



**INFORMATION AND PRIVACY COMMISSIONER
OF THE NORTHWEST TERRITORIES
2013/2014 ANNUAL REPORT**



**NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER**

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

August 25, 2014

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

Attention: Tim Mercer
Clerk of the Legislative Assembly

Dear Sir:

I have the honour to submit my annual report to the Legislative Assembly of the Northwest Territories for the period from April 1st, 2013 to March 31st, 2014.

Yours very truly

Elaine Keenan Bengts
Information and Privacy Commissioner
Northwest Territories

/kb

INDEX

COMMISSIONER'S MESSAGE	7
THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER	10
THE <i>ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT</i>	11
ACCESS TO INFORMATION	12
PROTECTION OF PRIVACY	13
THE PROCESS	13
MAKING AN ACCESS TO INFORMATION REQUEST	15
THE YEAR IN REVIEW	16
REVIEW RECOMMENDATIONS	18
REVIEW RECOMMENDATION 13-117	18
REVIEW RECOMMENDATION 13-118	21
REVIEW RECOMMENDATION 13-119	23
REVIEW RECOMMENDATION 13-120	24
REVIEW RECOMMENDATION 13-121	26
REVIEW RECOMMENDATION 13-122	27
REVIEW RECOMMENDATION 14-123	29
REVIEW RECOMMENDATION 14-124	31
REVIEW RECOMMENDATION 14-125	33
LOOKING AHEAD	35

ANNUAL REPORT 2013/2014

COMMISSIONER'S MESSAGE



This Annual Report marks the 17th year of the coming into force of the *Access to Information and Protection of Privacy Act* in the Northwest Territories. Much has changed in those seventeen years. Who would have thought, back in 1996, that people like Julian Assange and Edward Snowden would bring such focus to the public's right to access government information? Who would have considered the possibility that simply using your credit card could open the door to someone taking over your identity? Certainly in 1996 you would not have seen daily news reports about "hacking" and "massive data breaches". Information and privacy issues simply were not part of the day to day lexicon or a major part of the news cycle. Today, they are. Canada, of course, has had its own set of headlines. This spring, for example, Canada Revenue Agency had to shut down its servers to deal with a virus that made the system vulnerable. Some provinces have been dealing with issues such as employees deleting government records and using private email to conduct government business so as to avoid access to information requests. Access and privacy are no longer esoteric concepts. Canadians are beginning to discuss these issues around the water cooler every day. Citizens are increasingly concerned about the erosion of their individual privacy and are talking about privacy as a fundamental value. More and more often government is being asked to account for its actions through access to information requests. And more people are pointing to government and calling them out for failing to adequately protect personal privacy.

All of this translates into more work for my office. As noted in my last Annual Report, the time has come for a more dedicated approach to the work of the Information and Privacy Commissioner. For the last 17 years, the work of the office has been done on a very part time basis, along with my work as the Information and Privacy Commissioner of Nunavut and my work as a lawyer in a busy Yellowknife practice. Over the last few years, it has become increasingly difficult to keep up with the workload. I am also feeling more and more that the current structure of the office as a part time endeavor does not always engender the respect that should be given to the office or the role that it plays in helping to ensure openness and accountability in government. There is no time for pro-active work with government departments and little time to address pending legislation or keep up with new programs that may have an impact on the privacy rights of individuals. Perhaps more importantly, with the coming into effect of the *Health Privacy Act* in the spring or summer of 2015, I anticipate that the workload of the office will increase exponentially. I have, therefore, made a proposal to the Legislative Assembly to address some of these concerns and, in particular to establish a full time office with a full time administrative assistant/intake officer, and to plan for the inclusion of a full time investigator in fiscal 2016/2017. As of December 31st of this year, I will be discontinuing my legal practice in order to focus more of my time and attention on my work as the Information and Privacy Commissioner. In this way, I will be able to dedicate the extra time that will be necessary to address the work which will accompany the coming into force of the *Health Information Act* and to meet all of the other responsibilities of the Information and Privacy Commissioner under the two pieces of legislation.

In October 2013, Information and Privacy Commissioners from across Canada met in Vancouver and proposed comprehensive reforms to modernize access to information and privacy laws, including mandatory breach notification, a legislated duty to document, and stronger enforcement powers including penalties for non-compliance. That resolution was

appended to my last Annual Report. I understand that the Department of Justice is planning an overall review of the *Access to Information and Protection of Privacy Act*. Clearly, this is a timely project and I would encourage the Department to consider the suggestions made in this resolution. I also look forward to working with the Department on this review.

In closing, I would like to acknowledge the support and encouragement I always receive from the Standing Committee on Government Operations, before whom I appear every year to discuss my annual report. As well, I would like to acknowledge all of the ATIPP Coordinators in the various public bodies of the Northwest Territories who all work hard to ensure that the spirit and intention of the Access to Information and Protection of Privacy Act is respected.



THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

Established in 1997, the Office of the Information and Privacy Commissioner (OIPC) provides independent oversight and enforcement of the Northwest Territories' access and privacy law, the *Access to Information and Protection of Privacy Act*. This Act applies to 41 public bodies, including ministries, crown corporations, commissions and more.

The Information and Privacy Commissioner is appointed by the Commissioner of the Northwest Territories on the recommendation of the Legislative Assembly and holds office for a five year term. As an independent officer, the IPC can be removed from office only "for cause or incapacity" which allows her to comment freely and directly.

The Information and Privacy Commissioner (IPC) has the power to:

- Investigate, mediate and resolve matters concerning access to information disputes, and to make public recommendations to public bodies with respect to these matters;
- Investigate and resolve privacy complaints;
- Comment on the access and privacy implications of proposed legislative schemes or government programs;
- Engage in or commission research into matters affecting the carrying out of the purposes of the Act; and
- Educate the public about their access and privacy rights.

THE *ACCESS TO INFORMATION AND PROTECTION OF PRIVACY ACT*

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

1. public records must be accessible to the public; and
2. “personal information” must be protected by public bodies.

The Act outlines the rules by which the public can obtain access to public records and establishes rules about the collection, use and disclosure of information about individuals by public bodies in the Northwest Territories.

The ATIPP Act applies to all “public bodies”. This includes all Government of the Northwest Territories departments, crown corporations, and some boards, commissions and agencies.

The Supreme Court of Canada has declared that laws like the ATIPP Act are special kinds of laws that define fundamental democratic rights of citizens. They are “quasi-constitutional” laws that generally are paramount to other laws.

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

— Louis D. Brandeis

ACCESS TO INFORMATION

The *Access to Information and Protection of Privacy Act* gives the public the right to obtain access to most records in the custody or control of public bodies. While access is always the rule, there are a number of specific and limited exceptions to this right. Most of the exceptions function to protect individual privacy rights, to allow elected representatives to research and develop policy and the government to run the “business” of government. Because the Supreme Court of Canada has ruled that access to information legislation is “quasi-constitutional” in nature, all exceptions to disclosure are to be limited and narrowly defined.

To obtain a record from a public body, a request must be made in writing and delivered to the public body from whom the information is sought. When an applicant is not certain where the request should be directed, it can be submitted to the public body who he believes should have the information. If that public body does not have the records required, it has the obligation to ensure that it is forwarded to the appropriate public body.

When a request for information is submitted to a public body, that public body has a duty to identify all of the records which are responsive to the request. Once the responsive documents are identified, they are reviewed to determine if there are any records or parts of records which are exempt from disclosure under the Act before they are given to the Applicant. In most cases, public bodies must respond to access requests within thirty (30) days.

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

PROTECTION OF PRIVACY

Part II of the *Access to Information and Protection of Privacy Act* provides rules for when and how public bodies can collect personal information, what they can use such information for once it has been collected and in what circumstances that information can be disclosed to another public body or to a third party. It also provides a mechanism which allows individuals the right to see and make corrections to information held by public bodies about themselves.

This part of the Act also requires public bodies to maintain adequate security measures to ensure that the personal information which they collect cannot be accessed by unauthorized individuals.

When an individual has privacy concerns, those concerns can be referred to the Information and Privacy Commissioner for review. The IPC is authorized to investigate the complaint and to make recommendations to the public body.

THE PROCESS

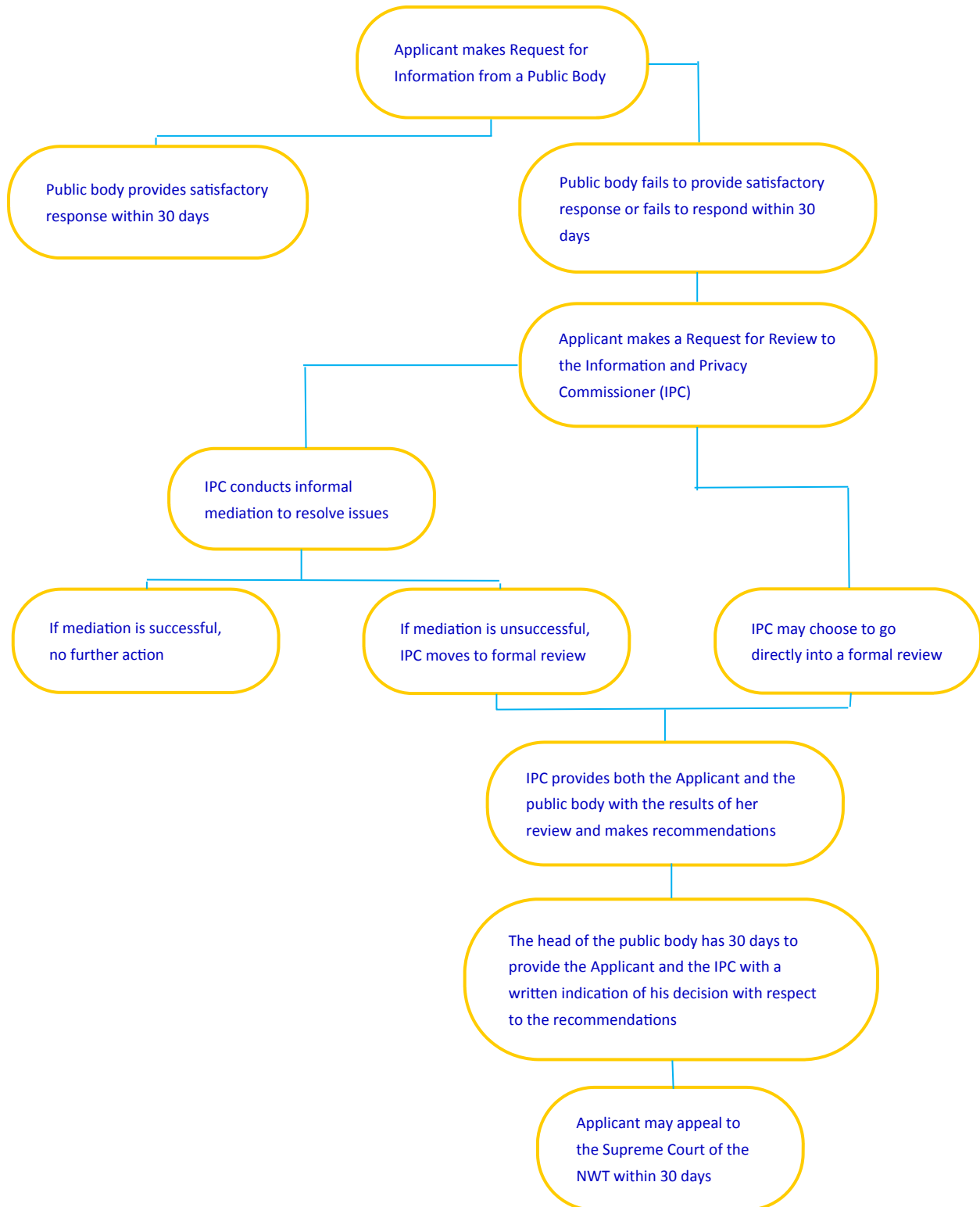
When the Information and Privacy Commissioner receives a Request for Review with respect to an access to information matter, she corresponds with both the Applicant and the public body involved to determine what records are involved and obtain an explanation from the public body as to the reasons for their decisions. The Applicant is also given the opportunity to provide input, as well as any third parties whose information is the subject of the request. The IPC has the benefit of being able to review copies of all of the responsive records in their original format and with any edits which have been applied by the public body in responding to the request. The IPC considers the input of all interested parties, the records themselves and

the provisions of the ATIPP Act and produces a report containing conclusions and recommendations. The IPC does not have any power to compel public bodies to either disclose or protect information from disclosure but she is required to make recommendations. The head of a public body must, however, respond to the recommendations made, indicating that the recommendations are accepted or rejected, or that other steps will be taken to address the matter. This response must be provided within 30 days of the IPC's recommendations and the Applicant has the right to appeal to the Supreme Court of the Northwest Territories if they are unhappy with the public body's decision.

The process is very similar for a complaint about the alleged improper collection, use or disclosure of personal information. The IPC will communicate with both the public body and the complainant, and with any other person who might have some information about the alleged breach to determine whether or not a breach of privacy occurred. Whether or not there has actually been an improper collection, use or disclosure of personal information, the IPC will prepare a report which will almost always contain comments and recommendations to improve policies and procedures so as to reduce the possibility of future breaches. The recommendations made by the IPC with respect to privacy issues are provided to the head of the public body and, once again, the public body will then have to decide whether or not to accept the IPC's recommendations. In the case of privacy complaints, the public body has 90 days to respond. There is no right to appeal the public body's decision respecting a privacy breach complaint.

A popular government, without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy; or, perhaps, both.
—Pres. James Madison, August 4, 1822

MAKING AN ACCESS TO INFORMATION REQUEST



THE YEAR IN REVIEW

In the 2013/2014 fiscal year, my office opened a total of 30 files, which is almost double the number of files opened in the previous fiscal year. These files included:

Requests for Review - Access to Information	12
Requests for Review - Privacy Issues	9
Privacy Inquiries (Private sector Breaches)	4
Pro-Active Breach Notification	2
Request for Review - Fee Assessment	1
Requests for Comment	1
Administrative	1

I was pleased to see two breach notifications during the fiscal year in which a public body discovered a potential breach of privacy and reported it to my office pro-actively. One of these turned into a formal complaint from a third party. The other was simply monitored by my office as the public body addressed the issue. Somewhat concerning is that in at least seven of the access matters, one of the issues was the public body's delay in responding to the Request for Information.

Several of the files opened this year involved complaints about privacy breaches in the private sector. Two of these were not for profit organizations who were clearly uneducated with respect to their obligations under the federal *Personal Information and Protection of Electronic Documents Act* (PIPEDA) to protect the information they gathered about individuals. I worked with these organizations and provided suggestions with respect to the issues raised. I also dealt with seven public bodies. The public bodies involved most often were the Department of Human Resources with seven, the Department of Transportation with six and the Department of Justice with four.

My office issued nine Review Recommendations during the fiscal year.



REVIEW RECOMMENDATIONS

REVIEW RECOMMENDATION 13-117

Category of Review:	Privacy Complaint
Public Body Involved:	Yellowknife Health and Social Services Authority
Sections of the Act Applied:	Section 43
Outcome:	Recommendations Accepted in Part

The Complainant in this case was upset about the way in which Yellowknife Health and Social Services Authority (YHSSA) had handled his information. Because of previous bad experiences, he had written to YHSSA directing that none of his personal health information was to be shared with anyone, whether within or outside of YHSSA, without his express written consent and signature. In response, the Complainant was advised that “theoretically, we require your consent only with respect to dissemination of information beyond the boundaries of YHSSA”. This said, YHSSA, also acknowledged the restriction on the sharing of his information. At some point, the Complainant was referred to a psychiatrist for a consultation. The Complainant refused to allow his medical records to be provided to the psychiatrist before the appointment because of his lack of trust in his primary care physician. He was initially refused an appointment as a result, but was eventually given that appointment. When he arrived for that appointment, he was refused access to the psychiatrist unless he signed a consent allowing the psychiatrist’s report to be shared with his primary care physician. He refused and, as a result, the consultation did not happen.

YHSSA advised that they work under a primary care model which places the primary care physician (PCP) at the hub of patient care. No referrals can be made to a specialist except by the PCP. Once the specialist has completed the consultation, the matter is referred back to the PCP who is then expected to implement the plan of care. Unless the PCP receives the consultation report, no plan of care can be implemented. YHSSA emphasized the ethical and professional responsibilities of physicians and specialists to each other.

The Information and Privacy Commissioner (IPC) found that, notwithstanding YHSSA's care model, the focus must remain on the patient to whom the information belongs. The ethical and professional responsibilities of physicians and specialists to the patient outweigh the ethical and professional responsibilities that exist between medical health providers. In situations in which the patient gives clear and unequivocal instructions that his personal health information is not to be shared without his consent, those wishes must be respected and in a way that does not prevent him from obtaining the medical care he needs. No person should be denied medical services because they want to maintain control over their own personal health information.

Three recommendations were made surrounding this issue:

- a) That an educational brochure about how personal health information is collected, used and disclosed by YHSSA be prepared and that this brochure be provided to all patients. The brochure should include the name and contact information for someone within the organization who can answer any questions;
- b) That YHSSA create policies and procedures to deal with situations in which a patient refuses to consent to the internal or external sharing of personal health information. The policy should clearly include a statement that no patient can be

denied services solely because he/she refuses to allow the sharing of his/her personal health information; and

- c) That YHSSA in this case find a way to provide the Complainant with the psychiatric health services he needs while still respecting his right to control access to his health records.

While the public body found the recommendations included some “reasonable and valuable suggestions”, the recommendations were only partially accepted. In particular, YHSSA felt that their standard consent form was sufficient to educate the public concerning how their personal health information would be used and disclosed and declined to produce a brochure to explain this. YHSSA did indicate that it was in the process of implementing a new privacy framework and relevant policies to deal with this situation were planned within that framework. They agreed to continue to work with the patient “in an attempt to find a mutually agreeable arrangement that protected the client’s rights, the practitioner’s obligations and permitted the functioning of the health authority within the health care system”. The public body, however, disagreed with the IPC’s view of how personal health information can be used once collected. They insist on continuing to rely on an undefined concept of “circle of care” which, as experience has shown, has very different meanings to different people. All of these issues will have to be dealt with in a far more structured and focused way upon the coming into force of the new *Health Information Act*.

Where a patient expresses a concern about the sharing of his/her personal information within the Authority, YHSSA needs to find a way to respect those concerns without denying the patient the medical services he needs.

— Elaine Keenan Bengts—Review Recommendation 13-117

REVIEW RECOMMENDATION 13-118

Category of Review:	Access to Information
Department Involved:	Department of Human Resources
Sections of the Act Applied:	Sections 8, 11, 14(1)(a), 14(1)(b), 23(2)(d) and 23(2)(i)
Outcome:	Recommendations Accepted

In this case, the Applicant sought records associated with a meeting that was held within his workplace at which the subject of discussion was himself. He was advised about the meeting after the fact and was, as a result of the information gathered during the meeting, required to obtain a medical certificate. He believed that erroneous information was imparted during this meeting and that the information was put on his personnel file. This request also contained a request that the public body's delay in responding to the application be addressed. He notes that the request was made on November 27th, that on December 18th a letter was written to him extending the response time to February 25th, and that in a subsequent discussion with the department prior to February 25th he was advised that the time was going to be further extended. It was March 15th before the response was finally received. Many of the records received contained blank spots and edits. The Department relied on sections 14 or 23 for the redactions.

On the delay issue, the IPC found that the public body failed to comply with the terms of the *Access to Information and Protection of Privacy Act* either in terms of appropriate process or in terms of the length of the delay. The Act provides only that a public body may extend the time for responding for "a reasonable" period of time. The reason for the extension was noted to be "administrative workload" which is not a reason for extension under the Act. Nor did the public

body provide any good reason for a two month extension past the original response date. There were only 61 records, approximately 150 pages. This is not a large number of records and the length of the extension was not reasonable in the circumstances. The IPC recommended that the department review its processes and procedures with respect to handling ATIPP requests so as to ensure that responses can be provided in a timely manner and in accordance with the Act.

With respect to the response provided, the IPC did a line by line review and recommended the disclosure of a number of the redacted records. She noted that disclosure is always the rule and where records or parts of records are withheld, those redacted portions must fall squarely within the exemption. Furthermore, where the exemption is a discretionary one, as provided for in section 14, the rule is always disclosure and if the discretion to refuse disclosure is used, it must be actively exercised, with reasons provided. To constitute “advice, proposals, recommendations, analyses or policy options” pursuant to section 14 such as to provide a discretionary exemption to disclosure, the information:

- a) must be sought or expected or be part of the responsibility of a person by virtue of that person’s position
- b) must be directed toward taking an action; and
- c) must be made to someone who can take or implement the action

The 30 day response period is in the Act for a reason. It’s not a goal, or a suggestion. It is a requirement.

— Elaine Keenan Bengts, Review Recommendation 13-118

REVIEW RECOMMENDATION 13-119

Category of Review:	Access to Information
Department Involved:	Department of Transportation
Sections of the Act Applied:	Sections 14(1)(b)(i) , 14(1)(b)(ii), 14(1)(d), 23(2)(a), 23(2)(d) and 23(2)(i)
Outcome:	Review Recommendations Accepted

The Applicant requested his own personal information arising out of a workplace dispute. The Applicant was a supervisor in a work place and several of those who he was supposed to be supervising had concerns about his activities. The public body identified a number of responsive records, most of which were provided to the Applicant without any edits. There were, however, also some records where were withheld either in full or in part. There were also concerns about the length of time it took to respond to the Applicant's request, originally made on November 28th, 2013. The time for responding was extended several times before he finally received his response on March 7th, 2014.

With respect to the extensions of time for responding to the Applicant, the IPC found that there were irregularities in the process and that the public body did not follow the requirements of the ATIPP Act. Furthermore, she found that the length of the extension was not "reasonable" in the circumstances.

With respect to the response provided, the IPC did a line by line review and recommended the disclosure of a number of the redacted records. As in Review Recommendation 13-118, she confirmed that disclosure is always the rule and exemptions should be narrowly interpreted and applied. When an applicable exemption is a discretionary one, the public body must actively exercise that discretion for every exclusion.

REVIEW RECOMMENDATION 13-120

Category of Review:	Privacy Complaint - Improper Collection of Personal Information
Department Involved:	Department of Education, Culture and Employment
Sections of the Act Applied:	Sections 40(c) (i)
Outcome:	Recommendations Accepted

An individual raised concerns about the collection of personal information by the Department of Education, Culture and Employment (ECE) from students who had received remissable loans through Student Financial Assistance (SFA) and who were seeking partial forgiveness of their loans for time spent working in the Northwest Territories upon completion of their education. In order to qualify, students had to prove residence in the Northwest Territories by providing three different pieces of evidence from three different months during each six month period of time.

There were eight kinds of records deemed acceptable:

- a) a lease agreement or mortgage for a home in the Northwest Territories;
- b) a property tax assessment for a home in the Northwest Territories;
- c) utility bills in the student's name ;
- d) bank statements (including credit card statements);
- e) proof that the student filed an NWT tax return with Canada Revenue Agency;
- f) a signed letter on letter head from an employer verifying the start and end dates of employment or pay stubs;
- g) employment insurance statements;
- h) Income Assistance financial case reports.

This Complainant found it impossible to meet the requirements, even though he had a full time job in Yellowknife. He lived with his parents and did not, therefore, have any of the first three options available to him. As he was working full time, the last two options were likewise not available. The tax return was filed only once a year and could only be used once. His joint bank account records were deemed unacceptable. ECE did advise the Complainant that he could provide them with a credit card bill if the details of the purchases indicated that significant purchases were being made in the Northwest Territories. The Complainant objected to this for privacy reasons and suggested that pay slips from an NWT employer should be sufficient.

The IPC commented that each of these pieces of documentation had differing levels of personal information on them, most of which had nothing whatsoever to do with proof of residency. For example, while a pay stub might show an NWT employer, it would also have hourly rate of pay, year to date income information, and the nature of the employee's contract among other things. Credit card and bank statements had even more information about spending habits and life style.

The IPC noted that the only information that the public body should be collecting is that information which could help to confirm that the individual was, in fact, resident in the Northwest Territories during the relevant time period. Furthermore, the least amount of information necessary to satisfy this question should be required.

The IPC made four recommendations to reduce the amount of personal information being collected.

REVIEW RECOMMENDATION 13-121

Category of Review:	Privacy Complaint
Department Involved:	Department of Justice
Sections of the Act Applied:	Sections 40, 43, and 48
Outcome:	No Recommendations Made

The Complainant in this case objected to the fact that the Sheriff's Office obtained and used his personal information from the Department of Health and Social Services and/or other government agencies in the Northwest Territories for the purpose of identifying and locating him to summons him for jury duty.

The Department of Justice pointed to Sections 8(2) and (3) of the *Jury Act* which provide that, notwithstanding the *Access to Information and Protection of Privacy Act*, the Director of Medical Insurance must, on request, provide the Sheriff with the names and addresses of those insured persons who have attained the age of 18 years to enable compilation of the jury list. This information is shared pursuant to an information sharing agreement between the Department of Health and Social Services and the Department of Justice. This agreement prohibits the subsequent use of the information, provides for a retention and disposal schedule, and sets standards for the security and confidentiality of the information.

In light of the legislative authority provided to the two departments in the *Jury Act*, the IPC found that the exchange of information for the purpose of creating the jury list was authorized. She made no recommendations.

REVIEW RECOMMENDATION 13-122

Category of Review: Privacy Concern - Collection of Personal Information

Department Involved: Department of Health and Social Services

Sections of the Act Applied: Section 40(1) and 40(2)

Outcome: Recommendations Accepted

This complaint came from an individual who felt that the Department of Health and Social Services was requiring personal information from him that they did not need. The Complainant was applying for a renewal of this NWT Health Care Coverage. The Department sent him a form to complete which included a question about whether he was employed, if so with whom, the employer's telephone number, whether he was eligible for benefits under an employer's or another's 3rd party insurance plan and if so the name of the plan and the insurance details. The information was requested for both himself and his spouse. The Complainant felt that the Department did not need to know any of this information to assess his eligibility for NWT Health Care coverage.

The Department explained that these questions were contained in Part B of the form, which is only required to be filled out if an applicant is enrolled in one of several programs that provide additional benefits (such as prescription drugs, medical equipment and supplies and dental services). They indicated that this information was required because outside insurance may affect the level of coverage received through the health care program.

While the IPC accepted that the Department had a legitimate reason for needing to know whether or not the applicant was covered by third party insurance, she felt that they were asking for too much unnecessary information. The ATIPP Act allows public bodies only to collect that information they need for the provision of a service. The department did not need to know whether or not the applicant or his spouse were employed. They only needed to know whether either of them had third party insurance.

The IPC also pointed out that when information is collected, the public body is required to inform the individual the purpose for which the information is being collected, the specific legal authority for the collection and the name and contact information for an employee of the public body who can answer questions about the collection. This was not done in this case.

The IPC recommended a review of the form in question to determine if it is truly necessary to collect employment information. She also recommended a fuller review of all form letters to ensure they properly describe the reason the information is being collected.

A photograph of a form with a pen pointing to it. The form has several fields with labels and checkboxes. The labels are: Mr Ms Personal Business Surname*: First name*: Company: Department: Street*: Postcode*: Town*: Country*: Telephone number: The pen is a silver and black ballpoint pen, pointing towards the 'Surname*' field.

REVIEW RECOMMENDATION 14-123

Category of Review: Privacy Complaint - Unauthorized Use/Disclosure

Department Involved: Department of Transportation

Sections of the Act Applied: Sections 47.1

Outcome: Recommendations Accepted

The Complainant was a truck driver working for a private sector company. He was pulled over by a Highway Transport Officer (HTO) working for the Department of Transportation and given a warning for speeding. He advises that when he got to work the next day, he was met with his co-workers teasing him about the warning. One of his co-workers was a room mate of the HTO and the Complainant alleges that the HTO improperly disclosed the information to the co-worker.

The Complainant made a complaint directly to the Department of Transportation. The person he met with about the matter recorded the conversation on a cell phone which caused the Complainant further concerns about how this information was going to be stored, used and the possibility of further disclosure.

The Department's investigation could not confirm the Complainant's statement and could find no one, other than the Complainant, who would admit that he had heard the co-worker teasing the Complainant and, of course, the roommate denied it. With respect to the recording, the Department says that the investigator ensured that his mobile device was password protected and remained in his possession until the recording was stored on the DOT network and once stored, the recording was deleted from the mobile device.

The IPC found that section 47.1 of the ATIPP Act sets out clearly that employees of public bodies are prohibited from disclosing any personal information received by the employee in the performance of services for the public body. While the public body had concluded that there was “no evidence” that the HTO had breached the Complainant’s privacy, the IPC did not agree. There was some evidence, although perhaps not enough to come to a definitive conclusion as to what had happened. The IPC found that while there should be an attempt to determine whether or not a breach actually occurred in a situation such as this, the issue is less about whether or not the allegation can be proved, and more about whether it can be disproved. Public bodies are responsible for ensuring that personal information gathered or obtained during the course of their employment is protected from unauthorized use and/or disclosure. Unless the allegation can be disproved, the department needs to look at what happened with an objective eye to see if there can be more done to protect individual privacy. The IPC also acknowledged that every GNWT employee is required to sign an Oath of Office and Secrecy. She noted, however, that this was far from a guarantee that the employee will comply with the oath and it should not be relied on as proof that no disclosure had occurred.

With respect to the recording, the IPC expressed concern about the use of a mobile device for recording an interview.

The IPC made four recommendations to help improve privacy practices within the Department of Transportation, including delivering additional ATIPP training to HTOs and reviewing with staff the existing policies and procedures with respect to mobile devices.

REVIEW RECOMMENDATION 14-124

Category of Review:	Breach of Privacy - Collection of Information
Department Involved:	Department of Human Resources
Sections of the Act Applied:	Sections 40, 43 and 48
Outcome:	Recommendations Accepted

The Complainant in this case applied for a job with the GNWT. He was advised that he did not meet the screening criteria and would not, therefore, be receiving an offer. The Applicant appealed the decision. On appeal, it was recommended that the competition be re-started from the screening stage and that the Complainant be granted an interview. During the interview, the candidates were asked to provide their references. Questions were raised by the selection committee with respect to a particular hiring policy, which was referred to the Corporate Services Unit. While waiting for a response, the selection committee completed the reference checks for both candidates to save time. The offer was made to the other candidate. The Complainant was upset that his references were checked even though he was not being offered the position. Normal practice is to check references only of the person to whom the offer is going to be made.

The first question was whether the public body used the Complainant's personal information in contravention of the Act and secondly whether, in interviewing the references, the public body improperly collected the Complainant's personal information.

In this case, the Department used and disclosed the Complainant's personal information when they contacted the references. While he consented, by implication, to the use and the disclosure, that consent was given on the understanding that the references would only be checked in the event that he was being offered the job. The use and disclosure was not, therefore, in accordance with the Act. Similarly, the collection of the Complainant's personal information from the references was non-consensual in the circumstances and therefore not in accordance with the Act.

The IPC made three recommendations:

- a) that the Complainant be provided with an apology;
- b) that any information collected from the references be destroyed; and
- c) that the department review and clarify its written policies with respect to the hiring process and, in particular, the checking of references



REVIEW RECOMMENDATION 14-125

Category of Review:	Privacy Complaint
Department Involved:	Department of Justice
Sections of the Act Applied:	Section 42
Outcome:	Recommendations Accepted in Part

The Complainant received a letter from the Department of Justice, his former employer, indicating that the department had discovered that personal income information about him had been inadvertently stored in a GNWT shared folder on the government network and, as a result, there was potential that the information could have been accessed by unauthorized individuals. The information was in a folder within a folder with an innocuous name which would not invite the curious and there was no evidence that anyone, other than authorized employees, had accessed the file but there were no audit capabilities to test that. All those working on the file were of the understanding that there were appropriate security mechanisms on the file to prevent unauthorized access, but they were wrong.

The IPC commented that there was no obligation under the *Access to Information and Protection of Privacy Act* for the public body to notify the Complainant about the breach and their decision to be pro-active in this regard was laudable. The public body recognized the potential seriousness of the situation and chose to address it directly and openly.

By the time the IPC had completed her review, the department had already taken a number of steps to improve their policies and procedures so as to avoid the possibility of such errors in the future. She did, however, make further recommendations:

- a) that consideration be given to adding audit capabilities to all of the GNWT's network systems so that when, as here, human error occurs, public bodies can audit the system to determine whether there had been any unauthorized access. The public body did not accept this recommendation. Instead, they indicated that they believed the issue was better addressed with the implementation of written procedures and/or guidelines that address the required security for personal information prior to any personal information being placed within a shared drive;
- b) that the Technology Service Centre conduct a systemic review of its network system and each department's "file shares" together with senior staff within each department to ensure that all drives have the necessary security. Both the Department of Justice and the Department of Finance agreed to review their file share folders annually. They pointed out, however, that this was not the responsibility of the Technology Service Centre, but of each department; and
- c) that those responsible for information management review all policies and procedures with respect to the management of information and, in particular, retention and destruction schedules. This recommendation was accepted.



LOOKING AHEAD

Every year I make recommendations in this section of my Annual Report to address issues that have come up from time to time with a view to improving how the Act meets its goals.

With the *Health Information Act* having been passed this year, the focus for the next year will be on preparation for implementation of the legislation. It is a complex piece of legislation, difficult to interpret and to understand and there will be a steep learning curve for everyone involved — in the health sector, in my office and with the public. As I noted in last year's Annual Report, this legislation will require a significant investment in education — the education of those working in the health sector as well as the education of the public. New policies and procedures will have to be developed well in advance of implementation so that health information custodians don't find themselves scrambling to figure things out at the last minute. Much work will also have to be done to ensure that the public has a good working understanding of how their personal health information will be collected, used and disclosed under the Act, what their choices are and the implication of those choices. The new legislation is only the first step. There is much more work to be done. I look forward to seeing this legislation implemented, however, as it is something that I have been advocating for for years.

One of the things that has become increasingly frustrating for me in the last few years is that public bodies rarely seem to consider the impact of new initiatives on either the right to access or the privacy of the individual. Nor do I often receive any request for comments when new programs, initiatives or legislation are being considered that might have an impact in my areas of expertise. For instance, a quick look at the website for the Department of Health and Social Services reveals a new NWT enhanced security birth certificate, a transformation of the way in which technology is being used to deliver health care (electronic medical records), a new Med-

Response clinical support line for community health workers which uses technology to connect people with services, and a discussion paper for improving the NWT Health and Social Services System. A new on-line registration system has been implemented by the Department of Transportation for motor vehicles and licenses. This is just the tip of the iceberg. All of these initiatives, and many more, may have impact upon how the government collects, uses and discloses personal information. This said, no one has considered asking my office for my comments or input on any of these initiatives. A recent legislative enactment which clearly will have privacy implications, the *Gunshot and Stab Wound Mandatory Disclosure Act*, passed without anyone thinking to ask for input from my office despite the significant privacy impact of that law. Access and privacy issues do matter to the ordinary man on the street. These issues need to be addressed during the planning stages of new programs. To this end, I would like to see a government wide policy requiring, as a minimum, that privacy impact assessments and access impact assessments be done in the earliest planning stages of new initiatives and that there is a check mark high up on the project planning sheet that says “consider whether or not the Information and Privacy Commissioner should be consulted or asked for comment.” While public bodies may not always agree with my input, and may choose to disregard any suggestions I might make, at least it will be clear that the issues were considered in the planning stages. And the public body will at least have the benefit of hearing another perspective.

No Annual Report of mine would be complete without a reference to the inclusion of municipalities under some form of access and/or privacy legislation. I understand that there is work being done to consider this matter further, including seeking the input of key stakeholders through a discussion paper. While I have yet to receive a copy of the discussion paper, or been consulted with respect to some of the issues which might be relevant to the discussion, I look forward to participating in this process and to finding a way to make our municipal governments more accountable through access and privacy legislation in the near future.

My current term as the Information and Privacy Commissioner of the Northwest Territories will come to an end in the fall of 2015. As noted in my opening comments, I have begun discussions with the Legislative Assembly about changing the structure of the office, with a view to setting up a full time office, with a full time administrator and an appropriate budget. With the coming into force of the *Health Information Act*, the time is right for a transition for this office and I hope to be able to help to oversee that transition over the next twelve months.





**NORTHWEST
TERRITORIES
INFORMATION
AND PRIVACY
COMMISSIONER**

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

25 août 2014

Assemblée législative des Territoires du Nord-Ouest
C. P. 1320
Yellowknife (Territoires du Nord-Ouest)
X1A 2L9

À l'attention de : Tim Mercer
Greffier de l'Assemblée législative

Monsieur,

J'ai l'honneur de soumettre à l'Assemblée législative des Territoires du Nord-Ouest mon rapport annuel pour la période du 1^{er} avril 2013 au 31 mars 2014.

Veillez agréer, Monsieur, mes sentiments distingués.

Elaine Keenan Bengts
Commissaire à l'information et à la protection de la vie
Privée Territoires du Nord-Ouest

/kb

TABLE DES MATIÈRES

MESSAGE DE LA COMMISSAIRE	43
COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE	47
<i>LA LOI SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DE LA VIE PRIVÉE</i>	49
ACCÈS À L'INFORMATION	50
PROTECTION DE LA VIE PRIVÉE	51
LE PROCESSUS	52
BILAN DE L'ANNÉE	54
PRÉSENTER UNE DEMANDE D'ACCÈS À L'INFORMATION	56
RECOMMANDATIONS RELATIVES AUX DEMANDES DE RÉVISION	57
RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-117	57
RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-118	61
RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-119	63
RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-120	65
RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-121	67
RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-122	69
RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 14-123	71
RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 14-124	73
RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 14-125	75
REGARD VERS L'AVENIR	77

RAPPORT ANNUEL 2013-2014

MESSAGE DE LA COMMISSAIRE



Le présent rapport annuel marque la 17^e année de l'entrée en vigueur de la *Loi sur l'accès à l'information et la protection de la vie privée* (la Loi) des Territoires du Nord-Ouest. Beaucoup de choses ont changé au cours des dix-sept dernières années. Qui aurait cru, en 1996, que des gens comme Julian Assange et Edward Snowden allaient attirer autant l'attention sur le droit d'accès de la population à l'information gouvernementale? Qui aurait envisagé la possibilité que le simple fait d'utiliser une carte de crédit puisse exposer le détenteur au vol d'identité? Chose certaine, en 1996, des sujets comme le « piratage » et les « atteintes graves à la protection des données » ne faisaient pas les manchettes chaque jour. Les sujets liés à l'information et à la protection de la vie privée ne faisaient pas partie de notre vocabulaire quotidien, et n'occupaient pas une place importante dans l'actualité. Aujourd'hui, la situation est bien différente. Le Canada, bien sûr, a connu sa part d'incidents qui ont marqué l'actualité. Par exemple, l'Agence du revenu du Canada a dû fermer ses serveurs ce printemps en raison d'un virus qui avait rendu le système vulnérable. Certaines provinces ont aussi connu des situations semblables, qu'il s'agisse de la suppression de dossiers gouvernementaux par des employés ou de l'utilisation de courriels privés par des

fonctionnaires de l'État pour éviter les demandes d'accès à l'information. L'accès à l'information et la protection de la vie privée ne sont plus d'obscurs concepts. Les Canadiens commencent à parler couramment de ces sujets entre eux. Les citoyens sont de plus en plus inquiets de l'érosion de leur droit à la vie privée, qu'ils considèrent comme une valeur fondamentale. Le gouvernement est de plus en plus souvent appelé à rendre compte de ses actions au moyen de demandes d'accès à l'information. Et les gens sont désormais plus nombreux à pointer le gouvernement du doigt et à dénoncer le fait qu'il néglige de protéger adéquatement les renseignements personnels.

Tout cela occasionne plus de travail pour mon bureau. Comme je le soulignais dans mon dernier rapport annuel, il serait opportun de donner une structure plus permanente au Commissariat à l'information et à la protection de la vie privée. En effet, au cours des 17 dernières années, j'ai rempli ma fonction de commissaire surtout à temps partiel, puisque j'agissais aussi comme commissaire à l'information et à la protection de la vie privée du Nunavut, tout en exerçant le droit dans un cabinet fort occupé de Yellowknife. Depuis quelques années, il est de plus en plus difficile de suffire à la tâche étant donné la somme de travail. En outre, je crois qu'en raison de la structure actuelle fondée sur le travail à temps partiel, le Commissariat et le rôle qu'il joue pour aider à assurer l'ouverture et la transparence du gouvernement ne jouissent pas toujours du respect qui leur est dû. Le Commissariat manque de temps pour travailler de manière proactive avec les ministères et il en a peu pour examiner les lois et règlements à l'étude ou rester au fait des nouveaux programmes qui peuvent avoir des répercussions sur le droit à la vie privée des gens. Plus important encore, avec l'entrée en vigueur de la Loi sur les renseignements médicaux au printemps ou à l'été 2015, je prévois une croissance exponentielle de la charge de travail du Commissariat. C'est

dans cette optique que j'ai soumis à l'Assemblée législative une proposition portant sur certaines de ces questions et, en particulier, sur la création d'un bureau permanent doté d'un adjoint administratif ou préposé à l'accueil à temps plein et l'ajout, dans le budget de 2016-2017, d'un enquêteur à temps plein. À compter du 31 décembre prochain, j'abandonnerai la pratique du droit pour me concentrer davantage sur ma fonction de commissaire à l'information et à la protection de la vie privée. Je pourrai ainsi consacrer tout le temps voulu au travail qui découlera de l'entrée en vigueur de la Loi sur les renseignements médicaux et assumer toutes les autres responsabilités de commissaire à l'information et à la protection de la vie privée en vertu de la Loi et du règlement afférent.

En octobre 2013, lors d'une réunion à Vancouver, des commissaires à l'information et à la protection de la vie privée des quatre coins du Canada ont adopté une résolution suggérant d'importantes mesures destinées à moderniser les lois sur l'accès à l'information et la protection de la vie privée, notamment le signalement obligatoire des atteintes à la vie privée, l'obligation légale de documentation et l'adoption de mesures plus strictes, y compris l'imposition de peines en cas de non-respect. La résolution en question était annexée à mon dernier rapport annuel. Par ailleurs, j'ai appris que le ministère de la Justice compte procéder à un examen en profondeur de la Loi sur l'accès à l'information et la protection de la vie privée. Il ne fait aucun doute que le moment est bien choisi, et j'invite le ministère à tenir compte des suggestions formulées dans le cadre de cette résolution. J'espère en outre avoir le plaisir de travailler avec le ministère à la conduite de cet examen.

En terminant, j'aimerais remercier le Comité permanent des opérations gouvernementales, à qui je présente chaque année mon rapport annuel, de l'appui et de la confiance qu'il m'a

toujours accordés. J'aimerais également saluer le travail de tous les coordonnateurs de l'accès à l'information et de la protection de la vie privée des divers organismes publics des TNO, qui ne ménagent pas leurs efforts pour veiller à ce que l'esprit et l'intention de la Loi sur l'accès à l'information et la protection de la vie privée soient respectés.



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

Créé en 1997, le Commissariat à l'information et à la protection de la vie privée est un organisme indépendant chargé de la surveillance et de l'application de la *Loi sur l'accès à l'information et la protection de la vie privée* des Territoires du Nord-Ouest. Cette loi régit 41 organismes publics, notamment des ministères, des sociétés d'État, des commissions et autres.

La commissaire à l'information et à la protection de la vie privée est nommée par le commissaire des TNO, sur la recommandation de l'Assemblée législative, pour un mandat de cinq ans. En tant que représentante indépendante, elle ne peut être destituée que « pour un motif valable ou en raison de son empêchement », ce qui lui permet de donner son avis en toute liberté et en toute franchise.

La commissaire à l'information et à la protection de la vie privée possède les pouvoirs suivants :

- mener des enquêtes, assurer la médiation et parvenir à un règlement dans des dossiers portant sur des différends en matière d'accès à l'information, et formuler des recommandations publiques à l'intention des organismes publics en ce qui a trait à ces dossiers;
- examiner et régler les plaintes pour atteinte à la vie privée;

- donner son avis sur les répercussions de textes législatifs ou de programmes gouvernementaux en matière d'accès à l'information et de protection de la vie privée;
- effectuer ou commander des recherches sur les dossiers qui nuisent à l'application de la Loi;
- sensibiliser la population à la question du droit d'accès à l'information et de la protection de la vie privée.

*Le droit à la vie privée, c'est le droit d'être
laissé tranquille – le plus fondamental des
droits, et celui auquel l'homme civilisé accorde
le plus d'importance.*

—Louis D. Brandeis

LA LOI SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DE LA VIE PRIVÉE

La *Loi sur l'accès à l'information et la protection de la vie privée* se fonde sur deux principes :

1. les documents publics doivent être accessibles au public;
2. les renseignements personnels doivent être protégés par les organismes publics.

La Loi définit les règles concernant l'accès aux documents publics; elle décrit aussi celles entourant la collecte, l'utilisation et la communication de renseignements personnels par les organismes publics des Territoires du Nord-Ouest.

La Loi s'applique à tous les organismes publics des TNO, incluant l'ensemble des ministères et des sociétés d'État ainsi que certains conseils, commissions et organismes.

La Cour suprême du Canada a déclaré que les lois comme la *Loi sur l'accès à l'information et la protection de la vie privée* sont des instruments spéciaux qui définissent certains des droits démocratiques fondamentaux que possèdent les citoyens. Il s'agit de lois « quasi constitutionnelles » qui ont généralement préséance sur d'autres lois.

ACCÈS À L'INFORMATION

La Loi donne au public le droit d'accès à la plupart des documents en la possession ou relevant des organismes publics. Si l'accès est toujours la norme, le droit d'accès est visé par un certain nombre d'exceptions spécifiques; la plupart de ces exceptions servent à protéger les droits concernant la vie privée des individus, à permettre aux représentants élus de rechercher et d'élaborer des politiques et à assurer le bon fonctionnement du gouvernement. Comme la Cour suprême du Canada a établi que la loi sur l'accès à l'information est de nature « quasi constitutionnelle », toutes les exceptions à l'accès du public aux documents doivent être limitées et définies avec précision.

Pour obtenir un document d'un organisme public, il faut en faire la demande par écrit et acheminer celle-ci à l'organisme public duquel on souhaite obtenir l'information. Si un requérant ne sait pas où adresser sa demande, il peut la transmettre à l'organisme public auquel il croit qu'elle est destinée. Si l'organisme en question ne possède pas les documents demandés, il doit s'assurer que la demande est acheminée à l'organisme public approprié.

Lorsqu'une demande d'accès à l'information est transmise à un organisme public, celui-ci a le devoir de trouver tous les documents visés par la demande. Il doit ensuite examiner ces documents pour déterminer s'ils peuvent être divulgués, en tout ou en partie, en vertu de la Loi, avant de les remettre au requérant. Dans la plupart des cas, les organismes publics doivent répondre aux demandes d'accès à l'information dans un délai de trente (30) jours.

Si la réponse n'est pas satisfaisante ou qu'elle n'est pas reçue dans le délai imposé par la Loi, le requérant peut demander à la commissaire à l'information et à la protection de la vie privée de réviser la décision.

PROTECTION DE LA VIE PRIVÉE

La Partie II de la Loi définit les règles que doivent respecter les organismes publics concernant la collecte des renseignements personnels, la manière dont ils peuvent être utilisés une fois colligés, ainsi que les circonstances permettant la communication de ces renseignements à un autre organisme public ou à des tiers. Elle établit aussi un mécanisme permettant aux individus de consulter leurs propres renseignements personnels détenus par un organisme gouvernemental et de demander des corrections, s'il y a lieu.

De plus, cette partie de la Loi exige que les organismes publics maintiennent des mesures de sécurité adéquates pour veiller à ce que les renseignements personnels dont ils font la collecte ne puissent être consultés par des personnes non autorisées.

Une personne aux prises avec un problème de protection des renseignements personnels peut présenter une demande de révision à la commissaire à l'information et à la protection de la vie privée. Celle-ci a le pouvoir de mener une enquête et d'adresser des recommandations à l'organisme public en question.

LE PROCESSUS

Lorsque la commissaire à l'information et à la protection de la vie privée reçoit une demande de révision relative à une question d'accès à l'information, elle communique avec le requérant et l'organisme public en cause pour déterminer quels documents sont concernés et obtenir une explication de l'organisme public quant aux raisons ayant mené à la décision. Le requérant et les tiers dont les renseignements sont visés par la demande ont eux aussi l'occasion d'exposer leur point de vue. La commissaire reçoit une copie de tous les documents visés par la demande dans leur version originale et de toutes les corrections apportées par l'organisme public en répondant à la demande. La commissaire tient donc compte du point de vue des parties concernées, des documents eux-mêmes et des dispositions de la Loi afin de rédiger un rapport accompagné de conclusions et recommandations. La commissaire n'a pas le pouvoir d'obliger les organismes publics à divulguer ou à cacher des renseignements, mais elle a l'obligation de formuler des recommandations. Le responsable de l'organisme public doit accepter ou refuser les recommandations formulées, ou encore indiquer que d'autres mesures seront prises à l'égard de la demande d'accès à l'information. La décision de l'organisme doit être communiquée à la commissaire dans les 30 jours suivant les recommandations, et le requérant a le droit d'en appeler devant la Cour suprême des TNO s'il n'est pas satisfait de la décision de l'organisme public.

Dans le cas d'une plainte portant sur une allégation de collecte, d'utilisation ou de communication de renseignements personnels de manière inappropriée, le processus est presque le même. La commissaire à l'information et à la protection de la vie privée communique avec l'organisme public et le plaignant ainsi qu'avec toute personne susceptible

de posséder des renseignements sur l'atteinte alléguée à la vie privée pour déterminer s'il y a effectivement eu atteinte à la vie privée. Que la plainte soit fondée ou non, la commissaire produit un rapport presque toujours accompagné de commentaires et de recommandations visant à améliorer les politiques et les procédures de manière à éviter de futures atteintes à la vie privée. Les recommandations formulées par la commissaire sur les questions de respect de la vie privée sont transmises au responsable de l'organisme public, qui décide ensuite d'accepter ou de rejeter les recommandations de la commissaire. Dans le cas de plaintes pour atteinte à la vie privée, l'organisme public dispose de 90 jours pour répondre. Aucun droit d'appel n'est prévu à la suite de la décision de l'organisme public dans le cas d'une plainte pour atteinte à la vie privée.

*Un gouvernement populaire sans information populaire, ou
les moyens de s'en procurer, n'est qu'un prologue à une farce
ou à une tragédie ou, peut-être, les deux.*

— Président James Madison, 4 août 1822

BILAN DE L'ANNÉE

Au cours de l'exercice 2013-2014, mon bureau a ouvert un total de 30 dossiers, soit près de deux fois plus que lors de l'exercice précédent. Au nombre de ceux-ci, mentionnons :

Demandes de révision – Accès à l'information	12
Demandes de révision – Protection de la vie privée	9
Demandes d'information sur la protection de la vie privée (atteintes dans le secteur privé)	4
Signalement proactif d'atteintes à la vie privée	2
Demandes de révision – Évaluation des droits	1
Appels de commentaires	1
Administration	1

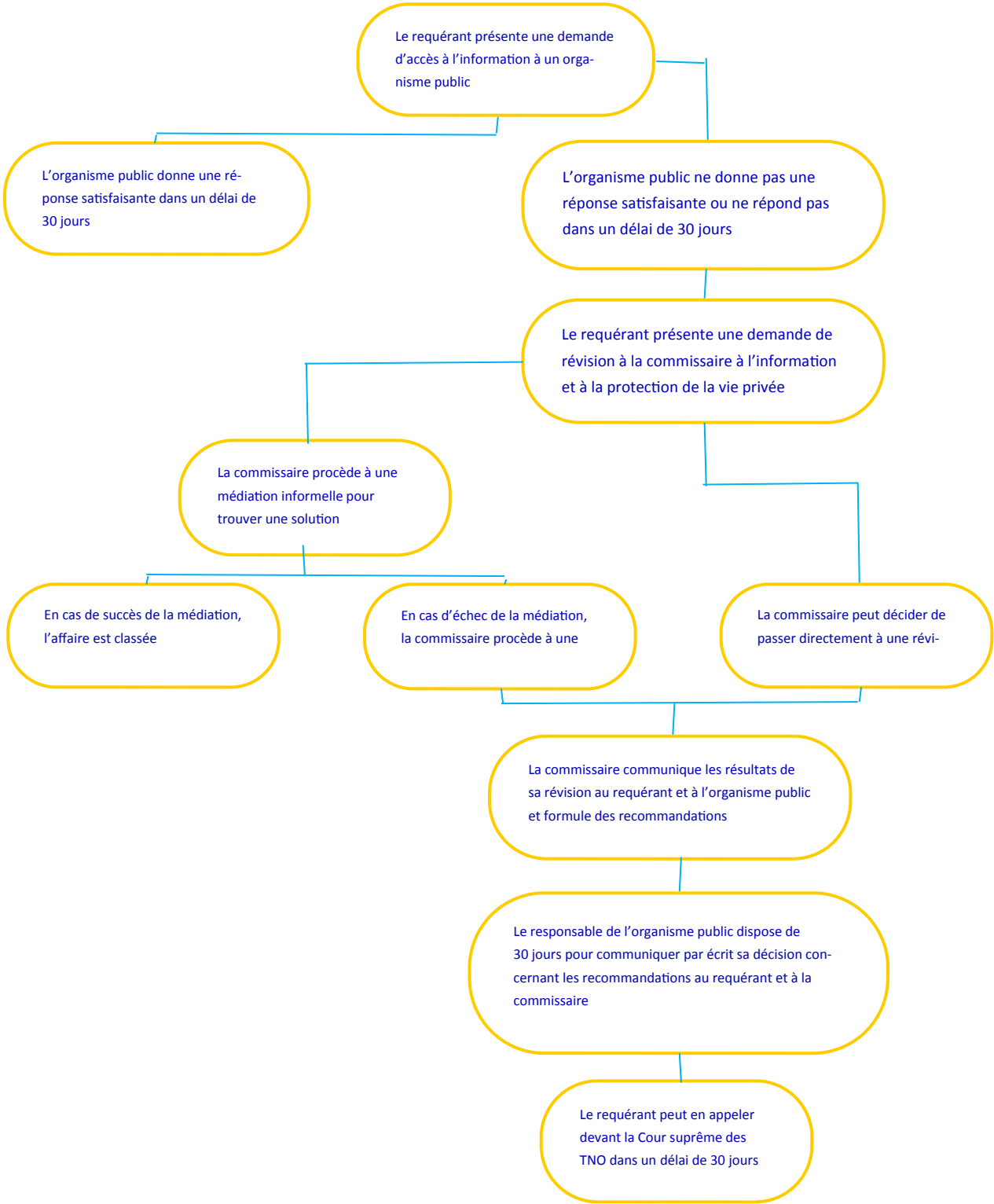
J'ai été ravie de recevoir cette année deux signalements d'atteinte à la vie privée. En effet, des organismes publics ont été témoins d'atteintes potentielles à la vie privée et se sont empressés d'en aviser mon bureau. Dans un des deux cas, le signalement a été suivi du dépôt d'une plainte officielle par un tiers. Dans l'autre cas, mon bureau a simplement exercé une surveillance puisque l'organisme public a réglé la question. Ce qui est plutôt préoccupant, c'est que, dans au moins sept des dossiers d'accès, un des problèmes était le temps de réponse de l'organisme public à la demande d'accès à l'information.

Plusieurs des dossiers ouverts cette année portent sur des plaintes pour atteinte à la vie privée dans le secteur privé. Dans deux cas, il s'agit d'organismes sans but lucratif qui ignoraient manifestement leurs obligations en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* fédérale destinée à protéger les renseignements personnels recueillis. J'ai travaillé avec ces organismes et leur ai fait des suggestions relativement aux problèmes soulevés. J'ai aussi traité avec sept organismes publics; les plus souvent concernés sont le ministère des Ressources humaines (sept dossiers), le ministère des Transports (six dossiers) et le ministère de la Justice (quatre dossiers).

Au cours de l'exercice, mon bureau a émis neuf recommandations relatives à des demandes de révision.



PRÉSENTER UNE DEMANDE D'ACCÈS À L'INFORMATION



RECOMMANDATIONS RELATIVES AUX DEMANDES DE RÉVISION

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-117

Catégorie de demande de révision :	Plainte pour atteinte à la vie privée
Organisme public en cause :	Administration des services de santé et des services sociaux de Yellowknife
Articles de la Loi concernés :	Article 43
Résultat :	Recommandations acceptées en partie

Dans ce cas, le plaignant était outré par la façon dont l'Administration des services de santé et des services sociaux de Yellowknife (ASSSSY) avait traité ses renseignements personnels. En raison de mauvaises expériences antérieures, il avait écrit à l'ASSSSY pour prier l'organisme de ne communiquer à personne, que ce soit à l'intérieur ou à l'extérieur de l'ASSSSY, aucun de ses renseignements médicaux personnels sans lui demander au préalable son consentement exprès écrit et signé. Voici ce que l'ASSSSY a indiqué au plaignant dans sa réponse : « En théorie, nous exigeons votre consentement seulement en cas de communication de renseignements à l'extérieur des frontières de l'organisme. » Cela dit, l'ASSSSY a aussi pris bonne note de l'interdiction de communiquer les renseignements du

plaignant. Lorsque, à un certain moment, le plaignant a été dirigé vers un psychiatre pour une consultation, il a refusé d'autoriser que son dossier médical soit transmis au psychiatre avant le rendez-vous parce qu'il ne faisait pas confiance à son médecin traitant. Par conséquent, un rendez-vous lui a d'abord été refusé, mais il en a finalement obtenu un. Lorsqu'il s'est présenté au rendez-vous, il a été avisé qu'il ne pouvait pas voir le psychiatre s'il ne consentait pas par écrit à autoriser son médecin traitant à recevoir le rapport du psychiatre. Il a refusé et la consultation n'a pas eu lieu.

L'ASSSSY a expliqué qu'elle fonctionne selon un modèle de soins primaires, en vertu duquel le médecin traitant est au centre des soins aux patients. Seul le médecin traitant peut diriger un patient vers un spécialiste. Après la consultation avec le spécialiste, le dossier revient au médecin traitant, qui est chargé de mettre en place le plan de soins. Si le médecin traitant ne reçoit pas le rapport de la consultation, aucun plan de traitement ne peut être mis en place. L'ASSSSY a insisté sur les responsabilités éthiques et professionnelles que les médecins et spécialistes ont les uns envers les autres.

La commissaire à l'information et à la protection de la vie privée a statué qu'en dépit du modèle de soins de l'ASSSSY, la priorité doit être accordée au patient à qui appartiennent les renseignements. Les responsabilités éthiques et professionnelles des médecins et des spécialistes envers le patient l'emportent sur les mêmes responsabilités qu'ont les fournisseurs de soins médicaux les uns envers les autres. Dans le cas où le patient donne des directives claires et sans équivoque pour que ses renseignements médicaux personnels ne soient pas divulgués sans son consentement, ces indications doivent être respectées, tout comme son droit d'obtenir les soins médicaux dont il a besoin. Aucun individu ne devrait se voir refuser des services médicaux parce qu'il désire rester maître de ses renseignements médicaux personnels.

Les trois recommandations suivantes ont été formulées relativement à ce dossier :

- a) que l'ASSSSY crée une brochure d'information à remettre à tous les patients sur la façon dont les renseignements médicaux personnels sont recueillis, utilisés et communiqués. Le nom et les coordonnées d'une personne de l'organisme qui peut répondre à toute question devraient figurer dans la brochure;
- b) que l'ASSSSY se dote de politiques et de procédures pour gérer les situations où un patient refuse d'autoriser la communication, à l'intérieur ou à l'extérieur, de renseignements médicaux personnels. La politique devrait établir clairement qu'on ne peut refuser des services à aucun patient pour la seule raison que celui-ci refuse d'autoriser la communication de ses renseignements médicaux personnels;
- c) que, dans ce cas, l'ASSSSY trouve un moyen de procurer au plaignant les services de santé psychiatrique dont il a besoin tout en respectant son droit de contrôler l'accès à ses dossiers médicaux.

Si l'organisme public a qualifié certaines des recommandations de « suggestions raisonnables et valables », les recommandations n'ont été acceptées qu'en partie. En particulier, comme l'ASSSSY estime que son formulaire de consentement standard est suffisant pour renseigner la population sur la façon dont les renseignements médicaux personnels peuvent être utilisés et communiqués, elle a refusé de produire une brochure explicative. L'organisme a toutefois indiqué qu'il procède actuellement à la mise en place d'un nouveau cadre en matière de protection de la vie privée, et que des dispositions appropriées pour gérer ce type de situation y seront intégrées. Il a accepté de continuer de travailler avec le patient afin de parvenir à une entente mutuellement acceptable qui protège les droits du client et les

obligations des praticiens, et qui permette le bon fonctionnement de l'organisme au sein du système de santé. L'organisme public n'est cependant pas d'accord avec la commissaire sur la façon dont les renseignements médicaux personnels peuvent être utilisés une fois recueillis. Il insiste pour continuer de miser sur le concept vague de « cercle de soins » qui, comme l'expérience l'a montré, a des significations très différentes d'une personne à l'autre. Toutes ces questions devront être gérées d'une façon beaucoup plus structurée et cohérente après l'entrée en vigueur de la nouvelle *Loi sur les renseignements médicaux*.

Lorsqu'un patient exprime des préoccupations à l'égard du partage de ses renseignements personnels au sein de l'Administration, l'ASSSY doit trouver un moyen de respecter ces préoccupations sans refuser au patient les services médicaux dont il a besoin.

— Elaine Keenan Bengts—Recommandation relative à la demande de révision 13-117

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-118

Catégorie de demande de révision :	Accès à l'information
Ministère en cause :	Ministère des Ressources humaines
Articles de la Loi concernés :	Articles 8 et 11 et alinéas 14(1)(a), 14(1)(b), 23(2)(d) et 23(2)(i)
Résultat :	Recommandations acceptées

Dans ce cas, le requérant cherchait à obtenir des documents associés à une réunion à son sujet, qui avait eu lieu à son travail. Il avait appris après coup la tenue de la réunion et, à la suite de celle-ci, on lui avait demandé de se procurer un certificat médical. Il croyait que des renseignements erronés avaient circulé pendant cette réunion, et que les renseignements en question avaient été portés à son dossier personnel. Cette demande renfermait aussi une demande de rappel à l'ordre de l'organisme public concernant le délai de réponse. Le requérant a expliqué que la demande a été présentée le 27 novembre. Le 18 décembre, il recevait une lettre prorogeant le délai de réponse jusqu'au 25 février et, dans une conversation avec le ministère antérieure au 25 février, il a été avisé que le délai allait être de nouveau prorogé. C'est finalement le 15 mars qu'il a reçu la réponse. Un grand nombre des documents reçus contenaient des blancs et des modifications. Le ministère s'est appuyé sur les articles 14 ou 23 pour justifier les éléments retranchés.

Sur la question du délai, la commissaire a conclu que l'organisme public a manqué à ses obligations en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*, tant sur le plan du processus que sur celui du délai. La Loi prévoit seulement qu'un organisme public peut proroger, pour une période de temps « raisonnable », le délai de réponse prévu. Le motif indiqué pour justifier la prorogation était un « surplus de travail administratif », mais il ne s'agit pas d'un motif valable de prorogation en vertu de la Loi. L'organisme public n'a pas non plus fourni un motif valable pour la prorogation de deux mois après la date de la première réponse. Il s'agissait seulement de 61 documents représentant environ 150 pages. Ce n'est pas un grand nombre de documents et, dans les circonstances, la durée de la prorogation n'était pas raisonnable. La commissaire a recommandé que le ministère revoie ses processus et procédures en matière de gestion des demandes d'accès à l'information pour faire en sorte que des réponses puissent être fournies en temps opportun et en accord avec la Loi.

Pour ce qui est de la réponse, la commissaire en a fait une analyse ligne par ligne et a recommandé la divulgation d'un certain nombre d'éléments retranchés. Elle a souligné que la divulgation est toujours la norme et que, lorsque des documents ou des parties de documents ne sont pas communiqués, les portions retranchées doivent bel et bien relever de l'exception. Qui plus est, si l'exception est de nature discrétionnaire comme le prévoit l'article 14, la règle est toujours la divulgation, et si le pouvoir discrétionnaire est utilisé pour refuser la divulgation, il doit être activement exercé, motifs à l'appui. Pour constituer « des avis, des propositions, des recommandations, des analyses ou des options de politiques administratives » en vertu de l'article 14 et être soumis au pouvoir discrétionnaire d'exception, les renseignements doivent :

- a) être recherchés ou escomptés ou relever de la responsabilité d'une personne en vertu du poste qu'elle occupe;
- b) être utilisés pour prendre une mesure;
- c) être transmis à une personne qui peut prendre ou mettre en place la mesure.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-119

Catégorie de demande de révision :	Accès à l'information
Ministère en cause :	Ministère des Transports
Articles de la Loi concernés :	Sous-alinéas 14(1)(b)(i) et 14(1)(b)(ii) et alinéas 14(1)(d), 23(2)(a), 23(2)(d) et 23(2)(i)
Résultat :	Recommandations relatives à la demande de révision acceptées

Le requérant demandait ses propres renseignements personnels en raison d'un conflit en milieu de travail. Il occupait un poste de superviseur et ses activités préoccupaient plusieurs de ses subordonnés. L'organisme public a trouvé un certain nombre des documents visés par la demande, et la plupart d'entre eux ont été remis au requérant sans avoir été modifiés. Toutefois, certains documents n'ont pas été communiqués, en tout ou en partie. La demande porte aussi sur les préoccupations à l'égard du temps de réponse à la demande du requérant,

qu'il avait présentée le 28 novembre 2013. Le délai de réponse a été plusieurs fois prorogé avant que celle-ci parvienne finalement au requérant le 7 mars 2014.

En ce qui concerne les prorogations du délai pour répondre au requérant, la commissaire a conclu qu'il y avait des irrégularités dans le processus, et que l'organisme public n'avait pas respecté les exigences de la Loi. En outre, elle a conclu que, dans les circonstances, la durée de la prorogation n'était pas « raisonnable ».

Pour ce qui est de la réponse, la commissaire en a fait une analyse ligne par ligne et a recommandé la divulgation d'un certain nombre des éléments retranchés. Comme dans la recommandation relative à la demande de révision 13-118, elle a souligné que la divulgation est toujours une règle, et que les exceptions devraient être étroitement interprétées et appliquées. Lorsqu'une exception applicable relève du pouvoir discrétionnaire, l'organisme public doit exercer activement ce pouvoir dans le cas de chaque exclusion.

Il y a une raison pour laquelle la période de réponse de 30 jours figure dans la Loi. Ce n'est pas un objectif ni une suggestion. C'est une exigence.

— Elaine Keenan Bengts, Recommandation relative à la demande de révision 13-118

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-120

Catégorie de demande de révision :	Plainte pour atteinte à la vie privée – Collecte inappropriée de renseignements personnels
Ministère en cause :	Ministère de l'Éducation, de la Culture et de la Formation
Articles de la Loi concernés :	Alinéa 40(c)(i)
Résultat :	Recommandations acceptées

Une personne a soulevé des préoccupations à l'égard de la collecte de renseignements personnels par le ministère de l'Éducation, de la Culture et de la Formation (MÉCF) auprès d'étudiants qui avaient reçu des prêts remboursables dans le cadre du programme d'aide financière aux étudiants et qui demandaient l'annulation partielle de leurs dettes en raison du temps travaillé aux Territoires du Nord-Ouest une fois leurs études terminées. Pour être admissibles, les étudiants devaient prouver qu'ils habitaient aux Territoires du Nord-Ouest en produisant trois preuves, établies à trois mois différents, pendant chaque période de six mois.

Huit types de documents étaient jugés acceptables :

- a) un bail ou une hypothèque pour une résidence aux Territoires du Nord-Ouest;
- b) un relevé de taxes foncières pour une résidence aux Territoires du Nord-Ouest;

- c) des factures de services publics au nom de l'étudiant;
- d) des relevés bancaires (y compris les relevés de cartes de crédit);
- e) la preuve que l'étudiant a présenté à l'Agence du revenu du Canada une déclaration de revenus des TNO;
- f) une lettre signée par un employeur sur papier à en-tête confirmant les dates de début et de fin d'emploi ou des bordereaux de paie;
- g) des relevés d'assurance-emploi;
- h) des rapports sur la situation financière dans le cadre de l'aide au revenu.

Le plaignant estimait qu'il lui était impossible de respecter ces critères, même s'il occupait un poste à temps plein à Yellowknife. Comme il vivait avec ses parents, il ne disposait d'aucun des trois premiers types de documents qu'il pouvait présenter. Et comme il travaillait à temps plein, il ne disposait pas non plus des deux derniers types de documents. La déclaration de revenus a été produite seulement une fois par année et ne pouvait être utilisée qu'une seule fois, alors que ses relevés de compte bancaire conjoint étaient jugés inacceptables. Le MÉCF a avisé le plaignant qu'il pouvait produire un relevé de carte de crédit si celui-ci comportait des achats importants effectués aux Territoires du Nord-Ouest. Le plaignant a refusé de le faire pour des raisons de confidentialité, en alléguant que les bordereaux de paie d'un employeur des TNO devraient suffire.

La commissaire a déclaré que chacun de ces documents comportait sa part de renseignements personnels et que la plupart d'entre eux n'avaient rien à voir avec une preuve de résidence. Par exemple, si un bordereau de paie porte le nom d'un employeur des

TNO, il comprend aussi entre autres le taux de salaire horaire, le montant cumulatif des gains et la nature du contrat de l'employé. Par ailleurs, les relevés bancaires et de carte de crédit contiennent encore plus de renseignements sur les habitudes en matière de dépenses et le style de vie.

La commissaire a souligné que l'organisme public devrait recueillir uniquement les renseignements pouvant aider à établir que la personne résidait bel et bien aux Territoires du Nord-Ouest pendant la période concernée. Qui plus est, on devrait exiger le moins de renseignements possible pour satisfaire ce critère.

La commissaire a formulé quatre recommandations pour réduire la somme de renseignements personnels recueillis.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-121

Catégorie de demande de révision : Plainte pour atteinte à la vie privée

Ministère en cause : Ministère de la Justice

Articles de la Loi concernés : Articles 40, 43 et 48

Résultat : Aucune recommandation formulée

Dans ce cas, le plaignant s'opposait à ce que le Bureau du shérif obtienne ses renseignements personnels du ministère de la Santé et des Services sociaux ou d'autres instances

gouvernementales des Territoires du Nord-Ouest et les utilise dans le but de l'identifier et de le trouver pour l'assigner à remplir ses fonctions de juré.

Le ministère de la Justice a invoqué les paragraphes 8(2) et (3) de la *Loi sur le jury* qui stipulent que, malgré la *Loi sur l'accès à l'information et la protection de la vie privée*, le directeur de l'assurance-maladie doit, sur demande, fournir au shérif le nom et l'adresse des assurés âgés d'au moins 18 ans pour permettre d'établir la liste des jurés. Cette information est partagée en vertu d'une entente de partage d'information conclue entre le ministère de la Santé et des Services sociaux et le ministère de la Justice. Cette entente interdit l'utilisation subséquente de l'information, prévoit un calendrier de conservation et de destruction et établit les normes pour assurer la sécurité et la confidentialité de l'information.

À la lumière de l'autorité législative conférée aux deux ministères par la *Loi sur le jury*, la commissaire a statué que l'échange de renseignements aux fins de la création d'une liste de jurés était autorisé. Elle n'a formulé aucune recommandation.



RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 13-122

Catégorie de demande de révision :	Question d'atteinte à la vie privée – Collecte de renseignements personnels
Ministère en cause :	Ministère de la Santé et des Services sociaux
Articles de la Loi concernés :	Paragraphe 40(1) et 40(2)
Résultat :	Recommandations acceptées

Cette plainte venait d'une personne qui estimait que le ministère de la Santé et des Services sociaux exigeait d'elle des renseignements personnels dont il n'avait pas besoin. Le plaignant présentait une demande de renouvellement de sa couverture d'assurance-maladie des TNO. Le ministère lui a envoyé un formulaire à remplir qui comportait une question visant à savoir s'il occupait un emploi et, si oui, qui était son employeur, son numéro de téléphone, s'il était admissible à des prestations en vertu d'un régime d'assurance d'un employeur ou d'un tiers et, le cas échéant, le nom du régime et les modalités de l'assurance. Il devait fournir ces renseignements pour lui-même et sa conjointe. Le plaignant jugeait que le ministère n'avait pas besoin de ces renseignements pour évaluer son admissibilité à la couverture d'assurance-maladie des TNO.

Le ministère a expliqué que ces questions faisaient partie de la Partie B du formulaire, qui doit être remplie seulement si un requérant est inscrit à un ou plusieurs programmes procurant des avantages supplémentaires (par exemple, les médicaments sur ordonnance, les

fournitures et le matériel médicaux et les soins dentaires). Il a souligné que ces renseignements sont requis parce qu'une assurance extérieure peut modifier le niveau de couverture obtenu dans le cadre du programme de soins de santé.

La commissaire a reconnu que le ministère avait une raison légitime de chercher à savoir si le requérant était ou non couvert par une assurance de tiers, mais elle était d'avis qu'il exigeait trop de renseignements non nécessaires. La *Loi sur l'accès à l'information et la protection de la vie privée* permet aux organismes publics de recueillir uniquement les renseignements dont ils ont besoin pour la prestation d'un service. Il n'était pas nécessaire pour le ministère de savoir si le requérant ou sa conjointe occupaient ou non un emploi. Il lui fallait uniquement savoir si l'un ou l'autre possédaient une assurance de tiers.

La commissaire a aussi souligné que l'organisme public qui recueille les renseignements est tenu d'informer la personne des fins auxquelles ils sont recueillis et de l'instance légale responsable de la collecte, et de lui communiquer le nom et les coordonnées d'un employé de l'organisme pouvant répondre aux questions relatives à la collecte. Or, cela n'a pas été fait dans ce cas.

La commissaire a recommandé une analyse du formulaire en question afin de déterminer s'il est absolument nécessaire de recueillir les renseignements sur l'emploi. Elle a aussi recommandé une analyse plus complète de toutes les lettres types accompagnant les formulaires pour s'assurer qu'une description adéquate de la raison pour laquelle les renseignements sont recueillis y figure.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 14-123

Catégorie de demande de révision :	Plainte pour atteinte à la vie privée – Utilisation ou communication non autorisées
Ministère en cause :	Ministère des Transports
Articles de la Loi concernés :	Paragraphe 47(1)
Résultat :	Recommandations acceptées

Le plaignant était un camionneur employé par une entreprise du secteur privé. Il a été interpellé par un agent du transport routier du ministère des Transports qui lui a remis un avertissement pour excès de vitesse. Lorsque le plaignant est retourné au travail le lendemain, il a été accueilli par ses collègues, qui l'ont taquiné à propos de l'avertissement qu'il avait reçu. Un des collègues en question était un camarade de chambre de l'agent du transport routier et, de l'avis du plaignant, ce dernier avait divulgué un renseignement de manière inappropriée.

Le plaignant a porté plainte auprès du ministère des Transports directement. La personne qu'il a rencontrée au sujet de la plainte a enregistré la conversation sur un téléphone cellulaire, ce qui a préoccupé encore plus le plaignant concernant la façon dont ses renseignements allaient être sauvegardés et utilisés, et la possibilité de nouvelle divulgation.

L'enquête du ministère n'a pas permis de confirmer l'affirmation du plaignant et personne, hormis le plaignant, n'a admis avoir entendu le collègue taquiner le plaignant et, bien sûr, le camarade de chambre a nié l'avoir fait. En ce qui a trait à l'enregistrement, le ministère a dit que l'enquêteur s'est assuré que son appareil mobile était protégé par un mot de passe et demeurait en sa possession jusqu'à ce que l'enregistrement soit sauvegardé sur le réseau du ministère et que, une fois sauvegardé, il était supprimé de l'appareil mobile.

La commissaire a statué que le paragraphe 47(1) de la Loi énonce clairement qu'il est interdit aux employés des organismes publics de divulguer des renseignements personnels reçus dans l'exercice de leurs fonctions au sein de l'organisme public. Si l'organisme a conclu qu'il n'existait « pas de preuve » que l'agent du transport routier avait porté atteinte à la vie privée du plaignant, la commissaire n'était pas d'accord; il existait certaines preuves, mais peut-être pas assez pour tirer une conclusion définitive sur ce qui était arrivé. La commissaire a statué que, pour déterminer s'il y a eu ou non atteinte dans une situation comme celle-là, il ne s'agit pas tant de savoir si l'allégation peut être prouvée ou non, mais si elle peut être réfutée. Les organismes publics sont responsables de s'assurer que les renseignements personnels recueillis ou obtenus au cours de l'emploi d'une personne sont protégés contre l'utilisation ou la communication non autorisées. À moins que l'allégation puisse être réfutée, il faut que le ministère se penche de façon objective sur ce qui est arrivé afin de déterminer s'il serait possible d'en faire plus pour protéger la vie privée des gens. La commissaire a aussi reconnu que tout employé du GTNO est tenu de signer un Serment professionnel et engagement au secret professionnel. Elle a toutefois souligné que cela est loin de garantir que l'employé tiendra son serment, et qu'on ne devrait pas s'en servir comme preuve pour établir qu'aucune divulgation n'a eu lieu.

En ce qui a trait à l'enregistrement, la commissaire s'est dite préoccupée par l'utilisation d'un appareil mobile pour enregistrer une entrevue.

Elle a formulé quatre recommandations pour aider à améliorer les pratiques en matière de vie privée au sein du ministère des Transports, notamment de proposer une formation supplémentaire sur la Loi aux agents du transport routier et de passer en revue avec le personnel les politiques et les procédures en place en ce qui a trait aux appareils mobiles.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 14-124

Catégorie de demande de révision :	Atteinte à la vie privée – Collecte de renseignements
Ministère en cause :	Ministère des Ressources humaines
Articles de la Loi concernés :	Articles 40, 43 et 48
Résultat :	Recommandations acceptées

Dans ce cas, le plaignant avait posé sa candidature à un poste au GTNO. Il a été avisé qu'il ne répondait pas aux critères de sélection, et que sa candidature n'était par conséquent pas retenue. Il en a appelé de la décision. Lors de l'appel, il a été recommandé que le concours soit repris à partir de l'étape de la présélection, et qu'une entrevue soit accordée au plaignant. Pendant l'entrevue, on a demandé aux candidats de fournir des références. Or, le

comité de sélection a soulevé des questions en ce qui concerne une politique d'embauche en particulier, qui ont été transmises aux Services généraux. En attendant une réponse, pour gagner du temps, il a procédé à la vérification des références des deux candidats. Le poste a finalement été offert à l'autre candidat, et le plaignant était outré que ses références aient été vérifiées même si on ne lui avait pas offert le poste. En temps normal, on vérifie seulement les références de la personne à laquelle on compte présenter une offre.

En premier lieu, il s'agissait de savoir si l'organisme public avait utilisé les renseignements personnels du plaignant en contravention de la Loi et, en deuxième lieu, si, en vérifiant les références, l'organisme avait recueilli des renseignements personnels du plaignant de manière inappropriée.

Dans ce cas, le ministère a utilisé et divulgué des renseignements personnels du plaignant au moment de communiquer avec les personnes données en référence. Si le plaignant avait consenti, implicitement, à l'utilisation et à la divulgation, le consentement avait été donné suivant l'idée que la vérification des références aurait lieu seulement dans l'éventualité où le poste lui serait offert. L'utilisation et la divulgation ne sont par conséquent pas conformes à la Loi. De même, la cueillette des renseignements personnels du plaignant auprès des personnes données en référence n'était pas consensuelle dans les circonstances et, par conséquent, était contraire à la Loi.

La commissaire a formulé trois recommandations :

- a) que des excuses soient présentées au plaignant;
- b) que tout renseignement recueilli auprès des personnes données en référence soit détruit;

- c) que le ministère revoie et clarifie ses politiques écrites en ce qui concerne le processus d'embauche et, en particulier, la vérification des références.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION 14-125

Catégorie de demande de révision :	Plainte pour atteinte à la vie privée
Ministère en cause :	Ministère de la Justice
Articles de la Loi concernés :	Article 42
Résultat :	Recommandations acceptées en partie

Le plaignant a reçu une lettre du ministère de la Justice, son ancien employeur, indiquant que le ministère avait découvert que des renseignements personnels sur le revenu le concernant avaient par inadvertance été sauvegardés dans un dossier partagé du GTNO sur le réseau du gouvernement et que, par conséquent, il était possible que des personnes non autorisées aient pu y avoir accès. Les renseignements se trouvaient dans un sous-dossier portant un nom anodin non susceptible de piquer la curiosité. Il n'y avait pas de preuve que quiconque, hormis les employés autorisés, avait accédé au fichier, mais aucun dispositif de vérification ne permettait de s'en assurer. Toutes les personnes travaillant sur le dossier avaient cru comprendre que des mécanismes de sécurité appropriés étaient en place pour prévenir l'accès non autorisé, mais elles avaient tort.

La commissaire a souligné que la *Loi sur l'accès à l'information et la protection de la vie privée* ne comprenait aucune obligation pour l'organisme public d'aviser le plaignant de l'atteinte et que sa décision de le faire était louable. L'organisme a reconnu la gravité potentielle de la situation et a décidé d'y remédier directement et en toute transparence.

Avant que la commissaire ait terminé son analyse, le ministère avait déjà pris un certain nombre de mesures pour améliorer ses politiques et procédures afin d'éviter que de telles situations se reproduisent. Elle a cependant formulé d'autres recommandations :

- a) que l'on envisage de doter tous les systèmes du réseau du GTNO de dispositifs de vérification pour que, lorsqu'une erreur humaine se produit, comme dans le cas présent, les organismes publics puissent procéder à une vérification du système pour savoir s'il a été l'objet d'accès non autorisés. L'organisme public n'a pas accepté cette recommandation. Il a plutôt indiqué qu'il valait mieux à son avis mettre en place des procédures ou des lignes directrices écrites pour assurer la sécurité des renseignements personnels avant que ceux-ci soient placés sur un disque partagé;
- b) que le Centre de services technologiques procède à un examen systémique de son système de réseau et des « partages de fichiers » de chaque ministère, de concert avec la haute direction, de façon à s'assurer que tous les disques sont dotés des mécanismes de sécurité nécessaires. Le ministère de la Justice et le ministère des Finances ont tous deux donné leur accord pour analyser chaque année leurs dossiers de fichiers partagés. Ils ont toutefois tenu à souligner que

REGARD VERS L'AVENIR

cette tâche ne relevait pas de la responsabilité du Centre de services technologiques, mais de chaque ministère;

- c) que les responsables de la gestion des renseignements passent en revue toutes les politiques et les procédures qui concernent la gestion des renseignements et, en particulier, les calendriers de conservation et de destruction. Cette recommandation a été acceptée.

Chaque année, dans la présente section de mon rapport annuel, je fais des recommandations pour régler des questions soulevées de temps à autre en vue d'améliorer la façon dont la Loi atteint ses objectifs.

Avec l'adoption cette année de la *Loi sur les renseignements médicaux*, la prochaine année sera consacrée à la préparation en vue de la mise en œuvre de la Loi. Il s'agit d'une loi complexe, difficile à interpréter et à comprendre, et la courbe d'apprentissage sera abrupte pour toutes les personnes concernées : le secteur de la santé, mon bureau et la population. Comme je le notais dans mon précédent rapport annuel, la mise en application de cette Loi devra s'accompagner d'une importante campagne de sensibilisation s'adressant non seulement aux personnes qui travaillent dans le secteur de la santé, mais aussi à l'ensemble de la population. Bien avant la mise en œuvre de la Loi, il faudra élaborer de nouvelles politiques et procédures à l'intention des dépositaires des renseignements médicaux de façon

à ce qu'ils n'aient pas à faire des pieds et des mains à la dernière minute pour bien s'y retrouver. Il y aura beaucoup de travail à faire pour veiller à ce que les citoyens aient une bonne compréhension pratique de la manière dont leurs renseignements médicaux personnels seront recueillis, utilisés et communiqués en vertu de la Loi, des choix qui s'offrent à eux et des répercussions de ces choix. La nouvelle Loi n'est que la première étape. Beaucoup de travail reste encore à faire, mais j'ai hâte d'assister à la mise en œuvre de cette Loi, que j'attends depuis des années.

Une des choses qui est devenue de plus en plus frustrante pour moi au cours des dernières années, c'est le fait que les organismes publics semblent rarement tenir compte des répercussions des nouvelles initiatives sur le droit d'accès à l'information ou sur la vie privée des gens. Par ailleurs, je ne reçois pas souvent de demandes de commentaires lorsque de nouveaux programmes ou de nouvelles lois ou initiatives pouvant avoir des répercussions dans mon domaine d'expertise sont envisagés. Par exemple, un coup d'œil rapide au site Web du ministère de la Santé et des Services sociaux permet d'apprendre qu'il existe maintenant aux TNO un nouveau certificat de naissance à la sécurité renforcée, que la façon dont la technologie est utilisée transforme la prestation des soins de santé (dossiers médicaux électroniques), qu'une nouvelle ligne d'aide clinique appelée Med-Response, qui utilise la technologie pour relier les gens et les services, a été mise en place à l'intention des travailleurs de la santé, et qu'un document de travail portant sur l'amélioration du système de santé et de services sociaux des TNO a été créé. En outre, le ministère des Transports a mis en place un nouveau système d'enregistrement en ligne pour les véhicules moteurs et les plaques d'immatriculation. Et ce n'est que la pointe de l'iceberg. Toutes ces initiatives et de nombreuses autres peuvent avoir des répercussions sur la façon dont le gouvernement

recueille, utilise et communique les renseignements personnels. Cela dit, personne n'a songé à s'adresser à mon bureau pour obtenir un avis ou un point de vue sur l'une ou l'autre de ces initiatives. Un autre texte législatif, la *Loi sur la déclaration obligatoire des blessures par balle et par arme blanche*, qui aura assurément des répercussions importantes sur la vie privée, a été adopté récemment sans que personne ne songe à demander le point de vue de mon bureau à ce sujet. Les questions d'accès à l'information et de protection de la vie privée sont pourtant importantes pour le citoyen ordinaire, et elles devraient être abordées aux étapes de la planification de nouveaux programmes. C'est dans cette optique que je souhaiterais voir instaurer à l'échelle du gouvernement une politique exigeant à tout le moins que des évaluations des répercussions sur la protection de la vie privée et l'accès à l'information soient effectuées dès les premières étapes de la planification de nouvelles initiatives, et qu'une directive figure au haut de la feuille de planification du projet selon laquelle il faut « déterminer s'il y a lieu ou non de consulter la commissaire à l'information et à la protection de la vie privée ou de lui demander son avis. » Les organismes publics ne sont peut-être pas toujours d'accord avec mon point de vue et peuvent choisir d'ignorer mes suggestions, mais au moins ainsi, il ne fera aucun doute que ces questions ont été prises en compte lors des étapes de planification. Et l'organisme public aura au moins l'avantage d'entendre un autre point de vue.

Mon rapport annuel ne saurait être complet sans que j'y aborde la question de l'inclusion des municipalités dans une forme ou une autre de dispositions législatives sur l'accès à l'information ou la protection de la vie privée. Je sais qu'il y a beaucoup de travail à faire pour aller plus loin dans cette voie, notamment solliciter le point de vue des principaux intervenants dans le cadre d'un document de travail. Je n'ai pas encore reçu d'exemplaire du

document de travail ni été consultée sur certaines des questions qui peuvent être pertinentes dans la discussion, mais j'espère prendre part à ce processus et trouver sous peu une façon de rendre nos administrations municipales plus responsables à l'avenir au moyen de dispositions législatives sur l'accès à l'information et la protection de la vie privée.

Mon mandat actuel de commissaire à l'information et à la protection de la vie privée des Territoires du Nord-Ouest prendra fin à l'automne 2015. Comme je l'indiquais dans mes commentaires d'introduction, j'ai entamé des discussions avec l'Assemblée législative à propos du changement de structure du Commissariat, en vue de créer un bureau permanent doté d'un administrateur à temps plein et d'un budget correspondant. Avec l'entrée en vigueur de la *Loi sur les renseignements médicaux*, le moment est bien choisi pour donner cette structure au Commissariat, et j'espère pouvoir aider à superviser la transition au cours de la prochaine année.

