



ANNUAL REPORT 2017/2018

Information and Privacy
Commissioner
Of the Northwest Territories





**OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER**
NORTHWEST TERRITORIES

P.O. Box 382
Yellowknife, NT
X1A 2N3

August 11, 2018

The Hon. Jackson Lafferty
Speaker of the Legislative Assembly
P.O. Box 1320
Yellowknife, NT
X1A 2L9

Dear Mr. Speaker

I have the honour to submit my annual report to the Legislative Assembly of the Northwest Territories for the period from April 1st, 2017 to March 31st, 2018.

Yours very truly

Elaine Keenan Bengts
Information and Privacy Commissioner
Northwest Territories

/kb

CONTENTS

COMMISSIONER'S MESSAGE	7
THE LEGISLATION IN BRIEF	14
<i>The Access to Information and Protection of Privacy Act</i>	14
Access to Information	14
Protection of Privacy	15
<i>The Health Information Act</i>	17
THE YEAR IN REVIEW	19
<i>Access to Information and Protection of Privacy Act</i>	19
<i>Health Information Act</i>	20
REVIEW REPORTS	22
Review Report 17-160	22
Review Report 17-161	23
Review Report 17-162	24
Review Report 17-163	25
Review Report 17-164	26
Review Report 17-165	27
Review Report 17-166	29
Review Report 17-167	31
Review Report 17-168	32
Review Report 17-169	33
Review Report 17-170	34
Review Report 17-171	35
Review Report 17-172	36
Review Report 18-173	37

Review Report 18-174	38
Review Report 18-175	39
Review Report 18-176	40
Review Report 18-177	41
TRENDS AND ISSUES - MOVING FORWARD.....	43
Comprehensive Review	43
Review of Policies.....	44
The Use of Fax Technology in the Health Sector	44
Education.....	45







COMMISSIONER'S MESSAGE



Last year in my Annual Report, I noted that strong access and privacy legislation is increasingly vital to the maintenance of our democratic ideals as the world changes in ways no one would have imagined in 1997 when the *Access to Information and Protection of Privacy Act* came into effect. Today, we live in the era of “fake news” and “the truth is not the truth” generated by powerful politicians, which makes strong public sector access and privacy legislation that much more important. It is vital to the health of our democracy and democratic ideals that we continue to encourage open and accountable government in our own backyard

and I maintain that one of the most powerful and important tools for doing that is strong access and privacy legislation. It has been more than two years since the Department of Justice undertook a public consultation on a review of the Act. Since then, I have heard very little about whether or not any next steps have been taken. Last spring, I was given an update on some of the likely directions that the department would be taking in its legislative proposal but I have heard virtually nothing since that time. While I understand that the wheels of government grind slowly and that the Department of Justice has been pre-occupied with developing legislation to deal with the upcoming legalization of cannabis, it is disheartening that it is taking so long to address this important piece of legislation. The Northwest Territories is now the last Canadian jurisdiction, but for Nunavut, to modernize its first-generation access and privacy legislation. I am hopeful that the next year will show more progress.

But modern legislation is not all we need. We need a real commitment to the spirit and intention of the Act and this year, more than any other year, I have seen a marked decrease in the willingness of public bodies to uphold those ideals. Many times this year public bodies have refused to follow



recommendations made, rejecting my analysis and application of the law. As my office has only recommendation making power, and the only recourse for an Applicant is an expensive, time-consuming and confusing appeal to the Courts, public bodies can easily avoid accountability when they refuse to follow recommendations made. I do understand that it is sometime uncomfortable for public bodies to disclose some records and that they would rather not do so, but it is for this very reason that the recommendations of the Information and Privacy Commissioner must have more impact. I am now convinced that this will require a change in the model used. Newfoundland and Labrador passed legislation in 2015 which has been touted as one of the best access and privacy laws in Canada and even the world. Under that legislation the Information and Privacy Commissioner continues to have only the ability to make recommendations. If a public body wishes to disregard those recommendations, however, it must ask the court for an order to allow it to do so. This change puts the onus on the public body, where it should be, to obtain court approval of its decision, rather than leaving it to an individual applicant to challenge that decision. I have encouraged the Department of Justice to use this model and I am hopeful that when new legislation is eventually tabled, it will incorporate this approach.

I was also concerned once again this year as we watched the City of Yellowknife stumble and trip awkwardly in dealing with a series of privacy breaches, beginning with the apparent theft of email correspondence containing all description of information, including sensitive personnel information, which email correspondence was then provided to and published by the local press. This was followed by the revelation of allegations that a senior City employee had been using City cameras to inappropriately surveil women in City facilities. At the time, I wrote to the City offering my assistance to begin a discussion about privacy issues and the creation of a strong privacy policy within City Hall, but I received no answer to my letter. This is not the first time I have offered to work with the City on privacy concerns. The non-response has, however, been consistent. The City does not seem to be interested in formalizing their access and privacy policies. It should be noted that the first time that I recommended that municipalities be included as public bodies under the *Access to Information and Protection of Privacy Act* was in my first Annual Report in 1998 – twenty years ago. The



recommendation has been repeated nearly every year since then but there has been no effort to make the necessary changes. With Nunavut recently having amended their Act to accommodate the inclusion of municipalities under ATIPP legislation, the Northwest Territories is now the only remaining Canadian jurisdiction in which municipal governments will not be required to meet minimum access to information and protection of privacy standards. The recent events at the City of Yellowknife and their failure to address the privacy implications of these events points to the clear need for legislation. Once again, I encourage the Department of Justice, when drafting its new legislation, to ensure that municipalities become subject to the same rules as other municipalities throughout the country.

This year has seen a continuing maturing of the *Health Information Act*. The Minister issued a series of policies and procedures as required by section 8 of the Act and we have seen more reporting of privacy breaches. These breach reports also indicate that those tasked with dealing with such breaches are becoming more adept at identifying the issues and addressing them. I am, however, still concerned about the fact that there have been so many breach reports involving a misdirected fax or unencrypted email. I have encouraged health professionals to abandon the older fax technology, which is less secure, requires more effort and more time than encrypted email in favour of newer, more secure means of communication. I simply cannot understand the apparent reluctance of the health sector to adopt the better technology when there is a simple and readily available solution to the problem that would involve little or no cost or training.

At the annual gathering of Canada's Information and Privacy Commissioners, which took place this year in Iqaluit, we heard from members of the Kwanlin Dün First Nation in the Yukon who are in the process of implementing their own access and privacy legislation. They told the story of how they started with a warehouse full of old, unmarked boxes, many of which had served as nests and/or food for rodents over the years and began to organize and collate that information into a well-organized, searchable system. They are now actively working on a law to ensure access to that



information by its members. It was and is an eye-opening tale of hard work and commitment to the task.



Canada's Information and Privacy Commissioners

At the same meeting we also heard from Professors Valerie Steeves and Jane Bailey from the University of Ottawa who talked to us about their e-Quality Project, a partnership of scholars, research and policy institutes, policymakers, educators, community organizations and youth. The project focuses on corporate policies in the digital economy, especially insofar as they concern privacy and ways to promote healthy relationships and respect for equality on-line and is aimed at young people and how they interact with the on-line world.

The economic model behind e-commerce (i.e. disclosure of information in exchange for service) creates a bias in favour of disclosure. Youth are the key to understanding the privacy implications of this bias, because, as early adopters of online media, they drop terabytes of data (often unknowingly) as they go about their daily lives. This data is processed to target them with behavioural marketing to shape their attitudes and behaviours, often outside the reach of existing regulations because privacy



policies do not provide full disclosure of the analytics used (making informed consent difficult), and profiling draws in non-personal data (which sidesteps the consent process).

Professor Steeves and Professor Bailey outlined some of their findings and shared their insight on how youth, in the day of Facebook, Snapchat and Instagram, manage their privacy. It was fascinating to hear about how young people view their privacy and alter their behaviour to protect what they consider to be their most private of information. There is, however, much work to be done to educate our young people on how best to ensure their privacy in the on-line world. To this end, I participated with my fellow Information and Privacy Commissioners from across the country in developing a number of lesson plans for teaching children about how to protect their privacy on line. These lesson plans have proven extremely popular in many jurisdictions. They are available on my website under “Resources” and I would encourage teachers in the Northwest Territories to take advantage of the good work done in this regard.

We also continued to update and improve our website at www.atipp-nt.ca. The website contains a lot of information about the work we do, including all of our Annual Reports, Review Reports and Special Reports, a copy of the Act and Regulations, links to helpful sites from other jurisdictions and organizations and much more information. We are continually updating it and adding more information. We hope that it will serve as a good resource to both public bodies and the public with respect to access and privacy matters. All indications are that the site is well used and that the Review Reports, in particular, are viewed and downloaded on a regular basis.

To end on a positive note, I am pleased to acknowledge that my budget has been increased to reflect the addition of a full time Deputy-Commissioner, to be shared with the Nunavut office. I am excited to have the extra help, particularly in light of the continuously increasing



work-load in recent years. I am currently working on filling that position and hope to have it filled within the next few months.

In closing, I would like, once again, to acknowledge and thank my assistant, Lee Phipers, for her continued support and assistance. Her passion, work ethic, and cheery disposition make my job so much easier.





THE LEGISLATION IN BRIEF

The Access to Information and Protection of Privacy Act

The *Access to Information and Protection of Privacy Act* enshrines two principles:

1. the right of the public to have access to government records; and
2. the right of the public to insist that their personal information not be collected, used, or disclosed except in accordance with specified guidelines.

It outlines the process for the public to obtain access to records and establishes when and how public bodies can collect, use or disclose personal information about individuals. It applies to 33 territorial departments, crown corporations and other public agencies.

Access to Information

Part I of the Act addresses the public's right to ask for and receive copies of public records. This right of access is so fundamental to our form of government that laws governing it in Canada have been deemed by the Supreme Court of Canada to be quasi-constitutional in nature. Such laws allow the public to participate more effectively in government and to hold government and governmental agencies to account. The right of access to government records is not, however, absolute. Sections 13 to 25 of the Act set out the specific and limited circumstances in which public bodies are either prohibited from disclosing information or have the discretion not to disclose the information requested. Public bodies are prohibited from disclosing information in three circumstances:

- a) where the information is subject to a cabinet confidence;
- b) where the disclosure would constitute an unreasonable invasion of an individual's privacy;
and
- c) where the disclosure would reveal the trade secrets of a third-party entity.



There are also a number of instances in which public bodies have the discretion to refuse access to public records, including where the records are subject to solicitor/client privilege, where the disclosure is reasonably likely to impair intergovernmental relations, and where the disclosure might interfere with a law enforcement matter.

Anyone can make a request for access to information held by a GNWT agency by submitting their request in writing to the public body from whom the information is sought. Once a request is received, the public body has 30 days to identify any responsive records, review them to assess what portion of those records might be subject to either a mandatory or a discretionary exception, and provide them to the Applicant. When an Applicant is not satisfied with the response received, he or she can ask the Information and Privacy Commissioner (IPC) to review the response given.

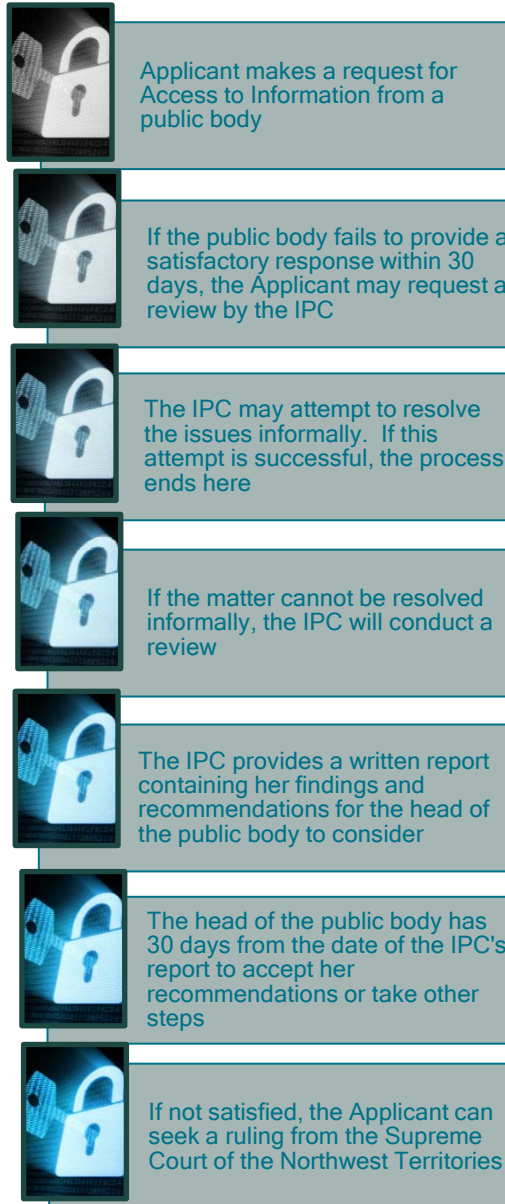
Protection of Privacy

Part II of the Act outlines the rules for when and how public bodies can collect personal information about an individual, what that information can be used for and by whom once it has been collected and in what circumstances such information can be disclosed to another public body or any other person or organization. This section requires government agencies to ensure adequate security measures to protect personal information from inappropriate use or disclosure and prohibits government employees from discussing personal information obtained during the course of their employment with any other person. This part of the Act also gives individuals the right to ask for a correction to personal information held by a public body.





The Access to Information Process





The Health Information Act

The *Health Information Act* came into effect on October 1st, 2015. Its purpose is to govern the collection, use and disclosure of personal health information while recognizing the need to use and disclose such information with as few barriers as possible to provide effective and efficient health care. The legislation applies to all records containing the personal health information of an identifiable individual. It applies to health information custodians in both the private and the public sectors.

The Act allows medical practitioners to assume, in most situations and with certain preconditions having been met, that an individual seeking health care has provided implied consent to the collection, use and necessary disclosure of their personal health information for the purposes of providing health care to the individual patient. If a patient has expressly indicated that the practitioner is not to rely on implied consent, the practitioner must obtain the patient's express consent except in very limited situations, such as emergency health care. The Act also gives the patient the right to put conditions on who has access to his or her personal health records and can direct, for example, that one or more practitioners, nurses, clerical staff or other employees in any particular office be prohibited from accessing that patient's file.

Overarching all of these provisions is the clear direction that a medical care worker's access to any personal health information is to be limited to that information which the care provider "needs to know" to do their job.

The *Health Information Act* also provides patients with the right to access any record containing his or her own personal health information held by a health information custodian. A process for requests for information similar to that in the *Access to Information and Protection of Privacy Act* is provided for, though it is a somewhat more complicated process and the time lines for responding are



potentially far longer than in the case of the ATIPP Act. A request for personal health information is also subject to the payment of fees, which contrasts with a request for personal information under the Access to Information and Protection of Privacy Act which allows only for the recovery of photocopying costs in the case of a request for personal information. There are also provisions for a patient to request that his personal health information be corrected if an error is made.

Where a person believes that a health information custodian has improperly collected, used or disclosed his or her personal health information, if they are not satisfied with the response they receive to a request for access to their personal health information, or if there is a dispute about the correction of medical health records, the *Health Information Act* allows the individual the right to request the Information and Privacy Commissioner to review the matter. With only a few minor differences, the review process is the same as under the *Access to Information and Protection of Privacy Act*. Once the review is completed, the health information custodian must decide to accept the recommendations made or take other steps within 30 days.

The rights of appeal under the *Health Information Act* are quite different than the rights of appeal under the *Access to Information and Protection of Privacy (ATIPP) Act*. For one thing, the right of appeal applies to breach of privacy issues in addition to access to information matters, and where there is a disagreement about a correction to personal information. Secondly, and perhaps more significantly, the Information and Privacy Commissioner has the right to launch an appeal of a decision of a health information custodian to the courts, a right reserved only to Applicants under the *ATIPP Act*.

Under the *Health Information Act* there is a positive duty imposed on health information custodians to give notice to any individual whose personal health information has been lost or stolen or if it is altered, destroyed or otherwise disposed of without authorization or been used or disclosed contrary to the provisions of the Act. This notice must also be given to the Information and Privacy Commissioner, who may choose to investigate the breach.



THE YEAR IN REVIEW

Access to Information and Protection of Privacy Act

The Office of the Information and Privacy Commissioner opened 53 files under the *Access to Information and Protection of Privacy Act* during 2017/2018, down slightly from the 61 files opened in 2016/2017. These files can be divided into a number of categories:

Requests for Review - Access to Information	15
Requests for Review - Privacy Issues	9
Consultations/Requests for Comment	7
Request for Review - Fee Assessment	5
Miscellaneous and Administration	5
Request for Correction to Personal Information	4
Breach Notification	3
Request for Review - Extension of Time	2
Request for Review - Third Party Objection	1
Breach Review (Commissioner Initiated)	1
Request to Disregard Access Request (S. 53)	1

These numbers indicate that, as in the previous year, requests for review of responses to access to information requests continues to be the primary focus. Breach of privacy complaints and breach notifications run a close second. This year our office also opened a file with a view to engaging the City of Yellowknife in a discussion about access and privacy issues in the light of the significant breaches of privacy which came to light through the media about stolen emails and the inappropriate use of cameras. The City did not respond to our letter and, as a result, no discussions took place. The Miscellaneous/ Administration files also included a number of speaking engagements, and media inquiries.



In addition to the matters resulting in the opening of a file, we have, of course, also dealt with many calls on a daily basis from people seeking basic information about the Act, which we deal with immediately and without the need to open a file.

Eighteen Review Reports were issued.

Health Information Act

The Health Information Act came into force on October 1st, 2015 and the number of files has skyrocketed this year, from eight files in 2016/2017 to 33 in 2017/2018. This is a positive development as it indicates that both the public and Health Information Custodians are beginning to pay more attention to their responsibilities surrounding the collection, use and disclosure of personal health information. Of these files:

- twenty-two were breach notifications received from the Department of Health and Social Services and the Northwest Territories Health and Social Services Authority pursuant to section 87 of the Act;
- six were breach of privacy complaints received from the public;
- two were privacy impact assessments received pursuant to section 89(2) of the Act;
- one was a request to review the response received to a request for access to personal health information pursuant to section 141;
- one was a review commenced on the Information and Privacy Commissioner's own motion pursuant to section 137(1);
- one was an administrative file

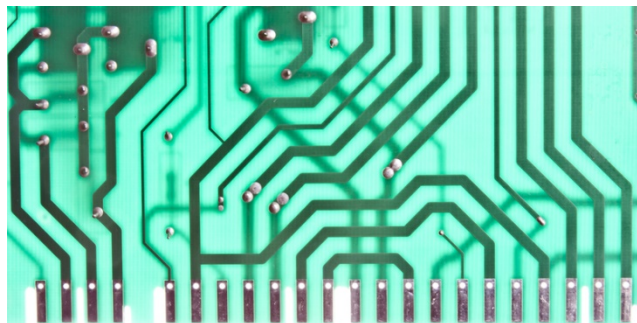
No Review Reports were issued under the *Health Information Act* in 2017/2018. In the case of most of the breach notifications, the breaches were relatively minor and corrected almost immediately. After discussions with the health information custodian in each case, the Information and Privacy



Commissioner was also satisfied with the steps taken to address the cause of the breach and to take steps to prevent further similar breaches. She did not, therefore, consider it necessary to do a formal review. Many of the breaches were the result of misdirected faxes from one office to another and the Information and Privacy Commissioner has, therefore, taken steps to do a systemic investigation on this issue.

There does not appear to have been any progress on meeting the requirement of ensuring that the public can avail themselves of the ability to control who has access to their personal health information as required by section 22 of the Act. There has, however, been some progress on the development of system wide standards, policies and procedures as required by section 8 of the Act in that we understand that the Minister issued a series of policies in May, 2017. The Office of the Information and Privacy Commissioner (OIPC) belatedly received a copy of those policies early in 2018 but they do not appear to be posted on line anywhere so that the public can read them. It is important for the public to be able to know how the Act is being implemented by way of policy directives.

As might be expected in light of the scope and of the health care system and the nature and extent of sensitive personal information that is collected, used and disclosed, there continue to be gaps that will need to be filled as the legislation continues to be applied.





REVIEW REPORTS

Review Report 17-160

Category of Review:	Access to Information - Deemed Refusal
Public Body Involved:	Yellowknife Housing Authority/NT Housing Corporation
Sections of the Act Applied:	Section 3(1)
Outcome:	- Recommendation with respect to policies accepted - Other recommendations rejected

The Applicant made a request to the Yellowknife Housing Authority (YHA) for access to his own personal information. He received no response and asked the Information and Privacy Commissioner (IPC) to review the matter on the basis of a deemed refusal. He was advised that the YHA was not a public body as defined in the *Access to Information and Protection of Privacy Act* and was directed to the Northwest Territories Housing Corporation (NTHC). The NTHC responded advising that the YHA had been directed to respond. No response was received. The IPC followed up with the NTHC and when no response was received to that correspondence, a review was commenced. The NTHC failed to respond to the IPC until well beyond the time frame provided by the IPC. In that response the NTHC argued that the Applicant had never made a formal request under the Act.

The IPC considered three issues. The first was what obligation the YHA had to respond to the request under the Act as it is not named as a public body subject to the Act. On this issue the IPC reiterated her findings from previous reviews that the Act applied to all records under the custody or control of a public body and that the relationship between the NTHC and YHA was such that the records were under the control of a public body (NTHC). The second issue was whether or not the Applicant had submitted a formal request under the *Access to Information and Protection of Privacy Act*. The IPC found that, while there might have been some initial confusion about this, that confusion was cleared up when the NTHC acknowledged receipt of the Applicant's request and advised him they were dealing with it. The third issue was the apparent lack of any process or procedure in place with



respect to how access to information requests should be handled by local housing authorities. The IPC recommended that NTHC establish a procedure to be shared with all local housing authorities outlining the steps to be taken when an access to information request is received. She further recommended that all local housing authorities have at least one designated employee responsible for ATIPP matters and that these individuals receive appropriate training. Finally, she recommended that there be an immediate response provided to the Applicant.

Review Report 17-161

Category of Review:	Request for Authorization to Disregard Request
Public Body Involved:	Department of Justice on behalf of itself, Department of Human Resources (now Finance), and Aurora College
Sections of the Act Applied:	Section 53
Outcome:	No Response Required

The Department asked that the Information and Privacy Commissioner authorize each of three public bodies to disregard further requests from a particular applicant who had submitted 25 separate requests to the Department of Human Resources (Finance) within a 12- month period, 9 to Aurora College in seven months and 2 over the course of one month to the Department of Justice. The Applicant had also directed 19 Requests for Review to the OIPC over the course of a year, as well as several privacy complaints. They argued that despite the best efforts of each of these departments to satisfy the Applicant's need for information, there was an underlying concern that their responses would never address the Applicant's concerns, which they said was evident from the tone and language of some of the Applicant's requests.

The IPC authorized each of the public bodies involved to limit the number of access to information requests from the Applicant to two at any one time.



Review Report 17-162

Category of Review:	Access to Information
Public Body Involved:	Department of Finance
Sections of the Act Applied:	Section 8, Section 12,
Outcome:	Recommendations Accepted

The Applicant made a request for information in relation to his employment with the Government of the Northwest Territories. The application was made to the Department of Finance. That department determined that it could only provide a partial response to the request and transferred the balance of the request to another department for response pursuant to section 12 of the Act, giving the Applicant notice of that transfer. With respect to that part of the request which the Department of Finance could respond to, there was some confusion with the response because, at the time, the Department was in the process of amalgamating with the Department of Human Resources and there was confusion over where the records were, therefore, located. The response was not provided within the 30 days provided for in section 8 of the Act. The department acknowledged that there was no explanation for the delay - that the ATIPP Coordinator simply lost track of the deadline.

The IPC recommended the creation of “bring forward” system for tracking access to information requests. She found that the Department of Finance had properly transferred portions of the request to another department and had done so in accordance with the Act. She made no recommendations with respect to the Applicant’s objections to that transfer.



Review Report 17-163

Category of Review:	Access to Information
Public Body Involved:	Department of Lands
Sections of the Act Applied:	Section 13(1)(b), Section 14(1)(b), Section 15(a), Section 23(2)
Outcome:	All Recommendations Accepted

The Applicant sought information in relation to the effort made to save the Robertson Head Frame at Con Mine in Yellowknife. The Department identified 67 records consisting of 245 pages of records and provided them to the Applicant with a number of redactions. They claimed that the following sections of the Act applied to justify the redactions:

- a) Section 13(1) which prohibits the disclosure of information subject to cabinet confidences;
- b) Section 14(1) which allows public bodies to withhold “consultations or deliberations” involving members of the public body;
- c) Section 15(a) which protects records subject to solicitor/client privilege;
- d) Section 23(1) which prohibits the disclosure of information which would constitute an unreasonable invasion of a third party’s privacy.

The IPC found that much of the information withheld pursuant to section 14 did not meet the criteria for the exception claimed because there was no advice sought or provided which was directed toward the making of a decision. She recommended the disclosure of some of the material redacted pursuant to this section. Similarly, she found that not all of the information redacted pursuant to section 13 would, if disclosed, reveal any cabinet confidence. She recommended the disclosure of some of the information redacted pursuant to this section. The IPC agreed with the public body with respect to the application of sections 15 and 23 and made no recommendations with respect to these items.



Review Report 17-164

Category of Review:	Privacy Complaint
Public Body Involved:	NWT Housing Corporation
Sections of the Act Applied:	Section 41(1)
Outcome:	All Recommendations Accepted

The NWT Seniors Society raised concerns on behalf of their members about changes to the NWT Housing Corporation's (NTHC) policies which required seniors and others in public housing to sign a document permitting NTHC to collect their personal information directly from Revenue Canada for the purpose of assessing rent. Some seniors expressed concerns about providing NTHC direct access to their Revenue Canada records and asked for an alternative but they were advised that unless they agreed, rent would be assessed on the basis of market rent and failure to pay rent would result in eviction. NTHC explained that the new policies resulted in far more secure exchange of information with fewer employees having any access to that information. They argued that the new method of collecting information respected the dignity of public housing tenants by treating them more like other tenants. At the same time, the new process would "drastically increase" the efficiency of the rental assessment process by enabling a switch from manual monthly assessments to an automated annual assessment.

The IPC noted that the right to privacy is about the right of the individual to choose what information about him or her is provided to whom and how. While she agreed that the new process was likely more privacy protective than the previous way of doing things, the consent required for participation in the subsidy programs was really no consent at all – it was a mandatory requirement to be considered for a rent subsidy. The IPC recommended:

- a) the development of policies/procedures to address situations in which a client (new or existing) is unwilling to provide consent for NTHC to access their CRA records without disqualifying them from receiving a subsidy;



- b) that consent for access to CRA records must be free and voluntary, and not coerced;
- c) that the consent obtained from clients be time limited and subject to renewal on a regular basis;
- d) that a copy of her Review Report be shared with other public bodies using a similar arrangement with Canada Revenue Agency.

However, where there is a reluctance and where the individual involved does not wish to provide the Housing Corporation with access to their CRA records, that wish must, in my opinion, be honored

Review Report 17-164

Review Report 17-165

Category of Review:	Access to Information
Public Body Involved:	Department of Human Resources (Finance)
Sections of the Act Applied:	Section 1, Section 23(1), Section 23(2), Section 23(5), Section 22, Section 5, Section 2 (personal information)
Outcome:	Recommendations Largely Accepted

The Applicant requested a copy of all statements made to investigators during a workplace harassment investigation which contained reference to himself or to his position. The Department refused access to all such records, citing section 23 of the Act (disclosure would constitute an unreasonable invasion of the privacy of a third party). They argued that in denying access to the records, they had “endeavored to balance the applicant’s right of access with the rights to privacy of the third parties. They disagreed with previous findings of the IPC including:

- a) that an opinion about an individual is personal information belonging to the person the opinion is about;



- b) that section 22 provides an exception for employment references only, and does not apply to opinions provided during a workplace investigation.

The department noted that it was the practice for investigators to inform witnesses at the start of all interviews that the statements are being supplied in confidence and will be kept confidential by the department so as to encourage employees to be open, honest and forthright in speaking about workplace issues.

In this case, third party consultations had been conducted pursuant to section 26. One of the third parties consented to the disclosure and four others did not respond. Others expressed “fear” of repercussions because of the “highly acrimonious relationship” between the parties, notwithstanding the fact that the Applicant was no longer employed with the GNWT and was no longer resident in the NWT.

The IPC reiterated her previous findings that an opinion expressed about an individual is the personal information of that individual, not the personal information of the person providing the opinion. She further reaffirmed her finding that section 22 applies only to information gathered “solely for the purpose of determining the applicant’s suitability, eligibility or qualifications for employment, awarding government contract or other benefits”. She found that while some of the content of the records in question invited redaction, it was inappropriate for the public body to withhold all of the records in their entirety. She found that where consent to disclosure was provided, there was no reason not to disclose the record in question and recommended the disclosure of the that statement with some minor redactions. She reviewed each of the remaining statements and recommended the disclosure of portions of each. Finally, the IPC recommended that the “practice” of providing assurances of confidentiality in workplace investigations be discontinued and that, instead, the practice be changed to accord with the legislative requirements of the ATIPP Act and existing GNWT policies such that it is clear that statements made may, in some circumstances, be disclosed to a complainant, a respondent, or other parties involved in the investigation.



While I can certainly understand the importance of stressing the need for confidentiality in terms of witnesses discussing matters outside of an investigative process and the need to be able to assure witnesses and parties that information will not be shared by the department beyond the confines of the investigation, it seems to me that if the public body truly intends to “balance” the rights of the complainant and of the respondent in such circumstances, their assurances of confidentiality must also be accompanied by a caveat that the information can (and likely will) be shared with the complainant and the respondent.

Review Report 17-165

Review Report 17-166

Category of Review:	Breach of Privacy
Public Body Involved:	Aurora College
Sections of the Act Applied:	Section 1, Section 40, Section 48
Outcome:	Recommendations Accepted

The Complainant asked the OIPC to review whether or not his employer, Aurora College, had improperly collected or attempted to collect personal health information for the purpose of administering his sick leave or other health related benefits received by him. He had several complaints including the existence of a secondary personnel file within the college administration offices, the number of people who had access to this secondary file (including a letter which contained what he considered to be untruthful opinions about him), that a form he had been asked to have completed by his physician had been altered such that the college was attempting to collect more information than they were entitled to, and that someone employed with the college called his mother and disclosed his personal health information, including unproven statements about his mental health and his employment status.



Aurora College admitted that it maintains a “copy” of some personnel files to allow for the administration and management of personnel within the program area, as authorized by the GNWT’s Human Resources Guidelines. Access to such files is limited, though during the course of the review the College determined that they should be restricting access further. With respect to the medical prognosis form, the college argued that the form was “altered” so as to direct the attention of the medical practitioner to the focus of their specific concerns. Finally, they confirmed that someone within the administration had contacted the Complainant’s mother after a particular incident in the workplace that raised concerns but that they had disclosed just enough personal information to indicate that they perceived an urgent need for the parent to contact the Complainant.

The IPC agreed that there was no inappropriate collection of personal health information by the college. There were, however, some questions about the way in which the Complainant’s personal information was used. She recommended that the Request for Medical Prognosis form, whether or not it was completed, should be put in a sealed envelope in both the official and secondary personnel files of the Complainant, with a notation that the contents were personal and confidential to be opened only with the consent of the Complainant, a court order or otherwise in accordance with law, with notice to the Complainant. She recommended as well that the college take steps to review their policies with respect to access to personnel files held by them such that only those with a “need to know” have access. The IPC found that the contact with the Complainant’s parent was justified pursuant to section 48(q) of the Act which allows disclosure where there is a genuine concern about the safety or well-being of any person. She did, however, recommend the establishment of a clear policy and procedure for such contact, when necessary.



Review Report 17-167

Category of Review:	Access to Information – Deemed Refusal
Public Body Involved:	Department of Human Resources (Finance)
Sections of the Act Applied:	Section 8
Outcome:	No New Recommendations Made

The Applicant made a request for information on June 23, 2016. The request was acknowledged on July 8th and on July 22 a fee assessment was issued. On July 28, the Applicant issued a revised request to avoid the application of fees. On August 5, the department acknowledged that the fee issue was resolved and indicated that a response would be provided by November 4th, after a third-party consultation took place. In September, the Applicant's lawyer and counsel for the Department of Human Resources agreed that the ATIPP request would be suspended during negotiations aimed at resolving issues between the Applicant and the GNWT. On November 17th, the Applicant withdrew from those negotiations and on November 23rd asked for a response to his request for information. The public body acknowledged the renewal of the request process and indicated that a response would be provided, but did not give the Applicant a date for their response. On December 7th, the Applicant sought a review, claiming deemed refusal. The responsive records were, in fact, provided to the Applicant on January 26th, 2017.

The IPC noted that these were the same circumstances as outline in Review Report 17-157, but with respect to a different Access to Information Request. She noted the recommendations made in that report. She made no new recommendations in this case.




Review Report 17-168

Category of Review:	Access to Information –Third Party Objection
Public Body Involved:	Department of Education, Culture and Employment
Sections of the Act Applied:	Section 26, Section 23,
Outcome:	Recommendation Accepted

A request received from a Third Party to review the Department's decision to disclose portions of a workplace investigation report in which the Third Party had been involved. The report had been requested by another party involved in the investigation. The Third Party argued that the investigation process had been very stressful for him and he did not see a valid reason why the report needed to be accessed since due process had been followed during the investigation process. He asked that the report be withheld in full.

The IPC found that the department had properly identified and removed any material in the report which, if disclosed, would constitute an unreasonable invasion of the third party's privacy and recommended that the report be disclosed as proposed.



The Section [Section 14] does not apply to justify the exclusion of information that indicates that a discussion took place, the topic of the discussion or the participants in that discussion.

Review Report 17-169



Review Report 17-169

Category of Review:	Access to Information
Public Body Involved:	Department of Human Resources (Finance)
Sections of the Act Applied:	Section 23, Section 14, Section 3
Outcome:	Recommendation to disclose the Applicant's own personal information rejected Recommendations with respect to the application of section 14 rejected in part

The Applicant sought information in relation to a specific job competition, including his own personal information and the personal information of the successful applicant. The Department identified 42 responsive records and provided him with a redacted copy of those records. The Applicant indicated he wanted the information to assist in researching and validating the claims, disputes and grievances of aboriginal people trying to gain employment or advancement in the public service.

The public body argued that the interview questions requested did not fall under the ATIPP Act because section 3(d) provides that questions used in an examination or a test are not subject to ATIPP requests. With respect to those portions of the records redacted pursuant to section 23 of the Act, they note that the disclosure of the successful candidate's information would be an unreasonable invasion of his privacy and that disclosure was, therefore, prohibited. They also argued that section 14(1)(b)(i) applied to some of the information in the records where the redacted portions of the records involved officials discussing topics in a confidential manner to determine various courses of action.

The IPC agreed that the interview questions, in this case, were outside the scope of the ATIPP Act because they were questions that the public body intended to use again in future job competitions. No recommendations were made with respect to these questions. She noted however, that the exclusion applied only to the questions, not the other parts of the record, including the information under "Expected Answer", "Response" and "Rating". With respect to the "Expected Answer" information, she found that section 18 of the Act provides the public body with the discretion to



refuse access to information relating to testing or auditing procedures or details of specific tests. She recommended the public body exercise their discretion with respect to this information. She recommended, as well, the disclosure of the answers which the Applicant provided to the questions, but agreed that the answers provided by other candidates, as well as scoring and ratings for other candidates were protected pursuant to section 23 of the Act. She found that much of the information redacted pursuant to section 14(1)(b) did not meet the criteria for such an exception and recommended the disclosure of that information.

Review Report 17-170

Category of Review:	Fee Waiver
Public Body Involved:	Department of Human Resources (Finance)
Sections of the Act Applied:	Section 5(3), Regulation 14, Section 7
Outcome:	Recommendation to create policies and criteria for fee waivers accepted Recommendation to consider “other matters” rejected


The Applicant made a request for his own personal information. The public body identified approximately 3,760 pages of responsive records and provided the Applicant with a fee estimate of \$940 based on 25 cents per page and requested a deposit of \$470 in accordance with Regulation 13. As a result of the initial fee estimate, the Applicant revised his request for information and a new fee estimate of \$213.75 was provided. The Applicant requested a fee waiver pursuant to Regulation 14 but that request was refused because the Applicant had not demonstrated proof of inability to pay, there were a large number of records requested, the Applicant had not provided any compromise solutions. They noted, as well, that the department had already provided considerable information in relation to the subject of the Applicant’s request in responses to previous requests from him.

The IPC found that the public body had not met their duty to assist the Applicant as required by Section 7 of the Act in that they did not provide him with any guidance as to the kind of information they would require to consider his request. As a result, the Applicant was not given a chance to



establish his financial hardship in a manner that would be satisfactory to the public body. She recommended the creation of a process and relevant criteria for assessing such waiver requests so that Applicants know what it is they need to show. She also found that the public body had failed to consider other reasons that might apply. She reviewed some of the considerations other than financial ones that she felt were relevant and should have been considered.

The IPC recommended that the department specify the information they required from the Applicant to assess his financial ability to pay and that the public body reconsider its decision not to waive fees based on factors other than financial hardship to the Applicant.



Section 7 of the Act imposes on public bodies a 'duty to assist' Applicants seeking information under the Act. In my opinion, this duty to assist imposes on public bodies the responsibility to at least offer an Applicant some guidance on what is expected of them in making a claim for a waiver of fees

Review Report 17-170

Review Report 17-171

Category of Review:	Correction to Personal Information
Public Body Involved:	Department of Human Resources (Finance)
Sections of the Act Applied:	Section 1, Section 45, Section 46(2)
Outcome:	No Recommendations Made

The Applicant, a former employee, had been involved in a workplace harassment investigation prior to his departure. He did not agree with the findings of the investigator and disagreed with many of



the things said about him by other witnesses. He asked that corrections be made in the investigator's report so that it reflected "the truth" as he saw it.

The IPC found that in order for section 45 to apply, the correction request must be directed toward personal information as defined in the Act and that the section applies only to factual information about an individual. It does not apply to any conclusions reached by an investigator, procedural steps taken by the investigator or opinions expressed either by the investigator or any of the witnesses, or to correct something said by a witness. Section 45 cannot be used, in effect, as a means of appeal or to change the conclusions reached. She found that none of the corrections requested by the Applicant were corrections contemplated by section 45. No recommendations were made.

Review Report 17-172

Category of Review:	Third Party Objection
Public Body Involved:	Aurora College
Sections of the Act Applied:	Section 33, Section 28(2)
Outcome:	Recommendations Accepted

An Applicant sought certain information in relation to a workplace harassment investigation to which he was a party. Another individual, who was also a party to the investigation, objected to the disclosure and asked this office to review the college's decision to disclose portions of the report on the basis that disclosure would constitute an unreasonable invasion of the Third Party's privacy.

The IPC determined that, in the form that the public body intended to release the records, all personal information about the Third Party had been removed and there could, therefore, be no unreasonable invasion of his privacy. She recommended the disclosure of the record as proposed.



Review Report 18-173

Category of Review:	Access to Information
Public Body Involved:	NT Health and Social Services Authority
Sections of the Act Applied:	Section 14(1) and 23(1)
Outcome:	Recommendations Accepted

The Applicant was an employee of a public body. He made a request for the contents of his personnel file, as well as the contents of any supervisory type files about him in the possession of the Applicant's supervisor and emails about him between several co-workers for a specified period of time. The Applicant was provided with a package of responsive records, but there was a considerable amount of information redacted pursuant to sections 14(1) and 23(1). The Applicant asked the OIPC to review the response received. He also suggested that there were handwritten notes that were missing from the responsive package and expressed, as well, concern about the apparent existence of a "shadow" personnel file.

The submissions from NTHSSA were extremely brief and noted that the information redacted pursuant to section 23(1) was "identifying information of a third party" and that the items withheld pursuant to section 14(1)(b) was "specific to consultation with employees of a public body".

The IPC found that most of the information withheld pursuant to section 14(1)(b) did not meet the criteria to qualify for the exception and recommended that most of that information be disclosed. She further found that the disclosure of information that relates to an employee's employment responsibilities as an officer or employee of a public body, even where the employee is identifiable, does not constitute an unreasonable invasion of the employee's privacy. She recommended the disclosure of much of the information withheld pursuant to section 23(1). She recommended that further searches be done specifically to locate hand written notes and other paper records.



Review Report 18-174

Category of Review:	Access to Information
Public Body Involved:	Department of Justice (Coroner's Office)
Sections of the Act Applied:	Section 16(1)(a)(i), Section 16(1)(c), Section 23(2)(a), Section 52(2), Section 23(2)(h)
Outcome:	Recommendations with respect to section 23 accepted Recommendations with respect to section 16 largely rejected Other Recommendations accepted in part

The Applicants were the executors of the estate of their son who had died in a work-related accident. They requested all records gathered or created by the Coroner's Office in the investigation of the accident. Most of the responsive records were disclosed in full or in part. Five records were withheld in full. These five records were all created by the R.C.M.P. and were withheld pursuant to section 16(1)(a)(i) and/or section 16(1)(c). Other records were withheld to protect third parties from an unreasonable invasion of their privacy.

One of the pieces of information consistently redacted from the records was the personal email address and name of an individual who worked, on a part time basis, as a Community Coroner. The IPC agreed that the personal email address was properly redacted. She recommended, however, that steps be taken to provide Community Coroners with access to GNWT email addresses or that directives be implemented prohibiting Community Coroners from communicating via personal email accounts unless the communication is encrypted. Also withheld were the names, email addresses and in some cases other business contact information of employees of certain third-party organizations. The IPC found that the disclosure of this information would not amount to an unreasonable invasion of any third party's privacy and recommended the disclosure of that information.

The public body also withheld some information on the basis that disclosure of the information could reasonably be expected to impair intergovernmental relations, arguing that any conversation



between the R.C.M.P. and the Coroner's Office is automatically deemed to be confidential and that disclosure would impair the relationship between the two governmental agencies. The IPC, however, found that a blanket exception was inappropriate and that in every case the public body had to establish that the communication was intended to be confidential and, even then, discretion needed to be exercised. Further, because access to information is a "right", it was incumbent on the public body to at least consult with the R.C.M.P. about disclosure. She noted that the *Coroner's Act* requires the R.C.M.P to provide information to the Coroner's office in certain circumstances, but nowhere in that Act does it provide that such information is deemed to be received in confidence. She therefore found that the suggestion that the R.C.M.P may no longer cooperate in Coroner's investigations if communications between them were disclosed was unfounded. She recommended the disclosure of large parts of the information that was withheld pursuant to section 16.

Review Report 18-175

Category of Review:	Access to Information – Fee Assessment
Public Body Involved:	Department of Human Resources (Finance)
Sections of the Act Applied:	Section 50
Outcome:	No Recommendation Made

The Applicant made 6 separate access to information requests to the same department on the same day. Five of these six requests were in relation to the same subject matter. The public body decided to combine the five related requests into one and provided the Applicant with a fee estimate based on the combined request. The Applicant objected to the combination of the five requests into one, arguing that if they had answered each request individually, there would have been low or no applicable fees under the Act. The Department argued that it was justified in combining the requests to reduce processing time, avoid the potential for delays, and so that an appropriate fee could be assessed. They noted that by doing things this way, they could avoid providing duplicate and repetitive files, helping to reduce the time and costs associated with the requests. They noted that



the combining of the requests made a minimal difference (\$1.00) in the cost to the Applicant in this case.

The IPC agreed with the public body's reasoning in this case and made no recommendation.

Where, as in this case, the public body combines a number of requests all received on the same day and all dealing with the same or overlapping records with respect to a single issue so as to take advantage of processing efficiency, it benefits the public body, the public interest, and the Applicant, all at the same time

Review Report 18-175

Review Report 18-176

Category of Review:	Access to Information – Fee Assessment
Public Body Involved:	Department of Justice
Sections of the Act Applied:	Section 5, Section 50
Outcome:	Recommendation Rejected

The Applicant, a member of the press, requested information in relation to an incident involving the use of fentanyl at a correctional facility in the Northwest Territories. The department assessed fees of \$195.00 for the access request. The Applicant sought a review on the basis that he perceived a discrepancy in the way in which fees were being charged by different departments.

The department noted that it had not yet converted its records to the Digital Integrated Information Management System (DIIMS) which would allow one person with the required authorization to search across both shared drives and email platforms, dramatically decreasing search times. As a result, individual searches are required, which results in more time and, therefore, more costs to the



Applicant. They noted, as well, that the nature of these records was such that they all contained significant amounts of personal information and they would have to be reviewed line by line to avoid disclosure of records that would result in an unreasonable invasion of third party privacy.

The IPC found that the costs assessed for photocopying and for searching and retrieving the records was reasonable, noting that the fact that the Department of Justice did not yet have the benefit of the DIIMS system was not a factor and that there was no requirement that a public body use a particular system or that they conduct their searches in a particular way. She noted, however, that the Regulations were inconsistent in that, while the fee schedule allows for a fee for “preparing and handling a record for disclosure”, Regulation 11(6) clearly states that a fee may not be charged for “the time spent in reviewing a record”. She found that the only time that can be charged to an Applicant is the time to “prepare and physically sever” the records for disclosure. The time to review the record and make decisions with respect to what redactions should occur constitutes “review” and is not time that can be charged back to the Applicant. Because this public body uses redaction software, the time necessary to actually physically sever the records should be “seconds per page”. She recommended reducing the fees assessed for “preparing and handling the record for disclosure” be reduced by 2/3. This would bring the total fees under the \$150.00 threshold for the charging of fees and recommended that no fees, therefore, be assessed.

Review Report 18-177

Category of Review:	Access to Information
Public Body Involved:	Department of Education, Culture and Employment
Sections of the Act Applied:	Section 1, Section 23(4)
Outcome:	Recommendations Accepted

The Applicant, a lawyer, made a request to the Department of Education, Culture and Employment on behalf of several of his clients, with the written consent of each client, for information in relation to an investigation into the complaints of sexual abuse against a named health care worker in a



particular community for a particular time frame. The response consisted of 10 pages of records, which were heavily redacted pursuant to section 23 of the Act, which prohibits the disclosure of information that would amount to an unreasonable invasion of the privacy of a third party. The public body had redacted all names and personal identifiers.

The IPC found that to the extent that the redacted information related to the names and positions of GNWT employees who dealt with the incident, section 23(4) provided that the disclosure of this information would not amount to an unreasonable invasion of privacy in that it was information in relation to the employee's responsibilities as an officer or employee or member of the public body. Further, because the perpetrator had already been identified (charged and convicted) in the small community and, in fact, had been named by the Applicant both in the access request and in civil proceedings before the courts, the disclosure of his name would not constitute an unreasonable invasion of his privacy. She did find, however, that some of the details about the perpetrator's state of mind would be an unreasonable invasion of his privacy. She recommended the disclosure of some additional information.





TRENDS AND ISSUES - MOVING FORWARD

Comprehensive Review

I would very much like to see the next steps taken in creating updated access and privacy legislation following the comprehensive review begun almost two years ago now. The world has changed dramatically in the twenty plus years since the current Act came into effect. The nature of government records and the way such records are created, managed and stored has changed completely. Paper records are now the relatively rare exception. Nearly everything is digital. Employees can (and often do) conduct business by email, text and other electronic means, sometimes outside of the GNWT system, and every government employee is responsible for the management of his or her own records. The ombudsman model that worked well two decades ago is not working as well as it once did. The Office of the Information and Privacy Commissioner requires more power to ensure compliance there must be consequences above and beyond being called out in an Annual Report when a public body refuses to accept the recommendations of the IPC. I heartily endorse and encourage the establishment of a system similar to that in Newfoundland and Labrador where the IPC still makes recommendations (rather than orders) but if a public body wishes to disregard or reject those recommendations, it must make an application to the court to authorize them to do so. Provisions must also be included to implement a means of ensuring that, once a recommendation is accepted, the public body follows through and implements it. There needs to be a clear duty to document conversations and actions taken by and on behalf of a public body so that the information is available on an access request, regardless of whether or not it was created on or by GNWT equipment. This is important legislation that badly needs updating and I strongly urge that amendments to the Act be made a priority.



Review of Policies

In addition to a review of the Act, there is also a need for a comprehensive review of policies and procedures with respect to the use of electronic records. There does not appear to be any policy that addresses, for example, the use of personal devices, text messaging and/or personal email accounts for the purpose of doing GNWT business. When is it appropriate for employees of a public body to use their own email address or their own personal device to communicate with respect to government business? Best practices would suggest that the use of personal devices and personal email addresses be prohibited except in exigent circumstances. When used, there should be clear and well-articulated directions with respect to the management of such communications and clear consequences for failure to comply with the policy. There should also be clear policies with respect to the encryption of email correspondence in any circumstance in which the email contains personal information, the use of jump drives and other portable memory devices and restrictions on the kind of information that can be downloaded onto devices such as laptops, tablets and other mobile devices that can be removed from the workplace. These are but a sampling of the policies and procedures that need to be in place to address today's reliance on digital communications. I would strongly recommend that a thorough review be done of all relevant policies and that old policies be amended and new policies created to deal with these issues.

The Use of Fax Technology in the Health Sector

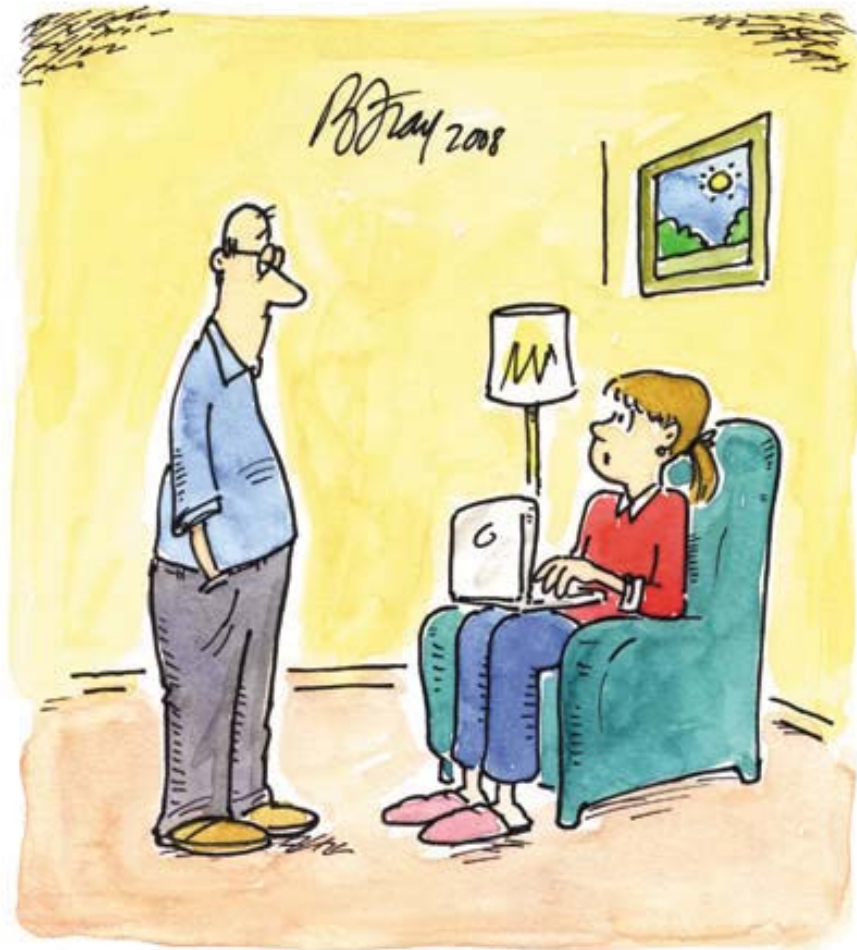
One of the issues that came up time and again over the course of this year was the continued use of fax machines by health care professionals to communicate with other health care professionals, with patients and with others. No less than nine of the twenty-two breach notifications received from health information custodians involved information that had been sent by fax and had ended up in the wrong hands. This is not a problem unique to the Northwest Territories. There appears to be an inherent reluctance within the health care sector Canada-wide to adopt more secure, modern technology. Personal health information is some of the most sensitive of personal information and it



should be treated accordingly. No significant effort or knowledge is needed to utilize email and encryption and it is time that the health care sector takes this simple step to decrease the incidents of breaches as a result of misdirected faxes. While emails can also go astray, simple encryption programs can serve to ensure the content of the email will not be inappropriately disclosed because only the intended recipient will be able to read the encrypted information. I encourage the Department of Health and Social Services to take the lead in this transition and create appropriate steps to create policies and procedures to encourage the health sector to update its communications strategies by reducing the use of faxes.

Education

As noted in my opening comments, education is a key for our children to learn to work in the digital world while being able to protect their privacy at the same time. This generation will “live” on-line and it is important that they have the tools, starting at a very young age, to do that safely. They need to be able to recognize the way in which their personal information is being mined and used so that they can make intelligent choices. We are behind the curve on ensuring that necessary education. That said, a lot of work has been done to develop appropriate age-level educational materials and course outlines. One of the projects that my counterparts from across the country and I have taken on is to create some basic lesson plans for this purpose. Three of these lesson plans have recently been published and these can be found on my website under the heading “Resources”. More needs to be done by the Department of Education, Culture and Employment to ensure that children start to learn about the value of their privacy, how to protect privacy on-line and how to deal with on-line bullying. This education has to begin right from kindergarten and continue all the way through to Grade 12. I would encourage the Government of the Northwest Territories to ensure that this education is embedded in the curriculum for all grades as soon as possible.



"OF COURSE I VALUE MY PRIVACY,..THAT'S WHY I ONLY SHARE MY PERSONAL INFORMATION WITH 700 OF MY CLOSEST FRIENDS!"



**OFFICE OF THE
INFORMATION
AND PRIVACY
COMMISSIONER**

NORTHWEST TERRITORIES



RAPPORT ANNUEL 2017-2018

Commissaire à l'information et à la protection de la vie
privée des Territoires du Nord-Ouest

Résumé

Table des matières

MESSAGE DE LA COMMISSAIRE	5
BILAN DE L'ANNÉE	11
Loi sur l'accès à l'information et la protection de la vie privée	11
Loi sur les renseignements sur la santé	12
TENDANCES ET ENJEUX - POUR ALLER DE L'AVANT	15
Un examen approfondi.....	15
L'examen des politiques.....	16
L'utilisation des télécopieurs dans le secteur de la santé	17
L'éducation	17





MESSAGE DE LA COMMISSAIRE



L'année dernière, dans mon rapport annuel, j'ai noté que des lois solides en matière d'accès à l'information et de protection de la vie privée sont plus essentielles que jamais au maintien de nos idéaux démocratiques alors que le monde change de manière que nous n'aurions pas pu imaginer en 1997 lorsque la *Loi sur l'accès à l'information et la protection de la vie privée* est entrée en vigueur. Aujourd'hui, nous vivons à l'ère des « fausses nouvelles » et des « faits alternatifs » générés par des politiciens puissants, ce qui rend d'autant plus importante la législation sur l'accès à l'information et la protection de la vie privée du secteur public. Il

est essentiel pour la santé de notre démocratie et de nos idéaux démocratiques que nous continuions à encourager un gouvernement ouvert et responsable chez nous et je maintiens que l'un des outils les plus puissants et les plus efficaces pour ce faire est une législation solide sur l'accès à l'information et la protection de la vie privée. Il y a plus de deux ans que le ministère de la Justice a entrepris une consultation publique sur un examen de la loi. Depuis, j'ai très peu entendu parler de la progression de ce projet. Au printemps dernier, on m'a fait part de certaines des orientations que le ministère pourrait prendre dans sa proposition législative; depuis, plus de nouvelles. Je comprends que le gouvernement est un immense navire difficile à piloter et que l'élaboration des lois entourant la légalisation du cannabis a tenu le ministère de la Justice particulièrement occupé, mais il est décourageant de constater qu'il prenne tant de temps pour régler cette importante mesure législative. Les Territoires du Nord-Ouest sont maintenant la dernière entité canadienne, exception faite du Nunavut, à moderniser sa législation sur l'accès à l'information et la protection de la vie privée de première génération. J'espère que des progrès seront réalisés au cours de la prochaine année.



Cependant, une législation moderne n'est pas une panacée. Nous avons besoin d'un engagement réel à l'égard de l'esprit et de l'intention de la loi et cette année, plus que toute autre année, j'ai constaté une diminution marquée de la volonté des organismes publics de défendre ces idéaux. Plusieurs fois cette année, les organismes publics ont refusé de suivre les recommandations formulées, rejetant mon analyse et l'application de la loi. Comme mon bureau n'a que le pouvoir de formuler des recommandations et que le seul recours pour un demandeur est un pourvoi — coûteux, long et complexe — devant les tribunaux, les organismes publics peuvent facilement éviter de rendre des comptes lorsqu'ils refusent de suivre les recommandations formulées. Je comprends qu'il est parfois inconfortable pour les organismes publics de divulguer certains documents et qu'ils préfèrent s'y soustraire, mais c'est justement pour cette raison que mes recommandations doivent avoir plus d'impact. Je suis maintenant convaincue que la situation nécessite une modification du modèle utilisé. En 2015, Terre-Neuve-et-Labrador a adopté une loi sur l'accès à l'information et la protection de la vie privée réputée la meilleure du genre de toutes les provinces canadiennes, et peut-être même du monde entier. En vertu de cette loi, le commissaire à l'information et à la protection de la vie privée ne détient toujours qu'un pouvoir de formuler des recommandations. Toutefois, un organisme public qui souhaite ignorer ses recommandations doit d'abord obtenir l'autorisation d'un tribunal. Cette nouvelle loi oblige l'organisme public, comme il se doit, à obtenir l'approbation de la cour, au lieu d'obliger le demandeur à contester la décision devant les tribunaux. J'ai encouragé le ministère de la Justice à prendre la loi terre-neuvienne comme modèle, et j'ai bon espoir qu'une fois déposée, la nouvelle loi prendra acte de cette approche.

Encore une fois cette année, je me suis aussi inquiétée de la gestion maladroite de la Ville de Yellowknife d'une série de violations de la vie privée, à commencer par le vol apparent de correspondances électroniques contenant toute une gamme de renseignements, notamment des informations sensibles sur le personnel. Cette correspondance a ensuite été transmise à la presse locale, qui l'a publiée. Cette révélation a été suivie par l'annonce qu'un membre du personnel cadre



aurait utilisé les caméras de surveillance de la Ville de Yellowknife pour surveiller des femmes indûment dans des installations municipales.

À l'époque, j'ai écrit aux représentants de la ville pour leur proposer mon aide afin d'instaurer un dialogue sur les enjeux en lien avec la protection des renseignements personnels et l'adoption d'une politique de confidentialité robuste à l'hôtel de ville. Ma lettre est restée lettre morte.

Ce n'est pas la première fois que je tends la main à la Ville pour traiter des questions de confidentialité, et ce n'est pas la première qu'on fait la sourde oreille à mes propositions. La ville ne semble pas souhaiter formaliser ses politiques en matière d'accès à l'information et de protection de la vie privée. Fait à noter : J'ai recommandé que les municipalités soient considérées à titre d'organismes publics en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* pour la première fois dans mon premier rapport annuel en 1998, il y a vingt ans. J'ai répété cette recommandation presque chaque année depuis, mais aucun effort n'a été déployé pour apporter les rectificatifs nécessaires. Comme le Nunavut a récemment modifié sa loi sur l'accès à l'information et la protection de la vie privée pour qu'elle s'applique aux municipalités, les Territoires du Nord-Ouest sont le dernier territoire canadien à ne pas imposer de normes minimales de protection sur l'accès à l'information et la protection de la vie privée aux administrations municipales. Les événements récents qui ont secoué la Ville de Yellowknife, et son incapacité à prendre les mesures nécessaires dans de telles circonstances, ne font que souligner l'importance d'une telle loi. J'exhorte à nouveau le ministère de la Justice à faire en sorte que les municipalités ténoises soient assujetties aux mêmes lois et règlements que les municipalités du reste du Canada.

Cette année, les travaux de modernisation de la *Loi sur les renseignements sur la santé* se sont poursuivis. Le ministre a mis en œuvre un train de politiques et de procédures, comme l'exige l'article 8 de la Loi, et nous avons constaté une hausse des signalements de violations de la vie privée. Ces signalements nous laissent croire que les personnes chargées de s'en occuper cernent les problèmes et les règlent plus facilement. Toutefois, je suis toujours préoccupée par le nombre de



signalements concernant des télécopies envoyées au mauvais numéro, ou des courriels non chiffrés. J'ai encouragé les professionnels de la santé à abandonner le télécopieur, archaïque, peu sûr, complexe et chronophage, au profit du courriel chiffré, un moyen de communication récent et sûr. Je ne comprends pas l'apparente réticence du secteur de la santé à passer à une technologie supérieure lorsqu'une solution simple et accessible est à portée de main, et ce, sans frais de formation, ou presque.

Lors de la rencontre annuelle des commissaires à l'information et à la protection de la vie privée, organisée cette année à Iqaluit, nous avons eu droit à une présentation de membres de la Première Nation des Kwanlin Dün du Yukon, qui sont en train d'instaurer leur propre législation en matière d'accès à l'information et de protection de la vie privée. Ils nous ont raconté comment ils sont partis d'un entrepôt rempli de vieilles caisses non identifiées qui, au fil du temps, avaient soit servi de nid pour les oiseaux, soit servi de nourriture pour les rongeurs. Ils ont commencé à organiser et à rassembler l'information en un système bien organisé et facile à consulter. Ils concentrent maintenant leurs efforts à l'adoption d'une loi pour encadrer l'accès à cette information par les membres de la Première Nation. Leur témoignage s'est révélé un exemple de travail acharné et d'engagement des plus enrichissants.

Lors de la même rencontre, les professeures Valerie Steeves et Jane Bailey de l'Université d'Ottawa nous ont entretenus de leur projet *e-Quality Project*, un partenariat d'universitaires, d'instituts de recherches et de politiques, de décideurs, d'éducateurs, d'organismes communautaires et de jeunes. Le projet met l'accent sur les politiques des entreprises à l'ère de l'économie numérique, spécialement en ce qui a trait à la confidentialité, aux relations saines, au respect de l'égalité en ligne, et souhaite sensibiliser les jeunes aux interactions en ligne.



Le modèle économique derrière le commerce électronique (c'est-à-dire la divulgation d'information en échange de services) incite les utilisateurs à divulguer des renseignements. Les jeunes sont la clé pour comprendre les implications de ce type de comportement sur la confidentialité, car, en tant qu'utilisateurs précoces de médias sociaux et de services en ligne, ils disséminent des téraoctets de données (souvent sans le savoir) de façon quotidienne. Ces données sont utilisées pour les cibler avec du marketing comportemental afin de façonner leurs attitudes et leurs comportements, souvent au mépris des réglementations existantes sur la confidentialité, puisque les politiques de confidentialité ne divulguent pas complète l'analyse employée (rendant difficile le consentement éclairé), et que le profilage permet également de récolter des données non personnelles, et qui évite le processus de consentement.

Les professeures Steeves et Bailey ont présenté certaines de leurs conclusions et ont fait part de leurs observations sur la manière dont les jeunes, à l'ère de Facebook, Snapchat et Instagram, gèrent leur vie privée. C'était fascinant d'entendre comment les jeunes perçoivent leur vie privée et modifient leur comportement pour protéger ce qu'ils considèrent comme leur information la plus confidentielle. Toutefois, il reste beaucoup à faire pour éduquer nos jeunes sur la meilleure façon de protéger leur vie privée en ligne. À cette fin, j'ai participé avec mes confrères commissaires à l'information et à la protection de la vie privée de tout le pays à l'élaboration d'un certain nombre de plans de cours pour enseigner aux jeunes comment protéger leur vie privée en ligne. Ces leçons se sont révélées des plus populaires dans de nombreux territoires et de nombreuses provinces. Elles sont disponibles dans mon site Web sous l'onglet Ressources et j'encourage les enseignants des Territoires du Nord-Ouest à tirer parti du bon travail accompli à cet égard.



Nous avons également continué à mettre à jour et à améliorer notre site Web (www.atipp-nt.ca). Il contient quantité d'informations sur notre travail, notamment tous nos rapports annuels, nos rapports de révision et nos rapports spéciaux, la loi et ses règlements, des liens vers des sites utiles d'autres territoires, provinces et organisations et bien plus encore. Nous mettons continuellement notre site à jour et y ajoutons de nouvelles informations. Nous souhaitons qu'il constitue une ressource de qualité pour les organismes publics et le public en ce qui a trait aux questions d'accès à l'information et de protection de la vie privée. Tout indique que le site est consulté fréquemment et que les rapports de révision, en particulier, sont consultés et téléchargés régulièrement.

Pour conclure sur une note positive, je suis heureuse de mentionner que mon budget a été augmenté pour tenir compte de la création d'un poste de commissaire adjoint à temps plein, qui travaillera également pour la commission du Nunavut. Je suis heureuse de pouvoir compter sur une personne supplémentaire, particulièrement en raison de la charge de travail toujours croissante depuis quelques années. Je travaille actuellement à l'embauche de cette personne, et j'espère la recruter d'ici les prochains mois.

Finalement, j'aimerais souligner le travail de mon adjointe, Lee Phypers, et la remercier pour son soutien indéfectible. Sa passion, son éthique de travail et son optimisme facilitent grandement mon travail.





BILAN DE L'ANNÉE

Loi sur l'accès à l'information et la protection de la vie privée

Au cours de l'exercice 2017-2018, le Commissariat à l'information et à la protection de la vie privée a ouvert un total de 53 dossiers en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*, ce qui représente une légère baisse comparativement aux 61 dossiers ouverts au cours de l'exercice précédent. Les dossiers ouverts se répartissent dans les catégories suivantes :

Demandes d'examen — Accès à l'information	15
Demandes d'examen — Protection de la vie privée	9
Consultations — Demandes de commentaires	7
Demandes d'examen — Évaluation des droits	5
Affaires diverses et administratives	5
Demande de correction de renseignements personnels	4
Notification d'atteinte à la protection des données	3
Demandes d'examen — Prorogation de délais	2
Demandes d'examen — Objection d'une tierce partie	1
Examen en cas d'atteinte à la protection des données (demandé par la commissaire)	1
Demande de ne pas tenir compte d'une demande d'accès à l'information (article 53)	1

Comme pour l'année dernière, ces données indiquent que les demandes d'examen relativement aux réponses aux demandes d'accès à l'information constituent l'essentiel du travail du commissariat. Les



violations de la confidentialité et les notifications d'atteinte à la protection des données arrivent en deuxième position. Cette année, notre bureau a également ouvert un dossier en vue d'engager la Ville de Yellowknife dans un dialogue sur les questions d'accès à l'information et de protection de la vie privée, à la lumière des violations graves qui ont fait la manchette dans l'affaire des courriels volés et de l'usage inapproprié des caméras de surveillance. La Ville n'a pas répondu à notre lettre, et aucune discussion n'a été entamée. Le dossier des affaires diverses et administratives comprend également un certain nombre de conférences et de demandes de renseignements des médias.

En plus des questions qui ont donné lieu à l'ouverture de dossiers, nous avons naturellement traité, sur une base quotidienne, nombre d'appels de personnes qui souhaitent obtenir des renseignements de base au sujet de la Loi; nous avons répondu à leurs demandes immédiatement, sans ouvrir de dossier.

Dix-huit rapports d'examen ont été rendus publics.

Loi sur les renseignements sur la santé

La *Loi sur les renseignements sur la santé* est entrée en vigueur le 1^{er} octobre 2015 et le nombre de dossiers a explosé cette année, passant de huit en 2016-2017 à 33 en 2017-2018. Cette évolution est positive, car elle indique que le public et les dépositaires de renseignements sur la santé accordent dorénavant une attention accrue à leurs responsabilités en ce qui concerne la collecte, l'utilisation et la divulgation de renseignements personnels sur la santé. Parmi ces dossiers, mentionnons:

- vingt-deux notifications d'atteinte à la protection des données reçues du ministère de la Santé et des Services sociaux et de l'Administration des services de santé et des services sociaux des Territoires du Nord-Ouest en vertu de l'article 87 de la Loi;



- six plaintes pour atteinte à la vie privée ont été reçues du public;
- deux plaintes étaient des évaluations des répercussions sur la vie privée reçues en vertu du paragraphe 89(2) de la Loi;
- une demande d'examen de la réponse reçue suivant une demande d'accès à des renseignements sur la santé, en vertu de l'article 141;
- un examen a été lancé à l'initiative de la commissaire à l'information et à la protection de la vie privée, en vertu du paragraphe 137(1);
- un dossier administratif.

Aucun rapport d'examen n'a été publié en vertu de la *Loi sur les renseignements sur la santé* au cours de l'exercice 2017-2018. Dans la plupart des cas de notifications de violation, les infractions étaient relativement mineures et corrigées presque immédiatement. Après discussion avec le dépositaire de renseignements sur la santé dans chaque cas, la commissaire à l'information et à la protection de la vie privée était satisfaite des mesures prises pour remédier à la cause de la violation et pour éviter d'autres infractions similaires. Elle n'a donc pas jugé nécessaire de procéder à un examen formel. Nombre de ces violations résultaient de l'envoi de télécopies mal adressées d'un bureau à un autre. La Commissaire à l'information et à la protection de la vie privée a donc pris des mesures pour mener une enquête systémique sur ce dossier.

Il ne semble pas y avoir eu de progrès en ce qui concerne l'obligation de s'assurer que le public puisse contrôler qui a accès à ses renseignements personnels sur la santé, comme l'exige l'article 22 de la Loi. Toutefois, des progrès ont été accomplis dans l'élaboration de normes, de politiques et de procédures applicables à l'échelle du système, comme l'exige l'article 8 de la Loi. Nous comprenons que le ministre a rendu publique une série de politiques en mai 2017. Le Commissariat à l'information et à la protection de la vie privée a reçu tardivement une copie de ces politiques au début de 2018, mais les documents ne semblent pas être disponibles en ligne pour que le public puisse les lire. Il est important que le public soit en mesure de savoir comment la loi est mise en œuvre au moyen de directives.



Comme on pouvait s’y attendre compte tenu de la portée de la Loi et de l’importance du système de santé ainsi que de la nature et de l’étendue des renseignements de santé personnels collectés, utilisés et divulgués, il restera des lacunes à combler à mesure que la Loi continue d’être mise en œuvre.





TENDANCES ET ENJEUX – POUR ALLER DE L'AVANT

Un examen approfondi

J'ai très hâte de voir les prochaines étapes dans la mise à jour de la législation sur l'accès à l'information et la protection de la vie privée, une fois que sera terminé l'examen approfondi entrepris il y a maintenant près de deux ans. Le monde a beaucoup changé depuis l'entrée en vigueur de la *Loi* actuelle, il y a plus de vingt ans. La nature des archives gouvernementales et la façon dont elles sont créées, gérées et entreposées ne sont plus du tout les mêmes. Les documents papier ne sont plus que des exceptions relativement rares. Presque tout est numérique. Les employés communiquent souvent par courriel, par texto et par d'autres moyens électroniques, parfois en dehors du système du GTNO, et chaque employé du gouvernement est responsable de la gestion de ses propres archives. Le modèle de l'ombudsman ne fonctionne plus aussi bien qu'il y a vingt ans. Le Commissariat à l'information et à la protection de la vie privée a besoin de plus de pouvoir pour veiller au respect des exigences, et il doit y avoir des conséquences qui vont au-delà d'une simple mention dans un rapport annuel lorsqu'un organisme public refuse de suivre les recommandations du Commissariat. J'appuie de tout cœur l'établissement d'un système semblable à celui de Terre-Neuve-et-Labrador : le Commissariat y formule bien des recommandations (plutôt que des ordonnances), mais si un organisme public souhaite les ignorer ou les rejeter, il doit en faire la demande à un tribunal pour y être autorisé. Des dispositions doivent également être mises en place pour qu'il y ait moyen de s'assurer qu'une fois une recommandation acceptée, l'organisme y donne effectivement suite. On devrait, par ailleurs, être clairement tenu de consigner les échanges et les actions prises par l'organisme public ou en son nom, et l'information devrait être accessible sur demande, qu'elle ait



été créée ou non à l'aide du matériel du GTNO. Bref, cette loi importante a cruellement besoin d'une mise à jour, et j'insiste pour qu'on y voie une priorité.

L'examen des politiques

En plus de réviser la *Loi*, il faut procéder à un examen complet des politiques et procédures relatives à l'utilisation des documents électroniques. Il ne semble pas y avoir de politique qui traite, par exemple, de l'utilisation des appareils personnels, des textos ou des comptes de courriel personnels dans le cadre des activités du GTNO. Quand est-il approprié qu'un employé d'un organisme gouvernemental utilise sa propre adresse électronique ou son appareil personnel pour communiquer dans le cadre des affaires gouvernementales? Les pratiques exemplaires suggèrent que l'utilisation d'adresses et d'appareils personnels soit interdite, sauf en cas d'urgence. Le cas échéant, il devrait y avoir des directives limpides en ce qui concerne la gestion de telles communications, et des conséquences claires en cas de non-respect de la politique établie. Il devrait aussi y avoir des politiques claires à l'égard de l'utilisation des clés USB et autres dispositifs de stockage portatifs, ainsi que du chiffrement de la correspondance par courriel dans toutes les circonstances où les messages contiennent des renseignements personnels; il faudrait par ailleurs restreindre les types de données téléchargeables sur les ordinateurs portables, tablettes et autres appareils pouvant être emportés à l'extérieur du bureau. Ce ne sont là que quelques exemples des politiques et procédures à mettre en place pour tenir compte de la dépendance actuelle aux communications numériques. Je recommande fortement qu'un examen approfondi de toutes les politiques pertinentes soit effectué afin que les politiques archaïques soient mises à jour et que de nouvelles soient élaborées pour s'attaquer à ces enjeux.



L'utilisation des télécopieurs dans le secteur de la santé

Parmi les questions qui ont été soulevées à maintes reprises cette année, je note celle des télécopieurs, que les professionnels de la santé utilisent encore aujourd'hui pour communiquer avec d'autres professionnels, avec les patients et avec des tierces parties. Pas moins de 9 des 22 avis d'atteinte à la vie privée reçus de la part de dépositaires de renseignements médicaux impliquaient des informations qui ont été transmises par fax et qui se sont retrouvées dans les mauvaises mains. Ce problème n'est pas l'apanage des Territoires du Nord-Ouest. C'est l'ensemble du secteur médical canadien qui semble résister aux nouvelles technologies de communication, pourtant plus sûres. Les renseignements médicaux personnels sont parmi les informations les plus confidentielles qui soient, et ils devraient être traités en conséquence. L'utilisation des courriels et du chiffrement ne requiert pas d'efforts supplémentaires ou de connaissances particulières; il est donc temps que le secteur prenne cette mesure simple pour diminuer le nombre d'atteintes à la vie privée qui résultent de télécopies mal acheminées. Certes, les courriels peuvent aussi s'égarer, mais de simples programmes de cryptage permettent d'en chiffrer le contenu afin qu'ils ne puissent être consultés que par le destinataire voulu. J'invite le ministère de la Santé et des Services sociaux à prendre les devants dans cette transition et à définir des étapes appropriées pour la création de politiques et procédures afin d'encourager le secteur à mettre à jour ses stratégies de communication en réduisant le recours aux télécopieurs.

L'éducation

Comme je l'ai mentionné dans mes remarques préliminaires, l'éducation est fondamentale si nous voulons que nos enfants apprennent à travailler dans un monde numérique tout en étant en mesure de protéger leur vie privée. Cette génération « vivra » en ligne, et il est important qu'elle ait très tôt les outils nécessaires pour le faire de façon sécuritaire. Autrement dit : pour agir avec discernement, les jeunes doivent comprendre la façon dont leurs renseignements personnels sont recueillis et utilisés. Nous sommes en retard pour ce qui est d'assurer cette éducation essentielle. Néanmoins,



beaucoup de travail a été fait pour élaborer du matériel pédagogique et des plans de cours appropriés selon l'âge. Un des projets que mes homologues de partout au pays et moi-même avons entrepris consiste à créer des modèles de plans de cours. Nous en avons récemment publié trois, et vous pouvez les trouver sur mon site Web, dans la section « Ressources ». Le ministère de l'Éducation, de la Culture et de la Formation doit redoubler d'efforts pour que les enfants comprennent l'importance du respect de la vie privée et pour qu'ils apprennent comment la protéger en ligne et comment faire face à la cyberintimidation. Cette éducation doit commencer dès la maternelle et se poursuivre jusqu'en 12^e année. J'encourage le gouvernement des Territoires du Nord-Ouest à s'assurer que ces éléments soient intégrés au programme de tous les niveaux scolaires, et ce, dès que possible.



Bien sûr, j'accorde de l'importance à ma vie privée c'est pourquoi je ne partage mes informations personnelles qu'avec 700 de mes amis les plus proches.



**COMMISSARIAT À
L'INFORMATION ET
À LA PROTECTION
DE LA VIE PRIVÉE**

TERRITOIRES DU NORD-OUEST