSB) immediately by email, and put the $25.00 fee received from the Applicant into the mail for delivery to the LSB. The request was for information about severance packages paid by the LSB over a period of years, including the number of such packages, the total value of the packages, the break-down of gender for those who

received the severance packages and how many non-disclosure agreements had been signed.

Two months later, the LSB responded to the Applicant saying that the LSB did not keep those kinds of statistics and did not, therefore, have a record containing that information. They declined to provide any responsive records.

The IPC found that the LSB failed to comply with its duty to assist the Applicant in a number of respects, including their failure to respond to the Applicant's preliminary questions, their failure to respond within 30 days and their failure to provide records responsive to the request for information. Further, she found that while the requested information may not be contained in a single record, the LSB should be able to easily identify and compile the information requested into a single document, with very little research or effort - in fact far less effort than would be required to review the records for disclosure. The spirit and intention of the Act, along with the duty to assist set out in section 7 required the public body to at least communicate with the Applicant to advise that there was no one record containing that information but that the information could be compiled. If the Applicant was not satisfied with a compiled record, the public body was required under the Act to provide the Applicant with the records from which he could compile the statistics himself.

> To the extent that a public body feels that a request is unclear, they are obligated to consult with the Applicant to fine tune the request.
>
> Review Report 19-156

The IPC recommended that the Regulations be amended to reflect that the "head" of the LSB is the CEO of that organization and that the LSB appoint an ATIPP Coordinator at a senior level in the organization with delegated authority from the CEO to receive and address access to information requests and privacy complaints, with final decisions remaining with the CEO. She further recommended that the LSB provide necessary ATIPP training and create a set of policies and procedures to deal with access requests. She recommended that the Applicant be provided with a compiled response to his request for information with the Applicant's consent or, if the Applicant would not consent to receiving a compiled document, that the LSB identify and disclose all source records from which the Applicant could compile the information he desired.

Review Report 19-157

Category of Review: Privacy Breach Review - Commissioner's own motion

Public Body Involved: Legal Services Board

Sections Applied: Section 2, Section 3, Section 42, Section 42.1

Outcome: Recommendations largely accepted

While undertaking another review, it came to the attention of the IPC that senior employees of the LSB were using gmail and other non-government email accounts to conduct their work for the LSB. She exercised her powers pursuant to section 49.2 of the Act to a conduct a review as to whether the use of gmail for government purposes was compliant with ATIPPA.

The IPC found that Section 42 of the Act requires the public body to protect personal information by making reasonable security arrangements against such risks as

unauthorized access, collection, use, disclosure or disposal and section 42.1 requires public bodies to conduct privacy impact assessments before implementing any system that might impact on the privacy of Nunavummiut. She found that the use of a gmail account and/or a personally owned computer by the Executive Director/Chief Executive Officer to conduct the business of the LSB does not accord with the public body's obligations to protect the personal information of individuals or the business and that, while gmail may well have sufficient protection measures in place, it was impossible to know this without having conducted a privacy impact assessment (PIA).

She recommended the immediate discontinuance of the use of gmail and that the LSB require all employees to take steps to ensure that all existing email and other business records in relation any work of the LSB be transferred to servers administered either by the GN or to an appropriate and dedicated LSB server to ensure that business records are documented and stored in a way that facilitates retrieval for future operational and legal requirements. She recommended, as well that the LSB create an appropriate file management system applicable to all employees, contractors and board members so as to ensure records are appropriately saved and retained in a format that can be easily retrieved for future use. She recommended that the LSB develop and implement a comprehensive set of privacy policies and that the GNWT ensure adequate resources were available to the LSB to meet their obligations under the ATIPP Act.

Review Report 19-158

Category of Review: Breach Notification

Public Body Involved: Department of Health

Sections Applied: Section 49.7, Section 49.8, Section 49.9, Section 49.10, Section 49.12

Outcome: Recommendations accepted

The Department of Health reported that an envelope containing mental health information about four identifiable patients had been delivered to the wrong person. The envelope was intended to be delivered to a health care provider but instead was delivered to someone working in another government agency with a similar name.

The intended recipient's name was written as the first initial of their first name and their last name. The internal "station" number was written on the envelope, but not the department of the intended recipient.

The IPC found that the delivery of this envelope to the wrong department constituted an unauthorized disclosure of personal information and that the breach represented a significant risk of harm to the individuals involved.

A number of recommendations were made, including:

- that the Department of Health update its Health Directive - Sending and Receiving Confidential Email and Mail to include guidance on how to use internal mail when dealing with personal health information.
- that the Department of Health ensure that every employee of the Department whose job description includes the handling of personal health information be provided with privacy training

- that the Department create and implement a breach management policy
- that the Department take immediate steps to introduce health specific privacy legislation to the Legislative Assembly for consideration

Review Report 19-159

Category of Review: Access to Information

Public Body Involved: Legal Services Board

Sections Applied: Section 5, Section 7, Section 14(1)(f)

Outcome: Recommendations accepted

The Applicant made a request for information in relation to the salaries of senior employees of the LSB and requested information in relation to how much time the CEO actually spent in Nunavut. The LSB identified some responsive records but refused to disclose any of them or any part of them, citing section 14(1)(f) and section 7.

The issues in this case were similar to those in Review Report 19-156. The IPC found that the LSB had failed to comply with its duty to assist as set out in section 7 of the Act. Further, she found that in refusing to disclose any portion of the responsive records, the LSB did not comply with section 5 which requires the disclosure of partial records when protected information can be redacted so as to protect that information. The IPC recommended that LSB review its records to identify all records which would contain the information responsive to the Applicant's question in relation to the dates the Executive Director was in Nunavut and disclose those records to the Applicant, subject only to applicable redactions. Alternatively, but only with the Applicant's agreement, it was recommended that the LSB provide the Applicant with a compiled response answering his specific question. She further recommended that the LSB review the agenda and minutes at issue and actively exercise their discretion on a line by line basis.

> Here, where there was no one record that was responsive to the request, LSB was still required to have either provided all the responsive records so the Applicant could have deduced the answer to his question himself, or worked with him to propose that they simply provide an answer to his question based on the information available in their records.
>
> Review Report 19-159

Review Report 19-160

Category of Review: Privacy Complaint

Public Body Involved: Nunavut Housing Corporation/ Local Housing Organization

Sections Applied: Section 1, Section 43, Section 47, Section 48, Section 49.8

Outcome: Agreed with findings. Recommendations noted.

An Applicant asked the Information and Privacy Commissioner to determine if it was appropriate for a Local Housing Organization (LHO) to disclose to the community Alcohol Education Committee that a tenant was in arrears so as to prevent that tenant from ordering alcohol. The Applicant and several others in the community living in public housing units received letters in which they were advised that those tenants in arrears would be reported to the local alcohol education committee because one of the conditions that had to be met in order for someone to purchase alcohol was that the person ordering liquor could afford to do so without creating any hardships for the family.

The intention was to get the tenants to pay their arrears so they wouldn't be reported to the Alcohol Education Committee.

The IPC immediately contacted the LHO and asked them to hold off on disclosing those names until this office could review the intended disclosure to determine whether it was in compliance with the Access to Information and Protection of Privacy Act. The LHO immediately withdrew the letters and no information was disclosed. The IPC, however, proceeded with the review to provide guidance for the future. She found that the proposed disclosure of personal information would most definitely have been an unauthorized disclosure under ATIPP. She recommended that the individual responsible for the notice referred to in the report immediately be given in-depth training on the obligations of public bodies to protect personal information in its custody and control and on when the use or disclosure of that information is (and is not) authorized under the legislation and that all managers with all Local Housing Organizations be required to complete similar training within one year with follow up training required on an annual basis.

> In my opinion, the threat contained in the notice given to tenants was an abuse of authority and completely unethical in that it represented either an intention to knowingly disclose personal information contrary to the ATIPP Act, or was an act of coercion made by the LHO employee knowing that he could not or would not follow through with it.
>
> Review Report 19-160

Review Report 19-161

Category of Review: Breach Notification

Public Body Involved: Department of Health

Sections Applied: Section 49.7, Section 49.8, Section 49.9, Section 49.12,

Outcome: Recommendations accepted

The Department of Health reported that dental records containing the personal health information of a number of children was missing. The records had been sent from a community health centre to the Manager of the Oral Health Project in Iqaluit via courier. The package was signed for at the office in Iqaluit but could not be found thereafter, despite thorough searches, including going back to the courier company to conduct additional searches.

The Information and Privacy Commissioner found that the loss of the records constituted a material breach of privacy under the Access to Information and Protection of Privacy Act. She made recommendations with a view to preventing similar breaches in the future, including:

a) that the Sending and Receiving Confidential Email and Mail Policy be reviewed and updated to reflect guidance on when documents can be sent by email and that the policy should reflect that original documents should not be sent without a backup copy held somewhere, to be held at least until there is confirmation that the originals have been received at their intended destination;

b) that the Department develop and implement a comprehensive privacy training policy to be provided on hire and again at least every two years.

c) that if not already in place, the Department develop a clear procedure to be followed for all received mail so that it is tracked within the public body until such time as it reaches its final destination

Review Report 19-162

Category of Review: Access to Information

Public Body Involved: Department of Justice

Sections Applied: Section 14(1)(a), Section 15(a), Section 15(c),

Outcome: Recommendations accepted

The Applicant made a request for his own personal information in relation to a report prepared by an employee of the Department which resulted in the Applicant being denied certain privileges. Ninety eight pages of responsive records were identified but some information was redacted pursuant to sections 14(1)(a) (advice and recommendations), 15(a) (solicitor/client privilege) and 15(c) (correspondence involving legal matters). The Applicant requested a review of the items redacted and also of the Department's delay in responding to his request.

The IPC found that the Department was four days late in providing the Applicant with his response but that the delay in this case was not such that it would, by itself, have merited a full review. The IPC reviewed all of the responsive records and recommended the disclosure of additional information under both section 14 and section 15. She also recommended that the Department completely and fully exercise their discretion with respect to those items that did meet the criteria for these exceptions and that they provide the Applicant will a full explanation as to their reasons for applying discretion to withhold the information.

Review Report 20-163

Category of Review: Privacy Breach complaint

Public Body Involved:
Department of Education

Sections Applied: Section 48(l)

Outcome:
Recommendation to develop policies not accepted

The Complainant raised three privacy complaints against his employer. The first arose when information from his personnel file was reflected in a letter written by counsel for the Department to the Complainant's own counsel in relation to a workplace harassment allegation. The second was when the Complainant's supervisor insisted on having another supervisor present during the Complainant's performance evaluation meeting, even after the Complainant objected. The third arose when the Complainant's supervisor used video surveillance footage to call out the Complainant for his failure to lock the door of the work building when leaving the premises on a weekend.

The IPC found that Section 48(l) allows for the disclosure of personal information for use in the provision of legal services to the GN or one of its agencies and that, as the Complainant had hired a lawyer to make demands of the Department, the Department was authorized pursuant to section 48(l) to disclose relevant portions of the Complainant's personnel file to their own legal counsel. She further found that the supervisor's use of video surveillance footage to identify the employee who had failed to follow clear safety and security measures was not an unreasonable invasion of the Complainant's privacy because the Complainant was aware of the cameras and the purpose of the cameras (safety and security) and the use of the footage was within the purposes.

The IPC did find, however, that the insistence of the Complainant's supervisor on including another employee in the Complainant's performance evaluation meeting notwithstanding the Complainant's objections did constitute an unreasonable invasion of the Complainant's privacy.

The IPC recommended that those responsible for personnel management in all communities be provided with training in relation to their obligations to maintain client and employee privacy. She further recommended the development of policies around the performance evaluation process so as to ensure respect for employee privacy.

Review Report 20-164

Category of Review: Breach Notification

Public Body Involved: Department of Justice/ Legal Services Board of Nunavut

Sections Applied: Section 42, Section 42.1, Section 49.8, Section 49.9, Section 49.10

Outcomes:
LSBN:

- **Recommendation to give all current clients notice not accepted**
- **Recommendation to give public notice accepted**
- **Remaining Recommendations accepted**

Dept of Justice

- **Declined to respond to recommendations**

In the course of having providing IT assistance to the LSB, a contracted IT technician identified an active attempt by an unknown party to gain unauthorized access to the server several years earlier as well as several critical security

vulnerabilities which had left the system open to attack. These vulnerabilities had existed since at least 2011 and survived the transfer of data from an old server to a new one because the new server mirrored the same configuration as the old server that had been compromised. While it was impossible to determine whether the system had, in fact, been compromised the vulnerabilities were so extensive and had been there for so long that the IPC determined that the information on the servers was so insecure as to qualify as a breach of privacy as defined under section 49.8. The system appears to have been used for administration of the office and processing applications from the public for legal assistance and it therefore included significant amounts of personal information about both clients and staff.

The IPC found that the LSB was not in compliance with the *Access to Information and Protection of Privacy Act* in that they had not taken reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal of personal information as required by section 42 of the Act. She further found that the LSB was required, pursuant to section 49.10 to notify the public about the breach.

She recommended, among other things that:

a) the NLSB identify individuals potentially impacted by the breach and directly contact those who were, at the time of the discovery, active clients whose contact information was verifiable to notify them of the breach

b) the NLSB take additional steps to notify the general public about the breach by providing notice in all official languages in public spaces in each community affected, as well as by public service announcements on local radio and on the NLSB web site.

c) a Privacy Impact Assessment and a Threat Risk Assessment be conducted on the records management systems currently used by the NLSB and that appropriate safeguards be implemented to protect and secure personal information in the system

d) one person within the NLSB be designated as the privacy officer for the organization, responsible oversee access to information and protection of privacy, including ensuring that the NLSB meets its legislated requirements under the ATIPP Act

e) the NLSB create a privacy and security framework that reflects the 10 internationally recognized principles of privacy and security best practices and includes necessary completion of PIAs, staff training, roles-based access and auditing to ensure compliance.

> It appears that limited technical resources over an extended period of time contributed to the historical loss of records (prior to breach notification provisions coming into effect) and has contributed to the environment that allowed the vulnerabilities more recently identified by the IT consultant to exist undetected for so long.
>
> Review Report 20-164

Review Report 20-165

Category of Review: Privacy Breach Complaint

Public Body Involved: Department of Finance

Sections Applied: Section 43, Section 48(q), (s), Section 49.8, Section 49.9

Outcomes:

- **Finding of "material breach" not accepted**
- **Recommendation to provide additional training to supervisor not accepted because supervisor no longer in the position**
- **Recommendation to delete email not accepted**
- **Recommendation to focus privacy breach investigations on compliance with ATIPP rather than labour relations matters not accepted**

The complainant had a medical episode while at work and took himself to the health centre for treatment. The Complainant's supervisor not only followed him to the health centre and attended the Complainant's bedside without being invited to do so, he then disclosed personal information from the Complainant's personnel records to the health centre staff. The supervisor had to be asked to leave the health centre several times before complying. He followed up by sending an email from his GN email account to the Complainant's health care provider which contained additional personal information about the Complainant.

The IPC found that the actions of the supervisor amounted to a material breach of privacy as defined in section 49.8 of the ATIPP Act. She found that the supervisor used information about the Complainant's claim for medical leave to insinuate himself into the Complainant's medical care by attending at the hospital with the Complainant uninvited and by taking steps to communicate with the hospital about the Complainant without a request that he do so, and clearly without the Complainant's consent. Further, section 48(q) which allows a public body to disclose information necessary to protect the mental or physical health or safety of an individual did not apply here as the Complainant had seen himself to the health centre and did not pose a risk to himself or others. She further found that section 48(s)(ii) did not apply (disclosure allowed when the disclosure would clearly benefit the individual the information is about). She found that there was nothing in the disclosure to suggest that it benefited the Complainant and, in fact, had the opposite effect of upsetting him. Because of the sensitivity of the information disclosed, the breach was a material one under the Act.

The IPC recommended that the supervisor be required to undertake management training with a particular focus on the public body's responsibility to protect the privacy of its employees.

> This was health information and more specifically, mental health information. There remains stigma about mental health in our society. It is extremely sensitive personal information. Not only was this information used, but the Director took further active steps to disclose the information to the Complainant's health care providers in person and via email, despite the protests of the Complainant and the health care provider.
>
> Review Report 20-165

Review Report 20-166

Category of Review: Breach Notification

Public Body Involved: Department of Health

Sections Applied: Section 3(1), Section 42, Section 44, Section 48, Section 49.9, Section 49.7,

Outcome: Recommendations largely accepted

This matter was reported to the Department of Health by a member of the public in one of the smaller communities. He had picked up a prescription at the local health centre which had been delivered there by the privately owned pharmacy in Iqaluit. The bag in which the prescription arrived had the correct information on the label on the bag, but inside the bag was the individual's prescription along with another prescription for a completely unrelated third party in another community altogether.

Because the pharmacy, who made the error, is not a public body subject to the privacy provisions of the Access to Information and Protection of Privacy Act, the IPC found she had no jurisdiction to deal directly with the obvious breach of privacy (or the obvious and significant concerns for patient safety resulting from the error), she did provide comment on the role of the health centre in the community as the conduit for delivering prescriptions.

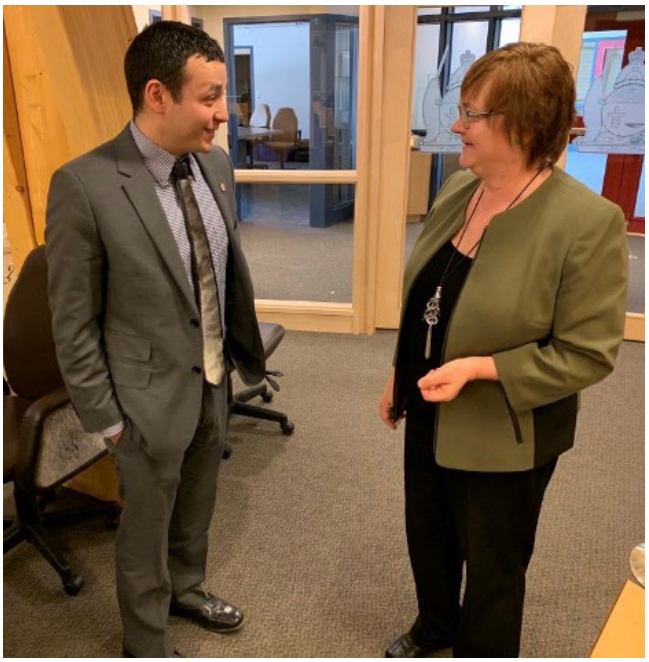
The IPC recommended, among other things

a) that the Department of Health take steps to review current processes and procedures in relation to their role in delivering prescriptions to residents;

b) that the Department, along with its retail pharmacy stakeholders, actively consider the issues raised as a result of this review and identify a lawful means for staff at the health centre to verify the contents of the pharmacies packages, which may require the express consent of the patient;

c) that the Department, along with its retail pharmacy stakeholders take steps via public communication in all official languages to encourage the public to report errors with respect to prescriptions received when discovered;

d) that, in the absence of private sector or health specific privacy legislation in Nunavut the Department include as part of the requirements of obtaining or renewing a pharmacist's license that the pharmacist comply with industry standards for privacy, incorporating the ten privacy principals, and that these be adequately incorporated into pharmacy operations and that there be a requirement for pharmacies to disclose to the Department any privacy breaches discovered.



Meeting with MLA Adam Lightstone at the Nunavut Legislature.

TRENDS AND ISSUES – MOVING FORWARD

LEGISLATIVE REVIEW

Nunavut has been, in some respects, well ahead of the rest of the country in amending its access and privacy legislation. It was the first, and is still one of the only, jurisdictions in the country which requires breach notification for all public bodies. However, there has never been a full and comprehensive review of the legislation. This is a standard requirement in most jurisdictions at regular intervals. As I have in past years, I strongly advocate for a formal and comprehensive review of the legislation, with public consultation and input from stakeholders.

RECORDS MANAGEMENT

When things go terribly wrong, like they did with the ransomware attack experienced by the Government of Nunavut in early November, we need to learn from those events. My Review Report on this attack has yet to be produced, largely because I have been unable to get any clear answers to many of the questions I have posed. While everything properly saved on the servers was properly backed up and recoverable, anything saved on a local computer has been irretrievably lost. What has been done to create an inventory of that information? This should have been done immediately, while memories were fresh. To ask employees, at this point, to go back to the end of their day on October 31st, 2019 and ask them to provide a list of even the kinds of information saved on their local devices, the results will not be nearly as complete as if this had been done in early November. Furthermore, since the attack, many employees have left their employment with the GN and it will, therefore, be impossible to create that inventory for all employees as of November 1st of last year. Transitory or not, records that existed on local devices at the time of the attack were still records subject to the Access to Information and Protection of Privacy Act. While we can't retrieve those records now, we can focus on better records management policies and better enforcement of those policies. With the transition to electronic records, more and more we are relying on individual employees to properly manage their own records, with no real training or guidance. If there are 300 employees in a public body, there are probably 300 records management styles. Records management needs more attention, with appropriate ORCS and ARCS, enforcement of records management policies, clear retention and destruction schedules and a focus on day to day file management. I would encourage the GN to invest more resources and manpower into its records management systems.

HEALTH SPECIFIC ACCESS AND PRIVACY LEGISLATION

I feel a bit like a broken record on this issue. Nunavut is the only jurisdiction in Canada that relies on its general access and privacy legislation to try to regulate these issues in the health sector. The requirement for the movement of information to provide comprehensive health care does not marry well with the rather stark terms of the *Access to Information and Protection of Privacy Act* , which has a far more lineal focus. While I am aware that work is being done on this, there has, to my knowledge, been no public consultation to date or any visible indication that this legislation is anywhere close to being presented to the Legislative Assembly for consideration. Judging from the number of privacy breach notifications

and privacy breach complaints being received from or involving the Department of Health, it is legislation that is greatly needed to help guide the appropriate collection, use and disclosure of personal health information.

MUNICIPALITIES

For many years, a staple and repeated recommendation contained in my Annual Report was that municipalities be brought under the legislation or that legislation be developed to address access and privacy matters at the municipal level. I backed off this recommendation in 2017 when amendments to the ATIPP Act set the groundwork for municipalities to become subject to the Act. These provisions have yet to be brought into force. I appreciated and understood at the time that it was going to take a large investment and a good deal of time to properly set municipalities up to be able to comply with the legislation – beginning with appropriate records management systems, the development of good records management protocols, policies and procedures, the clean-up and appropriate clear-out of historical records, and significant training of local municipal staff with respect to the obligations imposed by the Act. Unfortunately, it appears that little has been done in recent months to bring implementation any closer. Some initial steps were taken in the first year or eighteen months after the amendments were passed and I am aware that the ATIPP Manager had taken a leadership role in moving implementation ahead. This momentum, however, appears to have come to a halt when there was a change of personnel in this position. I therefore resurrect my long standing recommendation that this be made a priority for the GN and that the steps necessary to move municipalities closer to being ready and able to comply with their obligations under the coming legislation be renewed and accelerated.

TRAINING FOR ATIPP STAFF

If one were to read all of the Review Reports issued over the past year, one of the most commonly recurring themes in terms of recommendations is that public bodies provide their ATIPP Coordinators with more and better training with respect to their roles as the gatekeepers within the departments on these issues. The position of ATIPP Coordinator is an important one and requires the ability and the authority to make decisions with respect to what is, and what is not, appropriate to disclose in the context of an access to information request, and who understands and has the ability to address privacy concerns raised. These positions are not entry level positions. They require expertise and training, a strong familiarity with records management and an understanding of the way in which the GN operates. The GN has lost a number of its most experienced ATIPP Coordinators over the last several years and this is becoming obvious in the quality of responses to both Applicants and to this office. The importance of the role and the expertise required in an ATIPP officer needs to be recognized in the form of appropriate ratings for position evaluation and remuneration commensurate with the importance and expertise required. More ATIPP Coordinators should be encouraged and supported to take on-line training such as that offered by the University of Alberta's Faculty of Extension. ATIPP Coordinators should be encouraged to meet on a regular basis to discuss issues that have presented themselves and solutions applied. In short, more must be done to invest in, support and train these important employees.

FINAL WORD

As I leave the position of Information and Privacy Commissioner for Nunavut, I feel a sense of accomplishment and satisfaction. I am proud of the work that has been done by my office over the last twenty years to improve access and privacy for the people of Nunavut. The job has had its challenges and frustrations, but those have been far fewer than the successes and the changes for the better. I have learned much about this wonderful territory and its people – so strong and resilient and willing to work collaboratively for the betterment of the common good. I hope I have contributed just a little bit to the growth of Nunavut and that I have left this office strong and ready for the next Information and Privacy Commissioner to be able to continue this important work.

Thank you for having given me this opportunity to participate in history in a real and meaningful way.

PRIVACY IS ESSENTIAL

Grounded in a man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy or constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.

Justice G. LaForest
R v. Dyment [1988] 2 SCR 417, SCC

OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER
OF NUNAVUT

Website: atipp-nu.ca
Email: admin@atipp-nu.ca
Phone: 1-867-446-8631 | Toll Free: 1-888-521-7088

NU