TABLED DOCUMENT 24-17(4)
TABLED ON FEBRUARY 19, 2013

INFORMATION AND PRIVACY COMMISSIONER OF THE NORTHWEST TERRITORIES

ANNUAL REPORT 2011/2012

COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DES TERRITOIRES DU NORD-OUEST

RAPPORT ANNUEL 2011-2012

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

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

September 28, 2012

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

Attention: Tim Mercer
Clerk of the Legislative Assembly

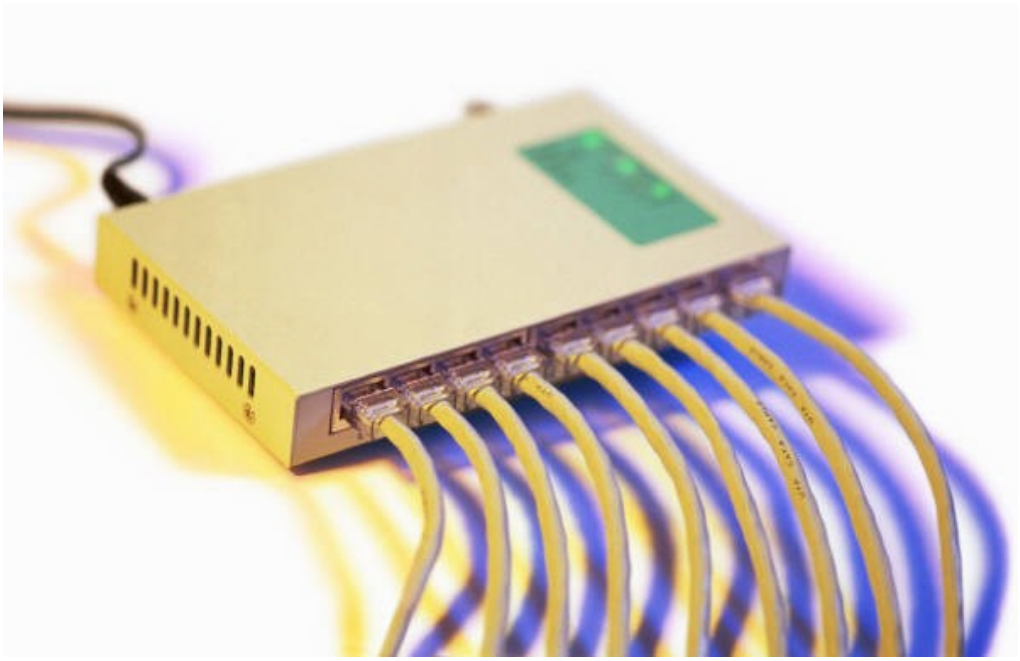
Dear Sir:

I have the honour to submit my annual report to the Legislative Assembly of the Northwest Territories for the period from April 1st, 2011 to March 31st, 2012.

Yours very truly

Elaine Keenan Bengts
Information and Privacy Commissioner
Northwest Territories

In Yellowknife: 403-669-0976 ♦ Toll free: 888-521-7088 ♦ Fax: 403-920-2511 ♦ E-mail: AttipComm@theedge.ca



INDEX

	Page
Commissioner's Message	6
The Legislation	9
The Year In Review	13
Review Recommendations	14
Review Recommendation 11-095	14
Review Recommendation 11-096	17
Review Recommendation 11-097	18
Review Recommendation 11-098	21
Review Recommendation 11-099	23
Review Recommendation 11-100	24
Review Recommendation 11-101	25
Review Recommendation 11-102	27
Review Recommendation 11-103	28
Review Recommendation 11-104	31
Looking Ahead	38

COMMISSIONER'S MESSAGE

When the Access to Information and Protection of Privacy Act was passed in 1994, we lived in a very different world. The Act was part of a country wide movement toward recognizing in legislation the basic democratic principal that members of the public have a right to know what government is doing on its behalf, and an independent way to verify that public bodies were following the rules. At the same time, the legislation recognized that governments hold a lot of personal information about citizens and that citizens have the right to feel confidence that that information is secure, protected and used only for the purposes that it is collected.

So much has changed in the intervening years. The prevalence of email as the primary means of communication in the work place, the advent of social media and the demands of the public for more effective information sharing and open data have presented new challenges are just the tip of the iceberg. In many ways, the new technologies have made the public both more aware of their right to access to public information and more concerned about the ability of public bodies to maintain the confidentiality of their personal information. Notwithstanding the changing technologies, however, the underlying principles of the Act – crafted so deliberately and carefully – continue to stand us in good stead.

The purposes of the Act are stated in the very first section of the Act, as follows:

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

(a) giving the public a right of access to records held by public bodies;

(b) giving individuals a right of access to, and a right to request correction of, personal information about themselves held by public bodies;

(c) specifying limited exceptions to the rights of access;

(d) preventing the unauthorized collection, use or disclosure of personal information by public bodies; and

(e) providing for an independent review of decisions made under this Act.

As noted by , Mr. Justice La Forest of the Supreme Court of Canada in the 1997 case of *Dagg v. Canada (Minister of Finance)* [1997], 2 S.C.R. 403 in what has proven to be the most enduring statement about the purpose of access and privacy legislation:

> The overarching purpose of access to information legislation … is to facilitate democracy. It does so in two related ways. It helps to ensure first, that citizens have the information required to participate meaningfully in the democratic process and secondly, that politicians and bureaucrats remain accountable to the citizenry ...
>
> Parliament and the public cannot hope to call the government to account without an adequate knowledge of what is going on; nor can they hope to participate in the decision-making process and contribute their talents to the formation of policy and legislation if that process is hidden from view. Access laws operate on the premise that politically relevant information should be distributed as widely as possible …

Rights to state-held information are designed to improve the workings of government; to make it more effective, responsive and accountable. Consequently, while the ATIA recognizes a broad right of access ... it is important to have regard to the overarching purposes of the Act in determining whether an exemption to that general right should be granted.

When the ATIPP Act was passed in 1994, no one could have predicted that information would have become so valuable a resource, nor that so much information could be stored so cheaply or manipulated so easily. The paperless office is now a reality and more and more government information is being stored electronically. Email is the primary way government employees communicate with each other and with those outside of government. The IT world we live and work in is not something that could be contemplated in 1994 when the Act was passed. And while the principals of the act continue to address the underlying purpose of contributing to the openness and accountability of public bodies, it is time to consider a review of the Act to ensure that those principles can be achieved in the face of current technologies, to fill gaps that have been created by the emerging technologies, and with a view to ensuring its continuing effectiveness in the future. This is not to say that the Act needs to be completely revamped, but the time has come for a review.

It has been, and continues to be, a great privilege to serve the public in the areas of access to information and privacy protection. I would like to thank the legislative assembly for providing me with the opportunity to undertake this important work.

The ability to manage and effectively use information is a core skill that needs to be at the centre of any public sector education and training strategy.

Hon. John Reid, Former Information Commissioner of Canada

THE LEGISLATION

THE ACT

The Access to Information and Protection of Privacy Act (ATIPPA) of the Northwest Territories was passed by the legislative assembly in 1995 and came into effect on December 31st, 1996. It establishes the rules for the collection, use and disclosure of information about individuals by public bodies in the Northwest Territories. It also outlines the rules by which the public can obtain access to public records.

The Act creates the office of the Information and Privacy Commissioner (IPC) to provide for independent oversight of decisions made by public bodies in applying and complying with the provisions of the Act. When questions arise with respect to the implementation and interpretation of the Act the IPC is available to provide her opinion and recommendations with respect to how the Act should be interpreted and applied. The IPC is an independent officer of the Legislature and is appointed by the Commissioner of the Northwest Territories on the recommendation of the Legislative Assembly. She reports to the Legislative Assembly of the Northwest Territories, and makes an annual representation to the Standing Committee on Government Operations. As an independent officer, the IPC can be only be removed from office "for cause or incapacity" on the recommendation of the Legislative Assembly.

ACCESS TO INFORMATION

The Act provides the public with a process to obtain access to most records in the possession or control of the 12 departments of the Government of the Northwest Territories and 26 other public bodies. Subject to a limited number of specific exceptions, the public has right to any record held by a public body. The specific and limited ex-

ceptions to the right to access function to protect individual privacy rights, to allow elected representatives to research and develop policy and the government to run the "business" of government. The Supreme Court of Canada has clearly held that exemptions to disclosure provided for in access to information legislation should be narrowly interpreted so as to allow the greatest possible access to government records.

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

To obtain a record from a public body, a request must be made in writing and delivered to the public body from whom the information is sought. When a request for information is received, the public body has 30 days to identify all of the records which are responsive to the request, review them to determine if there are any records or parts of records which are protected from disclosure under the Act and disclose them to the Applicant. The public body must endeavor to provide the applicant with as much of the requested information as possible, while at the same time respecting the limited exceptions to disclosure specified in the Act.

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.

In terms of the access to information function, the role of the Information and Privacy Commissioner is to provide an independent, non-partisan oversight of decisions made by public bodies in the Northwest Territories in relation to requests made under the Access to Information and Protection of Privacy Act for access to information by reviewing responses provided and making comments and recommendations.

When the Information and Privacy Commissioner receives a Request for Review, she will take steps to determine what records are involved and obtain an explanation from the public body as to the reasons for their decisions. In most cases, the Commissioner will receive a copy of the responsive documents from the public body involved and will review the records in dispute. The IPC will consider the responses received and provide the public body and the Applicant with a report and recommendations. The IPC generally does not have any power to make binding orders, but she is required to make recommendations. The head of the public body must then make a final decision as to how the government will deal with the matter.

If, in the end, the person seeking the information is not satisfied with the decision made by the head of the public body, they may apply to the Supreme Court of the Northwest Territories for a final determination of the matter.

PROTECTION OF PRIVACY

By its very nature, government collects and retains significant amounts of information about individuals - from medical and educational records to driving and financial information. Any time an individual interacts with a government agency, information is likely collected and retained. Part II of the Access to Information and Protection of Privacy Act establishes the rules about how public bodies can collect personal information, how they can use it once it has been collected and how and when they can disclose it to others.

The Act requires public bodies to ensure that they maintain adequate security measures to ensure that the personal information which they collect cannot be accessed by unauthorized personnel. This Part of the Act also provides the mechanism for individuals to be able to ask the government to make corrections to their own personal information when they believe that an error has been made.

Every person has the right to ask for information about themselves. If an individual finds information about themselves on a government record which they feel is misleading or incorrect, a request in writing may be made to correct the error. Even if the public body does not agree to change the information, a notation must still be made on the file that the individual has requested the correction.

The Act also provides a mechanism for the review of complaints where someone feels that their personal information has been improperly collected, used, or disclosed. Such complaints are submitted to the Information and Privacy Commissioner who will investigate the allegations to determine whether the complaint is well founded or not. In most cases, whether or not the complaint is well founded, the Information and Privacy Commissioner will provide a report and give the public body suggestions as to how to improve policies and procedures to improve privacy protections and avoid future breaches. The public body must respond to the recommendations made, but there is no further appeal available to the Complainant from the public body's decision on a privacy complaint.

Perhaps without a democracy, the transparency regime would never have blossomed, but also without the failures of this democratic system, the motivation among the people to formalize such a regime might not have been there.

Shehkar Singh, Founder member and former convener of the National Campaign for People's Right to Information (NCPRI), India

THE YEAR IN REVIEW

The fiscal year 2011/2012 was a busy one for the Information and Privacy Commissioner. In the 12 months between April 1, 2011 and March 31, 2012, the Information and Privacy Commissioner opened 27 files, up 35% from the previous year. The files can be divided into a number of categories:

a)	Breach of Privacy Complaints	5
b)	Access to Information Review Requests	10
c)	Requests for Comment on pending legislation or government program	5
d)	Privacy Complaints - Municipalities	2
e)	Request for Review - Fee Assessment	3
e)	Privacy Complaint re Private Sector Employer	1
f)	Administrative	1

Two of these files were closed without a formal recommendation being made because the Applicant abandoned his or her request before providing the Information and Privacy Commissioner with all of the information necessary to complete the review. In these cases, the Applicants were given a number of opportunities to perfect the Request for Review but failed to do so.

Two files involved privacy complaints against municipalities and were, therefore, outside of the formal jurisdiction of the Information and Privacy Commissioner. In each of these cases, the Information and Privacy Commissioner attempted to engage the

municipality in a discussion about the protection of privacy of employee information, but the municipality pointedly refused to engage in that discussion.

Seven of the matters considered by the Information and Privacy Commissioner involved the Department of Justice, including all three of the Fee Assessment reviews. It should be noted that all of these complaints arose out of an employee relations matter involving three employees. The Beaufort Delta Health and Social Services Authority were involved in three of the privacy complaints and Yellowknife Health and Social Services Authority were the public bodies involved in the other privacy complaints. Other public bodies which had matters before the Information and Privacy Commissioner included Environment and Natural Resources (2 matters), Human Resources (1 matter), Executive (1 matter), and Industry Tourism and Investment (1 matter).

Ten Review Recommendations were issued by the office of the Information and Privacy Commissioner in 2011/12.

The Act's basic purpose reflects a general philosophy of full disclosure unless information is exempted under clearly delineated statutory language. There are specific exemptions from disclosure set forth in the Act, but these limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act.... The Act's broad provisions for disclosure, coupled with specific exemptions, prescribe the "balance" struck between an individual's right to privacy and the basic policy of opening agency records and action to public scrutiny.

Tallis J.A., General Motors Acceptance Corp. of Canada v. Saskatchewan Government Insurance *(Sask.C.A.), [1993] S.J. No. 301, p. 5*

REVIEW RECOMMENDATIONS

REVIEW RECOMMENDATION 11-095

This review was requested by a news reporter. He was seeking access to a historical letter written by the then Minister of Education for the Northwest Territories to senior education officials in the Baffin Educational District (now in Nunavut). The subject of the letter, written more than 20 years ago, was how the Education District had dealt with complaints about former teacher, Edward Horne, who had been arrested on a number of sexual abuse charges and who was subsequently convicted on a large number of charges. While the letter had been referred to in court documents, the Nunavut Court of Justice had determined that it should be sealed because it had been provided in the context of pre-trial discovery and so was subject to the implied undertaking rule.

The public body provided a copy of the letter, heavily redacted, with a line by line explanation outlining why the severed portions of the letter had been refused. The public body cited Section 20 (1) (disclosure harmful to law enforcement), Section 21 (disclosure harmful to individual safety), and Section 23 (disclosure prohibited as a breach of third party personal information) for their refusal to disclose.

This was the second time that a member of the press had requested a copy of the same record. The issue was fully dealt with in Recommendation #10-192 and the recommendations in this case were the same. Specifically the recommendations were:

1. With respect to the claim that the disclosure of the letter was harmful to individual safety, (section 21), although Mr. Horne's time in the north obviously resulted in many victims and those victims continued

to suffer many years later, the public body did not provide sufficient evidence upon which one could conclude that the disclosure of the specific information contained in the letter could be "reasonably expected" to lead to further harm. For this section to apply, the public body would have to provide much more direct and cogent evidence of the possible harm and the expectation that it might occur.

2. With respect to the claim that there was a reasonable possibility that disclosure of portions of the letter would deprive a person (in this case the Government of the Northwest Territories) of the right to a fair trial or impartial adjudication, this exemption was intended to apply to individuals dealing with criminal or quasi-criminal matters before the court, not to protect the Government itself from disclosing information that might be the subject of pending civil litigation, particularly where there was nothing to support the allegation that the disclosure might have the stated effect.

3. Finally, with respect to the claim that the disclosure would constitute an unreasonable invasion of the personal privacy of third parties (Section 23), I concluded that there was, in fact, a good deal of personal information about third parties, including comments about the job performance of identifiable individuals and identifiable individuals working collectively and that these portions of the letter were protected from disclosure pursuant to Section 23(2)(g). I also concluded, however, that this did not justify the extent of editing done to the letter before it was provided to the Applicant.

I recommended the disclosure of large parts of the letter. The recommendations were, for the most part, accepted.

RECOMMENDATION 11-096

This matter came before the Information and Privacy Commissioner in the wake of a series of news reports about medical records being faxed to the wrong places. The Complainant in this case was concerned about messages being left on his family's home answering machine containing medical details about patients of the Yellowknife Health and Social Services Authority. The Complainant indicated that the last four digits of his home telephone number were the same as those belonging to a Yellowknife medical clinic. The first three digits were different. For a number of years, the Complainant had been receiving calls, almost on a daily basis, which were meant for the clinic. The Complainant advised that while many of the messages were from patients, there were also a significant number of messages being left by community health centers, doctors and their offices, as well as the R.C.M.P., sometimes with quite detailed information about patient and patient health. These messages were left on the Complainant's answering machine notwithstanding the fact that the machine clearly indicated that the caller had "reached the home of .....".

In making my recommendations, I observed that this was a system wide issue, not one that could be addressed solely by Yellowknife Health and Social Services Authority. That organization, in fact, was doing nothing wrong. However, every health authority and medical care provider in the Northwest Territories that is subject to the Access to Information and Protection of Privacy Act needed to be more aware of when they left messages and what those messages contain.

I recommended that there be a system wide written policy throughout the Northwest Territories and applicable to all medical health workers which addresses, at a minimum,

a) when it is and when it is not appropriate to leave a voice mail

b) when a voice mail message is left, what kind of information is and is not appropriate in the content of the voice mail

I further recommended that the policy must be made known to everyone working the government's health care sector and it's existence must be promoted and repeated so as to ensure that the importance of following the policy is reinforced.

The recommendations were accepted.

RECOMMENDATION 11-097

The Applicant in this case was seeking correspondence relating to a particular government project which he had been involved with as a contractor. The Applicant had agreed that he did not need to receive copies of records where he had been included in the distribution list, because those were records he already had in his possession.

Approximately 5000 records were identified as being responsive to the request. The Applicant had received a good number of records, many of which were highly edited. There were also a large number of the records which the public body refused to disclose completely. The Applicant asked my office to review the response.

This review focused on the use of email for communication. Almost all of the records identified as being responsive to the Request for Information were found in email communications, many of which jumped from subject to subject and were widely copied and shared and many of which contained multiple emails in an “email conversation”.

The public body was relying mainly on two sections of the Act to justify the exclusion of most of the information to which access was denied - section 14 which gives public bodies a discretion to refuse disclosure where the disclosure could reasonably be expected to reveal consultations or deliberations involving officers or employees of a public body, and section 15 which gives public bodies the discretion to refuse disclosure where the information is subject to any type of privilege available at law, including solicitor-client privilege. However, the public body had also redacted huge portions of the responsive records, claiming simply that they were "non-responsive" either because the Applicant had been included in the distribution list and, therefore, was already in possession of the record or because there had been a change in topic somewhere within the email chain, or several issues were discussed in one email.

In reviewing this matter, I reviewed each record, line by line and provided specific recommendations. Most of the recommendations were based on the following observations:

a) where a discretion is granted, the discretion must be exercised in a way that makes it clear that the discretion has been exercised - it requires some explanation to be given of the considerations that went into the exercise of that discretion. The scheme of the Act and the force of case law requires that the default position should always be disclosure and that the discretion to refuse disclosure should be exercised sparingly.

b) in applying section 14 (consultation or deliberations of officers or employees), I adopted the position set out in an early decision of the Alberta Information and Privacy Commissioner. In order to qualify for an exemption, the information must be:

(i) sought or expected, or be part of the responsibility of a person by virtue of that person's position,

(ii) directed toward taking an action, and

(iii) made to someone who can take or implement the action.

c) in applying section 15 (solicitor/client privilege), I used the test set out by the Supreme Court of Canada in *Canada v. Solosky* [1980] 1 S.C.R. 821 where Justice Dickson held that

… privilege can only be claimed document by document, with each document being required to meet the criteria for the privilege--(i) a communication between solicitor and client; (ii) which entails the seeking or giving of legal advice; and (iii) which is intended to be confidential by the parties.

d) a record is either responsive or it is not. One of the cautions about using e-mail as the main mode of communications is that ALL e-mails in a chain become part of "the record". The record cannot be chopped up into little bits, some of which is "responsive" to the request and some of which is not. Once identified as being a responsive record, the only reason that parts of the record might be severed is if those sections fall within one of the limited exemptions provided for in the Act. They can not be severed simply because they appear to be "off topic".

e) although the Applicant did not want to receive extra records where he was included in the distribution list for the email, there was no reason to redact these portions of the record when they were included in a page that was being otherwise being disclosed. Leaving these e-mails visible did not in any way add to the Applicant's costs because the page is already being provided and in many cases, leaving those portions of

the email intact would give context to the remainder of the record, which was important to understanding the entire conversation.

The Review report contained a total of 494 recommendations, based on a line by line, page by page review of the records. The recommendations were, for the most part, accepted. Those recommendations which were not accepted were mostly where the exemption relied on was solicitor/client privilege, where my interpretation and the public body's interpretation of the content of the emails differed.

RECOMMENDATION 11-098

In this case, the Applicant was seeking access to the minutes of the meeting of a "Mortality and Morbidity Committee" (M & M Committee) from the Stanton Territorial Health Authority in which the death of a family member had been discussed. The public body refused to disclose the record, claiming that the Evidence Act created a statutory prohibition preventing the disclosure of matters addressed by the Committee and documentation prepared by the Committee. Furthermore, the public body argued that there is a common law privilege that attaches to confidential communications. They point out that the members of the M &M Committee participate in the Committee under the expectation and assurance that its proceedings will remain confidential. They say that the guarantee of confidentiality is essential to the full and frank exchange of opinion that is needed to achieve the M & M Committee's goal of improving the quality of patient care.

In analyzing this request, I considered the case of *Steep v. Scott*, 2002 CanLII 53248 from the Ontario Superior Court in which Justice Egan discussed the application of a common law privilege to "quality assurance reports" or "peer review evaluations" of a hospital. At paragraph 5 of that decision, he states:

The four conditions necessary to establish common law privilege were first articulated by Wigmore and subsequently adopted by the Supreme Court of Canada in *Slavutych v. Baker* (1975)[1976] 1 S.C.R. 254 at p. 260, 55 D.L.R. (3d) 244 as follows:

1. The communications must originate in a confidence that they will not be disclosed;
2. This element of confidentiality must be essential to the full and satisfactory maintenance of the relationship between the parties;
3. The relation must be one which in the opinion of the community ought to be sedulously fostered;
4. The injury that would inure to the relation by the disclosure of the communications must be greater than the benefit thereby gained for the correct disposal of litigation

Having had the benefit of being able to review the record being requested, and using the analysis set out in the Ontario case, I was not satisfied that the record met the criteria for a common law privilege . In the Steep case, the records in question involved a detailed report prepared by a hospital employee outlining the facts and circumstances about a particular case after a review of the hospital records, interviews with medical personnel and a review of other correspondence. In this review, however, the record was a one page record of minutes which provided minimal detail with respect to the matter in issue. There was nothing in the record that would reveal any details of the incident or of the nature of the discussion that took place. If the record had contained more detail, statements made, specific conclusions reached, or recommendations for change, it is far more likely that the privilege would have applied, but, on

the facts of this case, the existence of the privilege had not been established. I recommended that the record be disclosed.

My recommendation in this case was not followed.

REVIEW RECOMMENDATION 11-099

In this case, a request had been made for "total billings for legal aid work by each law firm and sole practitioner for 2009-2010 fiscal year". Because of the nature of the information being sought, the public body advised the third parties involved that they were considering disclosing the information being requested, including the names of lawyers/law firms who had billed the Legal Services Board of the Northwest Territories during that fiscal year, along with the aggregate total of the amount paid to each of those lawyer/law firms. The Applicant in this case was one of those third parties and he objected to the disclosure of the information.

The third party was concerned about his competitive position. His contract was up for renewal and he was concerned that the disclosure of the amount of money he received from the contract would give his competitors an advantage over him. He was also concerned that the disclosure of the information could negatively affect his competitive position when bidding on similar contracts in other jurisdictions. In the circumstances, the onus fell on the Applicant to establish that the disclosure of the information could be "reasonably expected" to prejudice his competitive position and/or result in an undue financial loss.

In order for a Third Party to successfully prevent the release of information under section 24(1) (c), he needs to show only that there is a reasonable expectation that there is a reasonable expectation of probable harm should the information be disclosed.

The potential harm must be significant and the evidence must involve more than speculation and more than just a possibility of harm.

In this case, the third party was unable to convince me that the disclosure of the information requested would result in harm, particularly because the information which the public body proposed to disclose was aggregate information only which did not reveal any specific information about the terms or the conditions of the contract. I recommended that the records be disclosed.

My recommendations were accepted.

REVIEW RECOMMENDATION 11-100

An employee of the Beaufort-Delta Divisional Education Council (BDEC) requested copies of emails sent by certain other employees of the BDEC from BDEC computer equipment and addressed to a number of individuals employed both inside BDEC and elsewhere in which the content included comments about the Applicant.

The public body in this case failed to respond to the Applicant's first three requests for the information in question. It was only after the third request that the Applicant sought a review of the matter. This was more than 10 months after the first request for information had been made. When I first wrote to the public body, they did respond to my correspondence, but in doing so indicated that they needed to consult third parties as required by the Act. Nearly four months later, the public body finally responded to the Applicant, providing him with three pages of records, but those pages were significantly edited. No explanation was provided for the edits or the refusals. At this point, the Applicant renewed his request for review of the actual response

received. He was not satisfied that he had received all of the responsive records and he was not happy with the way in which the records had been edited.

Despite my request for a rapid response to the review process in light of the already existing delays, the public body again failed to respond to the review process until several requests from my office and two more months had elapsed. When they did respond, they acknowledged that they had, in fact, sent the Applicant the wrong set of edited records. They did not advise whether they had since forwarded him a corrected version.

This file was a study in how not to process an access to information request. It took more than two years for the Applicant to receive three pages, which were poorly edited. Most of the recommendations made in this case, therefore, were aimed at improving the public body's approach to Access to Information request.

The public body chose not to accept most of the recommendations made. They did agree to provide training to their staff in responding to ATIPP matters and to provide the Applicant with an apology for the manner in which they dealt with the access request. They accepted one substantive recommendation with respect to the disclosure provided to the Applicant, but rejected all other substantive recommendations made. It should be noted, as well, that the public body failed to respond to my recommendations within 30 days as required by the Act. It took not one, but two additional reminders from my office before that response was provided.

REVIEW RECOMMENDATION 11-101

In this case, a company requested information with respect to a particular Request for Proposals, including :

a) the total point scores for each supplier who submitted a tender;

b) point scores for each criteria on which each supplier was assessed;

c) proposals (in full) from each successful supplier;

d) rates offered by each supplier for the term of the standing offer;

e) annual spending per supplier.

The public body responded to the request, providing only the records in parts (a) and (e) of the request for information and the records in relation to the Applicant's own proposal. The public body relied on section 24(1), for their refusal to provide the remaining records requested which provides that a public body must refuse to disclose

a) the trade secrets of a third party,

b) any financial, commercial, scientific, technical or labour relations information obtained in confidence, that is of a confidential nature and was supplied by a third party in compliance with a lawful requirement; or

c) information, the disclosure of which could reasonably be expected to result in undue financial loss or gain to any person, prejudice the competitive position of a third party, interfere with contractual or other negotiations of a third party, or result in similar information not being supplied to a public body;

In doing the review, I did a page by page review of the records and made recommendations to the public body with respect to which of the records I felt should have been disclosed. In particular, I agreed that some of the information that had been withheld was the proprietary information of third party. However, there were other items that had been severed which contained nothing which would provide a reader with any

substantive information about the business practices of the third parties, nor was the information provided by the third parties. All that these records did was to provide a numerical comparison of how each of the proponents fared on each of the rating criteria. These records I recommended be disclosed.

My recommendations were accepted.

REVIEW RECOMMENDATION 11-102

The Applicant in this case asked me to review a decision by the Department of Human Resources not to disclose information he had requested in relation to his job interview for a specific position within a public body. For the most part, the Applicant was seeking information only about his own candidacy for the position. The public body disclosed a number of records, but withheld access to others and provided only redacted copies of several more. The public body relied on sections 23 (personal information), 22 (evaluative or opinion material compiled for employment purposes) and 3 (test questions) to justify their refusal to disclose certain records or parts of records.

In most respects, I agreed with the public body in terms of the information which had been redacted from the response provided to the Applicant. However, I disagreed with their application of Section 22. This section provides that:

> The head of a public body may refuse to disclose to an applicant personal information that is evaluative or opinion material compiled solely for the purpose of determining the applicant's suitability, eligibility or qualifications for employment or for the awarding of government contracts or other benefits when the information **has been provided to the public body**, explicitly or implicitly, in confidence. (Emphasis added)

The public body argued that the answers provided and rating given to each candidate for the position was "evaluative or opinion evidence" and was therefore protected by section 22. I pointed out, however, that section 22 contemplates that only information "provided to" the public body was protected from disclosure pursuant to section 22 and in this case, the information that the public body sought to protect was information created by the public body.

I also recommended that the public body disclose the questions the candidates were asked in the interview. The pubic body took the position, however, that these were outside of the scope of the Act, being "questions that are to be used on an examination or test". Section 3 of the Act takes such questions outside of the scope of the Act altogether. I disagreed that an interview process qualified as an examination or a test and recommended the questions be disclosed. I further recommended that the comments of the interviewers and the Applicant's own personal rating be disclosed.

The public body declined to follow my recommendation with respect to the disclosure of the answers given and the ratings assessed to each candidate in the interview , taking the position that Section 22, despite the clear wording in the Act, included "evaluations" produced by a GNWT staffing committee. The public body also refused to follow my recommendation with respect to the disclosure of the interview questions, taking the position that revealing the contents of the interview questions may affect the interview process by giving some candidates an unfair advantage over other candidates.

REVIEW RECOMMENDATION 12-103

This recommendation was issued in response to three separate, but related, requests for information. Each of the three Applicants, all employees of the same public body, requested information in relation to an investigation which was done in their work-

place over a period of five months. They were also seeking all written e-mail and other written materials between certain individuals within the workplace in relation to the issues raised. The request made by each of the three Applicants was virtually identical, but for the fact that they were each seeking only information which related to them personally.

In each case, the Applicants received letters informing them that their request would take longer than the 30 days normally allowed for a public body to respond to a Request for Information and that their response would be provided within 90 days of the initial request. At the end of that 90 day period, the public body sent each of the Applicants a second letter extending the response period a further 90 days. Each of the Applicants asked me to review the extensions of time. It should be noted that it wasn't until well into the second extension that the public body also provided the Applicants with significant fee estimates. This tactic served to further delay the response because under the scheme of the Act, when a fee estimate is provided, further work on responding to the access request is to cease until a deposit of half of the fee estimate, along with a commitment to pay the balance, is received. At the very latest, that fee estimate should have been provided to the Applicants at the time that the second extension was taken. By the time the Applicant's received the fee estimates, the public body had had their requests for more than four months.

The Access to Information and Protection of Privacy Act provides that public bodies must respond to an Access to Information request within 30 days unless that time period is extended pursuant to section 11. Section 11 allows a public body to extend the response time “for a reasonable period of time” where a large number of records is requested or must be searched to identify the requested record and meeting the time limit would unreasonably interfere with the operations of the public body.

The public body indicated that when they did their preliminary assessment of the requests, they determined that the volume of records requested was significant. They

also determined that the ATIPP Coordinator who would normally have addressed the request was in a conflict of interest and it was going to be necessary to have someone else within the department deal with the request. As a result, the public body sent the first extension letter to each of the Applicants advising them that their response would be delayed. As they got further into the processing of the requests, they identified a much larger volume of records than they had anticipated, which resulted in additional searching and handling to identify all of the responsive records. As a result, they sent the second letter extending the time further to a date approximately 5 months from the date of the original applications.

The issues boiled down to two:

a) were the extensions of time necessary because of the large number of records requested or to be searched such that meeting the time limit would unreasonably interfere with the operations of the public body;

b) was the length of the extension of time "reasonable"

I determined, based on the information about the records involved, that the public body had, in fact, met the first criteria allowing them to extend the time - there were a large number of records and meeting the time limit would have unreasonably interfered with the operations of the public body. I was not satisfied, however, that five months from the date of the application was a “reasonable” period of time. Furthermore, there is nothing in the Act that allows for an extension of an extension. The Act allows for one extension, not multiple ones.

I recommended:

a) that because of the delays, the public body waive any fee applicable to these Requests for Information;

b) that the public body provide the department's response to each of the three Applicants within 10 days of my recommendations;

c) if this department did not have redaction software to assist in the re view and processing of ATIPP requests, that it invest in such software forthwith so as to avoid unreasonable delays in responding to access requests in the future;

d) that the public body take steps to ensure that there is more than one person within the department who has the ongoing expertise and ability to deal with Access to Information requests.

My recommendations were essentially rejected. The public body refused to consider a fee reduction. Furthermore, by the time that the review recommendations were made, they said that they had provided the Applicants with responses to "modified requests" received from the Applicants. They felt that they had both the software and the manpower required to meet their obligations under the Act in most cases. They felt that this particular case was unique in its circumstances, which created the delay in responding. No further comment was provided with respect to whether or not they felt that the delay in responding in this matter was unacceptable.

REVIEW RECOMMENDATION 12-104

This review was initiated by an employee of Yellowknife Health and Social Services Authority (YHSSA) who was concerned about the lack of protection of personal health information within the electronic medical record (EMR) used by the Authority in its two Yellowknife primary care clinics. It was the Complainant's assessment that the EMR had been implemented without having first addressed privacy issues and that this, generally, had dramatically increased the risk of inappropriate use and/or disclosure of very sensitive health information because the number of people who had easy and apparently unmonitored access are greater and the ease of access is increased

because accessing a computer file can be done more discretely than pulling a physical file.

The EMR system operated by YHSSA is currently used in both Yellowknife clinic sites. It does not appear to be "interoperable" between the two sites such that someone in Clinic A can access the records of a patient who has seen a doctor in Clinic B, but it appears that staff (other than practitioners) rotate between the two clinics so that the number of people who have access to information in the system is about 150 people.

In undertaking this review, I learned a good deal about the EMR system which is in use by the Yellowknife Health and Social Services Authority. In particular, I learned that:

a) the system is not interoperable between the two primary care clinics, but the staff of the two clinics rotate so that there are a total of nearly 150 people who have some degree of access to the information in the system, including 5 mental health/addictions counselors, 8 administrative assistants, 18 clinic assistants, 8 billing clerks, 12 LPN's, 24 RN's, 6 managers, 4 records clerks, 1 quality risk management co-ordinator, 2 diabetes educators, 1 dietician, 1 medical social worker, 54 medical practitioners and 4 IT department employees.

b) each of these employees has received training in the use of the system, including a briefing about confidentiality and what constitutes appropriate access. In addition, all employees sign a confidentiality agreement when hired.

c) access to the system is controlled by the use of individual and unique user names and passwords. To log on to the EMR the user must first

log on to the YHSSA network, which is also username/password protected. It is not possible to access the system outside of the Yellow knife Health and Social Services' network.

d) individual sessions are "timed out" after a set period of inactivity;

e) access to the system is controlled by a "role based access" paradigm. "Roles" are defined by an employee's job description so that, for example, a physician may have access to the entire record, but the receptionist can only see more limited information about the patient (name, address, medical complaint, medication);

f) it is possible to "lock down" a patient's information such that it is available only to the employee who created the record, though this function is not widely used as it is considered to be counter to the core purposes of the EMR, which is the effective sharing of information to support the provision of comprehensive collaborative health care;

g) when an employee leaves the employ of YHSSA, revocation of access to the EMR system is part of the standard closure procedure;

h) the EMR itself is designed with "robust" audit functionality that records the action and identity of the user every time the system is accessed. This enables the review of concerning cases should they arise and al lows for the establishment of a routine auditing protocol. At the time of it's response (July, 2011) YHSSA indicated that they were "in the process" of implementing a routine EMR auditing process

i) unless precluded by legislation to the contrary, as in the case of child protection legislation, YHSSA takes the position that they, as a Health Authority, can share client information within the Authority as needed to facilitate their functions, without client consent.

One of the Complainant's specific concerns was that the "Encounter Record" found on the medical summary page of each individual's EMR is not only accessible, but

unavoidably so, by all 150 employees, regardless of the "role" they are assigned. This record is available when the medical summary is entered, when any client is booked for any reason and when any staff person makes a note about the visit. The information on this page can be quite sensitive - for example, the following things could well appear on this page:

- pregnancy
- substance abuse
- erectile dysfunction
- cancer screening
- therapeutic abortion
- psychiatric diagnosis - Bipolar Mood Disorder, Schizophrenia, Panic Attacks
- Sexually transmitted disease screening

In responding to this review, YHSSA decided that they would request a legal review of the EMR from their counsel. As part of that legal review, legal counsel conducted a Privacy Impact Assessment and made a number of recommendations which YHSSA have committed to addressing in their current and future planning. A copy of the report was provided to me as part of my review.

While the Report prepared by the public body's legal counsel quite correctly pointed out that Canadian courts have long recognized privacy rights in regard to one's personal information and that "informational privacy" has been defined as "the right of the individual to determine for himself when, how and to what extent he will release personal information about himself", there were significant differences between the author of the report and myself about what, exactly, that statement means. The public body took the position that there is an implied consent which allows YHSSA to use the personal health information of patients for any health care purpose within the

clinic once they have that information in their system, from counseling, to dietary issues, to obstetric or even social services matters. In my opinion, however, the current legislation allows the public body to use or disclose personal information gathered from the patient to only for the purpose of treating the specific presenting complaint. The current legislation allows a public body only to use personal information gathered for the purpose it was collected or for a use consistent with that purpose. Unless and until there is specific health privacy legislation, the Act, therefore allows information collected for the purpose of the patient's ear infection, for instance, to be used only to provide medical care relating to the ear infection, unless the patient provides his or her consent to a wider use. While I agreed that there is a certain parameter within which an implied consent to the use of personal health information can be assumed because it relates to the purpose for which the information was collected, that implied consent has a fairly narrow application under the Access to Information and Protection of Privacy Act.

Based on what I have discovered while doing this report, I expressed a number of concerns and raised a number of issues:

a) it appears that personal health information is not being compartmentalized but instead is being made generally available through all "departments" within the two major clinics and patients are unaware of how their information is being used and shared;

b) the "roles based" access to the EMR appears to have been defined so as to allow access to as much information as possible to as many people within the system as possible, but this does not comply with the spirit or intent of the Act, as it is currently written;

c) based on the information provided by the public body, it appeared that, at least to some extent, the technology was driving the solutions, rather than the other way around. In my opinion, the technology has to be able to respond to the needs of the system rather than letting the limitation of the technology define the privacy protections available;

d) I felt that a lot more work needs to be done to ensure that both the public and YHSSA fully understand both the benefits and risks inherent in an EMR. Yellowknife is a small town and inevitably at least one of the 150 people who have access to the system is going to have some connection to each patient who walks in the door, whether as a friend or a relative or a friend of a friend or relative. I also felt that it was wholly inappropriate that the Director of Social Programs has high level access to all YHSSA records, including counseling records;

e) the concept of "circle of care" needs to be defined and that definition should be created from the perspective of the patient, and within the limitations of the ATIPP Act, and not from the perspective of the efficiency of the system. At least until such time as the public is better educated about the system, YHSSA needs to find ways to protect personal health information "between departments" such that information collected for the purpose of mending the broken leg, for instance, is not available to the people engaged in counseling services.

f) the EMR system appears to offer only an "all or nothing" approach to the masking of information. Either electronic medical information is available to everyone in the system (subject to their roles) or it is available only to the author. There is no option available that would allow only one or two people to be prohibited from accessing a patient record. As other jurisdictions have discovered, it is the curious employee who is most often the cause of a wrongful use or disclosure of personal information. There has to be some function which allows the system to

"lock out" certain individuals from certain files. Not only must the system have that functionality, the public has to be aware that the "lock outs" are possible so that they know to ask for them.

g) more than a year after the launch of the EMR in the two Yellowknife clinics, there is either no auditing being done, or the auditing being done is minimal and without any underlying protocols or policies in place.

A number of recommendations were made based on these concerns. While the specific recommendations made were, for the most part, accepted by the public body, YHSSA did not in any way acknowledge that their current interpretation of how they can use personal health information within the two primary health clinics is in any way inappropriate or in breach of the Access to Information and Protection of Privacy Act. Nor did they commit in any way to limit the interchange of personal health information within the clinics between “departments” or service areas.

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

- John Ralston Saul

LOOKING AHEAD

Recommendation #12-104 summarized above was, in my opinion, one of the most significant reports I have prepared since taking office. While Yellowknife Health and Social Services and all other publicly run health institutions I have worked with are clearly aware of privacy concerns and are genuinely doing their best to "follow the rules", the rules are not well defined and the privacy protections in the Act are simply not being complied with. In many of my previous review recommendations, I have addressed the need for health specific privacy legislation. I know that this legislation is in the works, but it has been almost five years and there is still no indication as to when the legislation might be introduced. This really must be made a priority. As was highlighted in the YHSSA report and recommendations, there is a clear need to have legislation that addresses the specific challenges of maintaining privacy of personal health information while at the same time recognizing that electronic records, properly managed, can significantly improve the provision of health services. Electronic medical records must recognize the patient's right "to determine for himself when, how and to what extent he will release personal information about himself". There is also an immediate need to begin educating the public about electronic records and health privacy. Before any new legislation is rolled out, there should be a significant, well publicized and widespread public consultation, not only to judge the public's acceptance of the proposed legislation, but also to begin the educational process that will be necessary to ensure that the public understands how the legislation will affect them personally.

On another front, I am receiving more and more letters from people who are concerned about the way in which municipal authorities are collecting, using or disclosing personal information. This year I received two complaints concerning a municipality's use and/or disclosure of employee's personal information. In each case, if the allegations made by the Complainants were true, and if the Access to Information and Protection of Privacy Act applied, the breaches would have been real and serious. I attempted to engage the municipality involved in a discussion about policies, guide-

lines or best practices, but received no response to my correspondence. With no access and privacy legislation applying to municipalities, there are no legislative constraints on NWT municipalities, notwithstanding the fact that they all collect and retain significant amounts of personal information about citizens and employees. There is no oversight and no recourse for citizens when information is improperly used. Nor are there any rules which allow citizens access to the information that municipalities create and collect. The three northern territories are the only remaining jurisdictions which do not have information and privacy legislation for municipalities. This is an accountability issue and a way must be found to make it happen.

Finally, the Access to Information and Protection of Privacy Act has now been in force for 15 years. As noted in my opening comments, while the principles behind the Act are still very appropriate, the world - in particular the ability to collect, retain and manipulate data - has changed in ways that could never have been contemplated in 1994. Most Canadian jurisdictions, including some whose legislation is newer than ours, have undertaken a general review of their Access and Privacy legislation to address new realities and to fix weaknesses and areas requiring clarification. There is a need to evolve as the world of information changes. The increasing ability to retain ever greater amounts of information should bring with it increasing vigilance. I would, therefore, recommend once again that a review of the Act be placed on the legislative agenda, with a view to looking at whether or not its provisions are adequate to meet the challenges of 21st century technologies and to addressing some of the issues which have been raised in my Annual Reports over the years.

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

- Lord Acton

NORTHWEST TERRITORIES INFORMATION AND PRIVACY COMMISSIONER

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

Le 28 septembre 2012

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

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

Monsieur,

J'ai l'honneur de déposer mon rapport annuel à l'Assemblée législative des Territoires du Nord-Ouest pour la période du 1er avril 2011 au 31 mars 2012.

Veuillez agréer, Monsieur, mes salutations les plus distinguées.

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

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

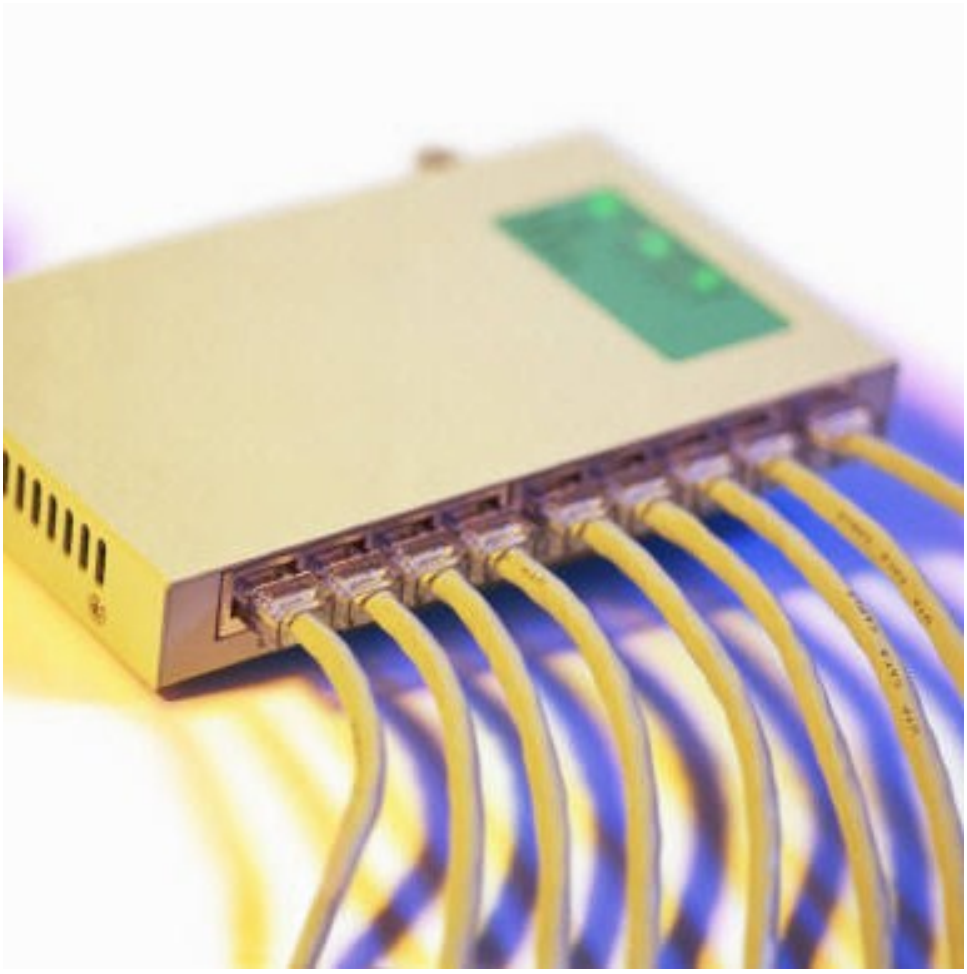


TABLE DES MATIÈRES

Message de la commissaire 44

La législation 47

La Loi 47

Accès à l'information 48

Protection de la vie privée 50

Bilan de l'année 52

Recommandations relatives aux demandes de révision 54

Recommandation relative à la demande de révision n° 11-095 54

Recommandation relative à la demande de révision n° 11-096 56

Recommandation relative à la demande de révision n° 11-097 57

Recommandation relative à la demande de révision n° 11-098 60

Recommandation relative à la demande de révision n° 11-099 62

Recommandation relative à la demande de révision n° 11-100 63

Recommandation relative à la demande de révision n° 11-101 65

Recommandation relative à la demande de révision n° 11-102 66

Recommandation relative à la demande de révision n° 12-103 68

Recommandation relative à la demande de révision n° 12-104 71

Regard vers l'avenir 79

MESSAGE DE LA COMMISSAIRE

Lorsque la *Loi sur l'accès à l'information et la protection de la vie privée* a été adoptée en 1994, nous vivions dans un monde différent. La *Loi* s'inscrivait dans un mouvement national vers la reconnaissance, dans la législation, du principe démocratique fondamental selon lequel le public a le droit de savoir ce que le gouvernement fait en son nom, ainsi que d'un mécanisme indépendant pour vérifier que les organismes publics suivent les règles. Parallèlement, la législation reconnaissait que les gouvernements détiennent beaucoup de renseignements personnels au sujet des citoyens et que ces derniers ont le droit d'avoir la certitude que ces renseignements sont en lieu sûr, protégés et utilisés aux seules fins pour lesquelles ils ont été colligés.

Dans l'intervalle, les changements ont été considérables. La prépondérance du courriel à titre de principale méthode de communication au travail, l'avènement des médias sociaux et les demandes, de la part du public, de méthodes plus efficaces d'échanges d'information et de données ouvertes, ont posé des défis qui ne sont que la pointe de l'iceberg. À bien des égards, les nouvelles technologies ont entraîné, chez le public, une plus grande conscience de son droit d'accès à l'information publique et une plus vive inquiétude quant à la capacité des organismes publics de maintenir la confidentialité des renseignements personnels. En dépit des technologies changeantes, toutefois, les principes sous-jacents de la *Loi* – posément et soigneusement rédigés – continuent de nous être utiles.

L'objet de la *Loi* est énoncé dans son tout premier article, comme suit :

1. La présente loi a pour objet d'accroître la responsabilité des organismes publics envers le public et de protéger la vie privée en :

(a) donnant au public un droit d'accès aux documents en la possession des organismes publics;

(b) donnant aux individus un droit d'accès aux renseignements personnels qui les concernent et que détiennent les organismes publics, ainsi que le droit de demander la correction de ces renseignements personnels;

(c) précisant des exceptions au droit d'accès;

(d) empêchant la collecte, l'usage ou la divulgation non autorisé de renseignements personnels par les organismes publics;

(e) prévoyant l'exercice de recours indépendants à l'égard des décisions prises en vertu de la présente loi.

Comme l'a souligné le juge La Forest de la Cour suprême du Canada en 1997, dans l'affaire Dagg c. Canada (Ministre des Finances) [1997], 2 R.C.S. 403, dans une déclaration qui s'est avérée des plus durables sur le but de la législation sur l'accès à l'information et la protection de la vie privée :

> La loi en matière d'accès à l'information a […] pour objet général de favoriser la démocratie, ce qu'elle fait de deux manières connexes. Elle aide à garantir, en premier lieu, que les citoyens possèdent l'information nécessaire pour participer utilement au processus démocratique, et, en second lieu, que les politiciens et bureaucrates demeurent comptables envers l'ensemble de la population. [...]
>
> Ni le Parlement ni le public ne sauraient espérer demander au gouvernement de rendre compte s'ils n'ont pas une connaissance suffisante de ce qui se passe; ils ne peuvent pas non plus espérer prendre part au processus decisionnel ni contribuer à l'établissement des politiques générales et des lois si ce

processus est tenu secret. […] Les lois sur l'accès à l'information présupposent que les renseignements pertinents sur le plan politique devraient faire l'objet d'une diffusion aussi large que raisonnablement possible. [...]

Les droits aux renseignements détenus par l'État visent à améliorer les rouages du gouvernement, de manière à le rendre plus efficace, plus réceptif et plus responsable. En conséquence, bien que la *Loi sur l'accès à l'information* reconnaisse un droit d'accès général [...], il importe de tenir compte de l'objectif général de cette loi pour déterminer s'il y a lieu de reconnaître une exception à ce droit général.

Lorsque la *Loi sur l'accès à l'information et la protection de la vie privée* a été adoptée en 1994, personne n'aurait pu prédire que l'information serait devenue une ressource aussi précieuse, ni qu'un volume d'information aussi important pourrait être conservé à si bon marché ou manipulé aussi aisément. Le bureau électronique est désormais une réalité. Un volume grandissant d'information gouvernementale est conservé sous forme électronique. Le courriel est la principale méthode des fonctionnaires pour communiquer entre eux et avec des personnes extérieures au gouvernement. L'univers dominé par les TI dans lequel nous vivons et travaillons n'aurait pas été envisageable en 1994 lors de l'adoption de la *Loi*. Et bien que les principes de la *Loi* continuent de soutenir l'objet sous-jacent de contribuer à la transparence et à la responsabilité des organismes publics, il est temps d'envisager une révision de celle-ci, pour veiller à ce que ces principes puissent être observés compte tenu des technologies actuelles, à combler les lacunes créées par les technologies émergentes et à s'assurer de son efficacité continue pour l'avenir. Il ne s'agit pas de faire une refonte complète de la *Loi*. Mais le temps est venu de la revoir.

Je me suis considérée privilégiée, et je continue de l'être, d'avoir servi le public en matière d'accès à l'information et de protection de la vie privée. J'aimerais remercier l'Assemblée législative de m'avoir donné la possibilité d'accomplir cette tâche importante.

LA LÉGISLATION

LA LOI

La *Loi sur l'accès à l'information et la protection de la vie privée* des Territoires du Nord-Ouest a été adoptée par l'Assemblée législative en 1995 et est entrée en vigueur le 31 décembre 1996. Elle définit les règles concernant la collecte, l'usage et la divulgation de renseignements sur les individus par les organismes publics des Territoires du Nord-Ouest. Elle décrit aussi les règles que doit suivre le public pour avoir accès aux documents publics.

La *Loi* crée le Commissariat à l'information et à la protection de la vie privée afin d'avoir un mécanisme indépendant de surveillance des décisions que prennent les organismes publics lorsqu'ils mettent en application et respectent les dispositions de la *Loi*. Lorsque surviennent des questions relatives à la mise en application et à l'interprétation de la *Loi*, la commissaire à l'information et à la protection de la vie privée donne son opinion et formule des recommandations sur la manière dont la *Loi* doit être interprétée et appliquée. La commissaire à l'information et à la protection de la vie privée est une représentante indépendante de la législature et est nommée par le commissaire des Territoires du Nord-Ouest, sur la recommandation de l'Assemblée législative. Elle relève de l'Assemblée législative des Territoires du Nord-Ouest et présente un rapport annuel au Comité permanent des opérations gouvernementales. En tant que représentante indépendante, elle ne peut être destituée que « pour un motif valable ou en raison de son empêchement » sur la recommandation de l'Assemblée législative.

ACCÈS À L'INFORMATION

La *Loi* fournit au public un processus lui permettant d'avoir accès à la plupart des documents en la possession ou relevant du gouvernement des Territoires du Nord-Ouest et des 26 autres organismes publics. Sous réserve d'un nombre limité d'exceptions particulières, le public a le droit d'accéder à tout document en la possession d'un organisme public. Ces exceptions particulières et d'un nombre limité au droit d'accès à l'information servent à protéger les droits concernant la vie privée des individus, à permettre aux représentants élus de rechercher et d'élaborer une politique et au gouvernement de mener les « affaires » publiques. La Cour suprême du Canada a clairement statué que les exceptions à la divulgation prévues dans la législation sur l'accès à l'information devraient être interprétées rigoureusement, pour allouer le plus grand accès possible aux documents gouvernementaux.

Toute personne, qu'elle vive aux Territoires du Nord-Ouest ou dans une autre région du monde, peut demander l'accès à un document gouvernemental. À moins que l'information demandée ne concerne les renseignements personnels du requérant lui-même, des droits de 25 dollars sont exigés. En cas de demandes concernant un nombre considérable de documents, des droits supplémentaires peuvent être exigés.

Pour obtenir un document d'un organisme public, il faut en faire la demande par écrit et l'acheminer à l'organisme public duquel on souhaite obtenir l'information. À la réception d'une demande d'accès à l'information, l'organisme public a 30 jours pour déterminer tous les documents éclairants pour la demande, les examiner pour déterminer s'ils ne devraient pas être divulgués, en tout ou en partie, en vertu de la *Loi* et les fournir au requérant. L'organisme public doit s'efforcer de fournir au requérant le plus de renseignements possible, tout en respectant les exceptions de divulgation limitées qui sont précisées dans la *Loi.*

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

Dans le cadre de son mandat sur l'accès à l'information, le rôle de la commissaire à l'information et à la protection de la vie privée est d'examiner, de manière indépendante et non partisane, les décisions prises par les organismes publics des Territoires du Nord-Ouest au sujet des demandes d'accès à l'information présentées en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*, en révisant les réponses fournies et en formulant des commentaires et des recommandations.

Lorsque la commissaire à l'information et à la protection de la vie privée reçoit une demande de révision, elle prend des mesures pour déterminer quels documents sont concernés et pour obtenir une explication de la part de l'organisme public, afin de connaître le motif de sa décision. Dans la plupart des cas, elle reçoit une copie des documents éclairants de l'organisme public concerné et revoit les documents en litige. Elle étudie les réponses reçues et achemine un rapport accompagné de recommandations à l'organisme public et au requérant. En règle générale, elle n'a pas le pouvoir d'émettre des ordonnances exécutoires, mais a l'obligation de formuler des recommandations. Le responsable de l'organisme public doit ensuite prendre une décision finale sur la manière dont le gouvernement traitera l'affaire.

Au bout du compte, si la personne qui voulait accéder à ces renseignements n'est pas satisfaite de la décision de ce responsable, son recours est de faire appel à la Cour suprême des Territoires du Nord-Ouest, qui tranchera définitivement la question.

PROTECTION DE LA VIE PRIVÉE

De par sa nature même, le gouvernement collige et conserve d'importants volumes de renseignements sur des individus, allant des dossiers médicaux et scolaires aux renseignements concernant la conduite automobile et les finances. Chaque fois qu'un individu traite avec un organisme gouvernemental, des renseignements sont probablement recueillis et conservés. La Partie II de la *Loi sur l'accès à l'information et la protection de la vie privée* décrit les règles que doivent respecter les organismes publics pour la collecte des renseignements personnels, la manière dont ces renseignements peuvent être utilisés lorsqu'ils ont été colligés, ainsi les modalités de la divulgation à des tiers.

La *Loi* exige que les organismes publics s'assurent de maintenir des mesures de sécurité adéquates pour veiller à ce que les renseignements personnels dont ils font la collecte ne puissent être consultés par le personnel non autorisé. Cette partie de la *Loi* stipule aussi le mécanisme selon lequel les individus peuvent demander au gouvernement d'apporter des corrections à leurs propres renseignements personnels lorsqu'ils estiment qu'une erreur a été commise.

Toute personne a le droit de demander des renseignements à son sujet. Si un individu découvre des renseignements qui le concernent dans un dossier gouvernemental et qu'il croit que ces renseignements sont trompeurs ou incorrects, il peut présenter une demande par écrit pour corriger l'erreur. Même si l'organisme public ne consent pas à changer les renseignements, une note doit être inscrite au dossier pour lequel l'individu a demandé une correction.

La *Loi* décrit aussi le mécanisme de révision des plaintes dans les cas où un individu estime que ses renseignements personnels ont été inadéquatement recueillis, utilisés ou divulgués. Ces plaintes sont présentées à la commissaire à l'information et à la protection de la vie privée, qui fait ensuite enquête sur les allégations, pour déterminer si une plainte donnée est fondée ou non. Que la plainte soit fondée ou non, dans la plupart des cas la commissaire produit un rapport et formule des suggestions d'amélioration des politiques et des procédures à l'organisme public, afin de rehausser les mécanismes de protection de la vie privée et d'éviter de futures atteintes à la vie privée. L'organisme public est tenu de répondre à ces recommandations, mais un plaignant ne dispose d'aucun autre recours contre la décision d'un organisme public au sujet d'une plainte pour atteinte à la vie privée.

Peut-être que sans démocratie, le régime de transparence n'aurait jamais prospéré, mais également sans les échecs de ce système démocratique, la motivation des personnes pour formaliser un tel régime n'aurait peut-être pas existé.

Shehkar Singh, membre fondateur et ancien responsable de la National Campaign for People's Right to Information (NCPRI) [Campagne nationale pour le droit de la population à l'information], Inde

BILAN DE L'ANNÉE

L'exercice 2011-2012 a été chargé pour la commissaire à l'information et à la protection de la vie privée. Au cours des 12 mois qui se sont écoulés du 1er avril 2011 au 31 mars 2012, elle a ouvert 27 dossiers, soit 35 % de plus que durant l'exercice précédent. Ils se répartissent dans les catégories suivantes :

Plaintes pour atteinte à la vie privée	5
Demandes de révision de décisions relatives à l'accès à l'information	10
Demandes de commentaires sur de nouvelles lois ou de nouveaux programmes du gouvernement	5
Plaintes pour atteinte à la vie privée – Municipalités	2
Demandes de révision – Évaluation des droits	3
Plainte pour atteinte à la vie privée – Employeur du secteur privé	1
Administration	1

Deux de ces dossiers ont été résolus sans formulation de recommandations officielles, parce que les requérants avaient abandonné leur demande avant d'avoir envoyé à la commissaire à l'information et à la protection de la vie privée l'ensemble de l'information pertinente pour achever la révision. Dans les deux cas, les requérants avaient eu plusieurs chances de compléter leur demande de révision mais ne l'ont pas fait.

Deux dossiers découlaient de plaintes pour atteinte à la vie privée contre des municipalités et n'étaient pas, par conséquent, du ressort officiel de la commissaire à l'information et à la protection de la vie privée. Dans les deux cas, cette dernière a tenté d'engager une discussion avec la municipalité concernée sur la protection du

caractère privé des renseignements sur les employés, mais la municipalité a catégoriquement refusé de participer à cette discussion.

Sept des dossiers examinés par la commissaire à l'information et à la protection de la vie privée mettaient en cause le ministère de la Justice, dont les trois demandes de révision des évaluations de droits. Il convient de souligner que ces plaintes découlaient toutes d'un problème de relations de travail mettant en cause trois employés. L'Administration des services de santé et des services sociaux de Beaufort-Delta était en cause dans trois des plaintes pour atteinte à la vie privée. L'Administration des services de santé et des services sociaux de Yellowknife était également l'un des organismes publics visés par des plaintes de cet ordre. Les autres organismes publics en cause dans les dossiers traités par la commissaire à l'information et à la protection de la vie privée étaient les ministères de l'Environnement et des Ressources naturelles (deux dossiers), des Ressources humaines (un dossier), de l'Exécutif (un dossier) et de l'Industrie, du Tourisme et de l'Investissement (un dossier).

Durant l'exercice 2011-2012, le Commissariat à l'accès à l'information et à la protection de la vie privée a formulé dix recommandations relatives à des demandes de révision de décisions.

La capacité de gérer et d'utiliser efficacement les renseignements est une compétence essentielle qui doit être au centre de toute stratégie d'éducation et de formation du secteur public.

M. John Reid, ancien Commissaire à l'information du Canada

RECOMMANDATIONS RELATIVES AUX DEMANDES DE RÉVISION

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION N^{O} 11-095

Cette demande de révision a été faite par un journaliste. Il voulait avoir accès à une lettre historique rédigée par le ministre de l'Éducation des Territoires du Nord-Ouest de l'époque, à l'intention des hauts fonctionnaires du district scolaire de Baffin (aujourd'hui, le Nunavut). L'objet de cette lettre, rédigée il y a plus de 20 ans, décrivait comment le district scolaire avait traité les plaintes contre un ancien enseignant, Edward Horne, qui avait été arrêté pour de nombreuses accusations d'agression sexuelle et avait été condamné par la suite pour de nombreuses infractions. Bien que les documents de tribunal aient mentionné la lettre, la Cour du Nunavut a décidé de la mettre sous scellé parce qu'elle avait été fournie dans le contexte du processus de communication préalable et, par conséquent, assujettie à la règle de l'engagement implicite.

L'organisme public a fourni une copie de la lettre considérablement élaguée, accompagnée d'explications juxtalinéaires décrivant pourquoi les portions supprimées n'étaient pas divulguées. Pour justifier son refus de divulguer la lettre intégrale, l'organisme public a invoqué le paragraphe 20 (1) (divulgation nuisible à l'exécution de la loi), l'article 21 (divulgation nuisible à la sécurité d'autrui) et l'article 23 (divulgation interdite car portant atteinte à la vie privée d'un tiers).

C'était la deuxième fois qu'un journaliste demandait une copie de ce document. Le dossier avait été entièrement réglé dans la recommandation relative à la demande de révision n^{o} 10-192 et les recommandations visant le présent dossier étaient analogues. Plus précisément, les recommandations formulées étaient les suivantes :

1. Pour ce qui est de l'allégation que la divulgation de la lettre serait nuisible à la sécurité d'autrui (article 21), bien que le passage de M. Horne dans le Nord ait manifestement fait de nombreuses victimes et que celles-ci ont continué de souffrir de nombreuses années plus tard, l'organisme public n'a pas présenté assez de preuves tangibles pour me permettre de conclure qu'on pouvait « vraisemblablement s'attendre » à ce que la divulgation de renseignements particuliers figurant dans la lettre puisse causer des préjudices supplémentaires. Pour que cet article soit applicable, l'organisme public aurait à fournir des preuves beaucoup plus directes et convaincantes des préjudices possibles et de la probabilité que ces derniers se matérialisent.

2. Pour ce qui est de l'allégation que la divulgation de parties de la lettre pourrait vraisemblablement priver une personne (dans ce cas, le gouvernement des Territoires du Nord-Ouest) de son droit à un procès équitable ou à un règlement impartial, il convient de souligner que cette exemption vise à protéger les individus qui se retrouvent devant la Cour pour des affaires criminelles ou quasi-criminelles, et non pas le gouvernement lui-même pour la divulgation d'information concernant une action civile en suspens, particulièrement lorsque rien ne soutient l'allégation que la divulgation aurait l'effet déclaré.

3. Enfin, concernant l'allégation que la divulgation constituerait une atteinte déraisonnable à la vie privée de tiers (article 23), j'ai conclu que la lettre comportait, de fait, une quantité appréciable de renseignements personnels de tiers, dont des commentaires sur le rendement professionnel d'individus identifiables et sur des individus identifiables travaillant ensemble, et que ces parties de la lettre étaient protégées contre la divulgation en vertu de l'alinéa 23(2)(g). J'ai également conclu, toutefois, que cela ne justifiait pas l'ampleur des suppressions apportées à la lettre avant son envoi au requérant.

J'ai recommandé la divulgation d'importantes portions de la lettre. Les recommandations ont été acceptées avec deux exceptions.

RECOMMANDATION RELATIVE À LA DEMANDE N^{O} 11-096

Cette demande m'a été présentée dans la foulée d'une série de nouvelles portant sur les dossiers médicaux qui étaient télécopiés aux mauvais endroits. Dans ce cas, le plaignant s'inquiétait de messages laissés sur son répondeur téléphonique à la maison comprenant des renseignements médicaux sur des patients de l'Administration des services de santé et des services sociaux de Yellowknife. Le plaignant a indiqué que les quatre derniers chiffres de son numéro de téléphone à la maison étaient les mêmes que ceux d'une clinique médicale de Yellowknife. Les trois premiers numéros étaient différents. Pendant plusieurs années, le plaignant a reçu des appels, presque quotidiennement, qui étaient destinés à la clinique. Le plaignant a indiqué que bien que plusieurs des messages venaient de patients, un grand nombre de messages étaient laissés par des centres de santé communautaire, des médecins et leurs bureaux ainsi que la GRC, parfois avec de l'information très détaillée sur un patient et son état de santé. Ces messages étaient laissés sur le répondeur du plaignant malgré le fait que le message du répondeur mentionnait clairement à la personne qui téléphonait : « Vous avez joint la résidence de… ».

En faisant mes recommandations, j'ai souligné qu'il s'agissait d'un problème à l'échelle du système, et non d'un problème devant être résolu seulement par l'Administration des services de santé et des services sociaux de Yellowknife. En réalité, cet organisme ne faisait rien de mal. Toutefois, toutes les administrations des services de santé et tous les fournisseurs de soins médicaux des Territoires du Nord-Ouest qui sont assujettis à la *Loi sur l'accès à l'information et la protection de la vie privée* doivent se montrer plus conscients du moment où ils laissent des messages et de la teneur de ceux-ci.

J'ai recommandé la rédaction d'une politique écrite à l'échelle du système partout aux Territoires du Nord-Ouest s'appliquant à tout le personnel médical et décrivant au moins :

a) à quel moment il est approprié de laisser un message vocal;

b) quel genre d'information est approprié et inapproprié dans la teneur d'un message vocal, lorsqu'on en laisse un.

J'ai de plus recommandé que l'on informe toute personne travaillant dans le secteur des soins de santé au gouvernement au sujet de la politique et que l'existence de celle-ci soit promue et répétée pour renforcer l'importance de respecter cette politique.

Les recommandations ont été acceptées.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION N^{O} 11-097

Dans ce cas, le requérant cherchait de la correspondance concernant un projet de gouvernement particulier auquel il avait participé à titre d'entrepreneur. Le requérant avait convenu qu'il n'avait pas besoin de recevoir de copies de documents pour lesquels il figurait dans la liste de distribution, car il s'agissait de documents qu'il avait déjà en sa possession.

On a déterminé environ 5 000 documents éclairants pour la demande. Le requérant avait reçu un bon nombre de documents, dont beaucoup avaient été fortement révisés. De plus, l'organisme public avait refusé de divulguer complètement un grand nombre des documents. Le requérant a demandé à mon bureau de revoir la réponse.

Cette révision portait sur l'utilisation du courriel pour la communication. On a découvert presque tous les documents considérés comme éclairants pour la demande d'information dans des communications par courriel dont beaucoup faisaient du coq-à-l'âne et étaient largement copiés et partagés et dont bon nombre contenaient plusieurs courriels dans une « conversation par courriel ».

L'organisme public invoquait principalement deux articles de la *Loi* pour justifier l'exclusion de la plupart des renseignements auxquels l'accès avait été refusé – l'article 14, qui accorde aux organismes publics le pouvoir discrétionnaire de refuser la divulgation dans le cas où la divulgation risquerait vraisemblablement de révéler des consultations ou des délibérations où sont concernés des cadres ou des employés d'un organisme public, et l'article 15, qui accorde aux organismes publics le pouvoir discrétionnaire de refuser la divulgation dans le cas où les renseignements sont protégés par tout genre de privilège d'ordre légal, y compris le privilège des communications entre client et avocat. Cependant, l'organisme public avait également supprimé une grande partie des documents éclairants, affirmant tout simplement qu'ils étaient « irrecevables », soit parce que le requérant figurait dans la liste de distribution et, par conséquent, était déjà en possession du document, soit parce que le sujet avait changé quelque part dans la chaîne de courriels ou que plusieurs sujets avaient été traités dans un courriel.

Dans la révision de cette affaire, j'ai examiné chaque document, ligne par ligne, et fourni des recommandations spécifiques. La plupart des recommandations se fondaient sur les observations suivantes :

a) Dans le cas où un pouvoir discrétionnaire est accordé, il doit être exercé de façon à faire savoir clairement qu'il a été exercé – il convient de donner une explication des considérations sur lesquelles avait reposé l'exercice de ce pouvoir discrétionnaire. L'esprit de la Loi et la jurisprudence stipulent que la solution par défaut devrait toujours être la divulgation et que le pouvoir discretionnaire de refuser la divulgation devrait être exercé modérément.

b) Aux fins de l'application de l'article 14 (consultation ou délibérations de cadres ou d'employés), j'ai adopté la position énoncée dans une décision préalable de la Commissaire à l'information et à la protection de la vie privée de l'Alberta. Pour pouvoir bénéficier d'une dérogation, les renseignements doivent être :

(i) recherchés ou attendus, ou faire partie de la responsabilité d'une personne en vertu de la position de cette personne,

(ii) orientés vers la prise de mesures,

(iii) mis à la disposition de quelqu'un qui peut prendre ou mettre en œuvre les mesures.

c) Aux fins de l'application de l'article 15 (privilège des communications entre client et avocat), j'ai utilisé le critère établi par la Cour suprême du Canada dans *Solosky c. La Reine* [1980] 1 R.C.S. 821 où le juge Dickson a conclu que :

> […] le privilège ne peut être invoqué que pour chaque document pris individuellement, et chacun doit répondre aux critères du privilège : (i) une communication entre un avocat et son client; (ii) qui comporte une consultation ou un avis juridiques; et (iii) que les parties considèrent de nature confidentielle.

d) Un document est éclairant ou il ne l'est pas. Une des mises en garde touchant l'utilisation du courriel comme principal mode de communication est que TOUS les courriels d'une chaîne font partie « du document ». Le document ne peut pas être découpé en petits morceaux, dont une partie est « éclairante » pour la demande et une partie ne l'est pas. Une fois qu'un document a été considéré comme éclairant, la seule raison pour laquelle des parties du document pourraient être séparées est le cas où ces parties relèvent d'une des dérogations particulières prévues par la *Loi.* Elles ne peuvent pas être séparées simplement parce qu'elles semblent être « hors sujet ».

e) Bien que le requérant ne voulait pas recevoir de documents supplémentaires pour lesquels il figurait dans la liste de distribution des courriels, il n'y avait aucune raison de supprimer ces parties du document alors qu'elles étaient incluses dans une page qui autrement était divulguée. Le fait de laisser ces courriels visibles n'a augmenté en aucune façon les dépens du requérant parce que la page est déjà fournie et que, dans de nombreux cas, le fait de laisser ces parties du courriel intactes fournirait un contexte au reste du document, ce qui était important pour comprendre la conversation entière.

Le rapport de révision contenait un total de 494 recommandations, fondées sur un examen juxtalinéaire, page par page des documents. Les recommandations ont été, pour la plupart, acceptées. Celles qui ne l'ont pas été concernaient le plus souvent des cas où la dérogation invoquée était le privilège des communications entre client et avocat, où mon interprétation et l'interprétation de l'organisme public du contenu des courriels différaient.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION N^{O} 11-098

Dans ce cas, le requérant demandait accès au procès-verbal d'une réunion d'un « Comité sur la mortalité et la morbidité » (le Comité) de l'Administration de santé territoriale Stanton durant laquelle le décès d'un membre de sa famille avait été discuté. L'organisme public a refusé de divulguer le document, alléguant que la *Loi sur la preuve au Canada* créait une interdiction fondée sur la législation prévenant la divulgation des dossiers traités et des documents rédigés par le Comité. De plus, l'organisme public a avancé qu'un privilège jurisprudentiel était rattaché aux communications confidentielles, soulignant que les membres du Comité y participaient en s'attendant en toute confiance à ce que les délibérations demeurent confidentielles. Il a déclaré que la garantie de confidentialité est essentielle au caractère franc et complet des échanges de points de vue sur les démarches que doit faire le Comité pour atteindre son but d'améliorer la qualité des soins administrés aux patients.

Lors de mon analyse de cette demande, j'ai tenu compte de l'affaire Steep c. Scott, 2002, CanLII 53248 de la Cour supérieure de l'Ontario, dans laquelle le juge Egan évoque l'application du privilège jurisprudentiel aux « rapport d'assurance de qualité » ou aux « évaluations par les pairs » émanant d'un hôpital. Au cinquième paragraphe de cette décision, il déclare :

Les quatre conditions nécessaires à l'établissement d'un privilège jurisprudentiel ont tout d'abord été définies par Wigmore et, par la suite, adoptées par la Cour suprême du Canada, dans Slavutych c. Baker et al. (1975)[1976] 1 R.C.S. 254, à la p. 260, 55 D.L.R. (3d) 244, comme suit :

1. Les communications doivent avoir été transmises confidentiellement avec l'assurance qu'elles ne seraient pas divulguées.

2. Le caractère confidentiel doit être un élément essentiel au maintien complet et satisfaisant des relations entre les parties.

3. Les relations doivent être de la nature de celles qui, selon l'opinion de la collectivité, doivent être entretenues assidûment.

4. Le préjudice permanent que subiraient les relations par la divulgation des communications doit être plus considérable que l'avantage à retirer d'une juste décision.

Comme j'avais eu la possibilité de consulter le document demandé, je n'étais pas convaincue qu'il satisfaisait au critère du privilège jurisprudentiel, en me fondant sur l'analyse de l'affaire de l'Ontario. Dans l'affaire Steep, les documents en question comportaient un rapport détaillé rédigé par un employé de l'hôpital et qui décrivait

les faits et circonstances entourant un cas particulier après un examen des dossiers de l'hôpital, des entrevues avec le personnel médical et un examen d'autre correspondance. Dans la présente révision, toutefois, le document consistait en une page de procès-verbal donnant des détails minimes sur la question dont il s'agissait. Rien n'y donnait de quelconques détails sur l'incident ou la nature de la discussion qui avait eu lieu. Si le document avait fait état de plus de détails, de déclarations effectuées, de conclusions particulières tirées ou de recommandations de changement, il est bien plus probable que le privilège jurisprudentiel aurait été pertinent mais, d'après les faits en l'espèce, l'existence de ce privilège n'avait pas été établie. J'ai recommandé de divulguer le document.

Dans ce cas, ma recommandation a été rejetée.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION N^{O} 11-099

Dans ce cas, on avait demandé « la facturation entière du travail d'aide juridique de chaque cabinet d'avocat et praticien exerçant seul pour l'exercice 2009-2010 ». À cause de la nature de l'information demandée, l'organisme public a informé les tiers concernés qu'il envisageait de divulguer l'information demandée, y compris le nom des avocats et cabinets d'avocats qui avaient présenté des factures à la Commission des services juridiques des Territoires du Nord-Ouest durant cet exercice financier, de même que le total général du montant versé à chacun. Le requérant était l'un de ces tiers et il s'est objecté à la divulgation de l'information.

Il s'inquiétait au sujet de sa compétitivité. Son contrat devait être renouvelé et il s'inquiétait du fait que la divulgation du montant qu'il avait reçu pour ce contrat donnerait un avantage à ses concurrents. Il s'inquiétait aussi du fait que la divulgation de l'information pourrait nuire à sa compétitivité lors de soumissions à des contrats semblables dans d'autres provinces et territoires. Dans ces circonstances, il lui

incombait d'établir que la divulgation de l'information « risquerait vraisemblablment » de porter préjudice à sa compétitivité ou d'entraîner une perte financière injustifiée.

Pour qu'un tiers parvienne à prévenir la divulgation en vertu de l'alinéa 24(1)(c), il lui suffit de démontrer qu'il pourrait s'attendre à une probabilité vraisemblable de préjudice s'il advenait que l'information soit divulguée. Le préjudice doit être important et la preuve ne doit pas reposer seulement sur des conjectures et une simple possibilité de préjudice.

Dans ce cas, le tiers n'est pas parvenu à me convaincre que la divulgation de l'information entraînerait un préjudice, particulièrement parce que l'information que l'organisme public se proposait de divulguer était des données globales ne révélant aucun renseignements précis sur les modalités du contrat. J'ai recommandé de divulguer les documents.

Mes recommandations ont été acceptées.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION N^{O} 11-100

Un employé du Conseil scolaire de division de Beaufort-Delta a demandé des copies de courriels envoyés par d'autres employés du Conseil à partir du matériel informatique du Conseil et adressés à plusieurs personnes employées au sein du Conseil et ailleurs dans lesquels le contenu comportait des commentaires sur le requérant.

Dans ce cas, l'organisme public a omis de répondre aux trois premières demandes du requérant pour l'information en question. Ce n'est qu'après la troisième demande que le requérant a exigé une révision de la question. Cela correspondait à plus de 10 mois après la première demande d'information. La première fois où j'ai écrit à l'organisme

public, j'ai reçu réponse à ma lettre, mais l'organisme m'annonçait qu'il devait consulter un tiers, comme le stipule la *Loi*. L'organisme public a répondu au requérant près de quatre mois plus tard, lui fournissant trois pages du dossier, mais ces pages étaient considérablement révisées. Aucune explication n'a été fournie pour les révisions ou les refus. À ce stade, le requérant a renouvelé sa demande de révision de la réponse qu'il avait obtenue. Il n'était pas convaincu d'avoir reçu tous les documents éclairants et était mécontent de la façon dont les documents avaient été révisés.

Malgré ma demande qu'on réagisse rapidement au processus des demandes de révision compte tenu des retards déjà existants, l'organisme public a encore une fois omis de réagir au processus de révision jusqu'à ce que mon bureau ait présenté plusieurs demandes et que deux autres mois se soient écoulés. Quand l'organisme public a répondu, il a reconnu avoir, effectivement, envoyé au requérant la mauvaise série de documents révisés. Il n'a pas indiqué s'il lui avait déjà envoyé une version corrigée.

Ce dossier est un cas exemplaire sur la façon de ne pas traiter une demande d'accès à l'information. Le requérant a dû attendre plus de deux ans pour recevoir trois pages, lesquelles étaient mal révisées. La plupart des recommandations faites dans ce cas visaient donc à améliorer l'approche de l'organisme public aux demandes d'accès à l'information.

L'organisme public a choisi de ne pas accepter la plupart des recommandations formulées. Il a convenu d'offrir de la formation à son personnel en réaction aux questions d'accès à l'information et de protection de la vie privée et de présenter au requérant des excuses sur la manière dont sa demande d'accès avait été traitée. Il a accepté une recommandation importante concernant la divulgation fournie au requérant, mais a rejeté toutes les autres recommandations importantes. Il convient de souligner également que l'organisme public a omis de répondre à mes recommandations dans les trente jours, tel que stipulé dans la *Loi.* Mon bureau a dû effectuer deux rappels supplémentaires avant de recevoir une réponse.

Dans ce cas, une entreprise a demandé de l'information concernant une demande de propositions particulière, y compris :

a) le total des points de chaque fournisseur ayant présenté une soumission;

b) les points obtenus pour chaque critère d'évaluation des fournisseurs;

c) les demandes (complètes) de chaque fournisseur retenu;

d) les taux offerts par chaque fournisseur pour la durée de l'offre à commandes;

e) les dépenses annuelles par fournisseur.

L'organisme public a répondu à la demande, fournissant seulement les dossiers relativement aux points (a) et (e) de la demande d'information et les documents s'appliquant à la proposition du requérant. Pour refuser de fournir le reste des dossiers demandés, l'organisme public s'est référé au paragraphe 24(1), qui stipule qu'un organisme public doit refuser de communiquer :

a) les secrets industriels de tiers;

b) des renseignements financiers, commerciaux, scientifiques, techniques ou ayant trait aux relations de travail qui ont été fournis par un tiers à titre confidentiel, qui sont de nature confidentielle et qui ont été fournis par un tiers en conformité avec une obligation légale;

c) des renseignements dont la divulgation risquerait vraisemblablement d'entraîner des pertes ou des profits financiers injustifiés pour une personne, de nuire à la compétitivité d'un tiers, d'entraver des négocia-

tions menées par un tiers en vue de contrats ou à d'autres fins ou d'en traîner la non-communication de renseignements semblables à un organisme public.

J'ai fait une révision page par page des documents et formulé des recommandations à l'organisme public concernant lesquels des documents auraient dû être divulgués à mon avis. Particulièrement, j'ai convenu qu'une information particulière qui n'avait pas été divulguée constituait un renseignement exclusif d'un tiers. Toutefois, d'autres points supprimés ne contenaient aucune information qui aurait fourni au lecteur de l'information importante sur les pratiques entrepreneuriales des tiers. De plus, l'information n'a pas été fournie par les tiers. Tout ce que ces documents ont accompli a été de fournir une comparaison numérique du rendement de chaque proposant dans chaque critère d'évaluation. J'ai recommandé que ces documents soient divulgués.

Mes recommandations ont été acceptées.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION N^{O} 11-102

Dans ce cas, le requérant m'avait demandé de réviser une décision du ministère des Ressources humaines de ne pas divulguer de l'information qu'il avait demandée relativement à son entrevue d'emploi à un poste particulier au sein d'un organisme public. Pour l'essentiel, le requérant ne recherchait que de l'information au sujet de sa propre candidature au poste. L'organisme public a divulgué de nombreux documents, mais a refusé l'accès à d'autres et n'a fourni que des copies expurgées de plusieurs autres. Pour justifier son refus de divulguer certains documents ou parties de documents, il a invoqué les articles 23 (renseignements personnels), 22 (évaluations ou opinions recueillies relativement à un emploi) et 3 (questions devant être utilisées dans le cadre d'examens ou d'épreuves).

À maints égards, j'étais d'accord avec l'organisme public pour ce qui est de l'information qui avait été supprimée de la réponse fournie au requérant. Toutefois, j'étais en désaccord avec l'invocation de l'article 22, qui stipule ce qui suit :

> Le responsable d'un organisme public peut refuser de divulguer au requérant des renseignements personnels qui consistent en des évaluations ou des opinions recueillies uniquement dans le but de déterminer ses aptitudes, son admissibilité ou ses compétences relativement à un emploi ou à l'attribution de contrats gouvernementaux ou à d'autres avantages, **si les renseignements en question ont été fournis à l'organisme public explicitement ou implicitement à titre confidentiel.** (caractères gras ajoutés)

L'organisme public a avancé que les réponses et évaluations données à chaque candidat au poste représentaient des « évaluations ou opinions » et qu'elles étaient, par conséquent, protégées par l'article 22. Toutefois, j'ai souligné que l'article 22 stipule que seuls les renseignements « fournis à » l'organisme public sont protégés de la divulgation par ses dispositions. Dans ce cas, l'organisme public avait créé les renseignements qu'il voulait protéger.

J'ai aussi recommandé que l'organisme public divulgue les questions posées aux candidats lors de l'entrevue. Toutefois, l'organisme public a soutenu que ces renseignements n'étaient pas visés par la *Loi*, car il s'agissait de « questions devant être utilisées dans le cadre d'examens ou d'épreuves ». L'article 3 de la *Loi* vise intégralement ces questions. Je ne suis pas de l'avis qu'un processus d'entrevue puisse être qualifié d'examen ou d'épreuve. J'ai donc recommandé de divulguer les questions. J'ai également recommandé que les commentaires des intervieweurs et l'évaluation personnelle du requérant soient divulgués.

L'organisme public a refusé de suivre ma recommandation de divulguer les réponses et les évaluations données à chaque candidat ayant passé l'entrevue, avançant que l'article 22, en dépit de sa formulation explicite, incluait les « évaluations » produites par un comité de dotation du GTNO. L'organisme public a également refusé de suivre ma recommandation de divulguer les questions de l'entrevue, soutenant que le fait de révéler leur teneur pouvait nuire au processus en donnant à des candidats un avantage injuste par rapport à d'autres.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION N^{O} 12-103

Cette recommandation a été faite en réponse à trois demandes de renseignements différentes mais reliées. Les requérants, tous des employés du même organisme public, ont fait une demande de renseignements concernant une enquête qui a été menée à leur lieu de travail sur une période de cinq mois. Ils demandaient aussi accès à tous les courriels et autres documents écrits se rapportant aux problèmes soulevés et échangés par certains individus au travail. Les demandes des trois requérants étaient pratiquement identiques excepté que chacun cherchait seulement l'information le concernant personnellement.

Dans chaque cas, les requérants ont été informés par courrier que le délai pour répondre à leur demande dépasserait les 30 jours normalement alloués à un organisme public pour une demande de renseignements et qu'une réponse leur serait fournie dans les 90 jours suivant la réception de leur demande initiale. À la fin du délai de 90 jours, l'organisme public a envoyé à chacun des requérants une deuxième lettre prorogeant le délai de réponse de 90 jours supplémentaires. Chaque requérant m'a demandé de réviser ces prorogations de délai. Il convient aussi de souligner que l'organisme public a présenté aux requérants des estimations élevées de droits, et ce, bien après la deuxième prorogation du délai de réponse. Cette tactique a servi à retarder davantage la réponse, car le mécanisme de la *Loi* veut que la soumission d'une estimation de droits entraîne la cessation de tout travail supplémentaire

concernant l'accès à la demande, jusqu'à la réception du versement de la moitié des droits estimés, accompagné de l'engagement à payer le solde. Les estimations des droits auraient dû être présentées aux requérants au plus tard au moment de la deuxième prorogation. L'organisme public avait reçu les demandes de renseignements des requérants depuis plus de quatre mois avant que ces derniers ne reçoivent leurs estimations de droits.

La *Loi sur l'accès à l'information et la protection de la vie privée* prescrit que les organismes publics doivent répondre à une demande d'accès à l'information dans les 30 jours suivant la réception de la demande, à moins que ce délai ne soit prorogé conformément à l'article 11. L'article 11 autorise un organisme public à proroger le délai de réponse « d'une durée raisonnable » quand il faut consulter ou rechercher un grand nombre de documents pour identifier le document requis et lorsque l'observation du délai entraverait de façon sérieuse le fonctionnement de l'organisme public.

L'organisme public a laissé entendre que, lors de son évaluation préliminaire des demandes, il avait établi que le volume de documents requis était important. Il a aussi établi que le coordonnateur de la *Loi sur l'accès à l'information et la protection de la vie privée,* qui aurait normalement traité la demande, était en position de conflit d'intérêt et qu'il fallait trouver quelqu'un d'autre au sein du ministère pour le remplacer. L'organisme public a donc envoyé la première lettre de prorogation aux requérants les informant que leur réponse serait retardée. Au fur et à mesure du traitement des demandes, l'organisme public a découvert un plus gros volume de documents que prévu, créant un surplus de recherche et de gestion pour identifier tous les documents éclairants. Une deuxième lettre a donc été envoyée, prorogeant davantage le délai à une date d'environ cinq mois ultérieurs à la date de la demande initiale.

En fin de compte, le problème se résumait à deux questions :

a) Les prorogations des délais (demandées à cause du grand nombre de documents demandés ou à rechercher, car le respect du délai aurait entravé d'une manière excessive le fonctionnement de l'organisme public) étaient-elles nécessaires?

b) La durée de la prorogation était-elle « raisonnable »?

J'ai établi, en me basant sur l'information des documents concernés, que l'organisme public avait en fait respecté les premiers critères l'autorisant à proroger le délai — le nombre de documents était important et honorer la date limite aurait entravé d'une manière excessive son fonctionnement. Par contre, je n'étais pas convaincue qu'un délai de cinq mois à partir de la date de la demande était un délai « raisonnable ». En outre, la *Loi* ne comporte pas de disposition autorisant la prorogation d'une prorogation. La *Loi* permet d'effectuer une prorogation, pas plusieurs.

J'ai recommandé :

a) que, en raison des délais, l'organisme public renonce à tout droit de service relié à ces demandes de renseignements;

b) que l'organisme public fournisse la réponse du ministère à chaque requérant dans les 10 jours suivant mes recommandations;

c) que si ce ministère ne possédait pas de logiciel de rédaction pour faciliter la révision et le traitement des demandes en lien avec la *Loi sur l'accès à l'information et la protection de la vie privée*, qu'il investisse dans un tel logiciel sans tarder afin d'éviter, à l'avenir, des délais excessifs de réponse aux demandes de renseignements

d) que l'organisme public prenne des mesures pour s'assurer qu'il y ait plus d'une personne au sein du ministère qui possède l'expertise et les compétences habituelles pour traiter des demandes d'accès à l'information.

Pour l'essentiel, mes recommandations ont été rejetées. L'organisme public a refusé de prendre en considération une réduction des droits de service. De plus, dans l'intervalle où les recommandations de révision ont été émises, l'organisme public a affirmé qu'il avait répondu aux « demandes modifiées » alors soumises par les requérants. L'organisme public a estimé avoir les logiciels et la main-d'œuvre nécessaires pour remplir ses obligations en vertu de la *Loi*, dans la plupart des cas. À son avis, ce cas particulier était unique de par ses circonstances et c'est ce qui avait causé le délai de réponse. Aucun commentaire n'a été émis à savoir si l'organisme public estimait que le délai de réponse dans cette instance était inacceptable.

RECOMMANDATION RELATIVE À LA DEMANDE DE RÉVISION N^{O} 12-104

Cet examen a été engagé par un employé de l'Administration des services de santé et des services sociaux de Yellowknife (ASSSSY) qui était préoccupé par le manque de protection des renseignements personnels sur la santé dans le système de dossiers médicaux électroniques utilisé par l'ASSSSY dans ses deux cliniques de soins primaires de Yellowknife. Le plaignant estimait que le système avait été mis en place sans que les questions de protection de la vie privée ne soient d'abord réglées et que cela avait, dans l'ensemble, augmenté considérablement le risque d'utilisation ou de divulgation inadéquate de renseignements médicaux très délicats parce que le nombre de personnes ayant un accès facile et apparemment non surveillé est plus élevé et qu'il est plus facile d'accéder discrètement à un fichier informatique qu'à un fichier imprimé.

Le système des dossiers médicaux électroniques exploité par l'ASSSSY est utilisé actuellement dans les deux cliniques de Yellowknife. Il ne semble pas être « interopérable » entre les deux emplacements, de sorte qu'un employé de la clinique A ne peut pas accéder aux dossiers d'un patient qui a vu un médecin à la clinique B, mais il semble que le personnel (autre que les praticiens) alterne entre les deux cliniques, de sorte que le nombre de personnes ayant accès à l'information dans le système s'élève à environ 150.

En entreprenant cet examen, j'ai beaucoup appris sur le système des dossiers médicaux électroniques utilisé par l'Administration des services de santé et des services sociaux de Yellowknife. En particulier, j'ai appris ce qui suit :

a) Le système n'est pas interopérable entre les deux principales cliniques de soins primaires, mais le personnel travaille aux deux cliniques en alternance, de sorte qu'un total de près de 150 personnes ont un certain degré d'accès à l'information dans le système, y compris 5 conseillers en santé mentale et en toxicomanies, 8 adjoints administratifs, 18 aides de clinique, 8 commis à la facturation, 12 infirmiers auxiliaires autorisés, 24 infirmiers autorisés, 6 directeurs, 4 commis aux documents, 1 coordonnateur de la gestion des risques en matière de qualité, 2 éducateurs spécialisés en diabète, 1 diététiste, 1 travailleur social médical, 54 praticiens et 4 employés du service de la TI.

b) Chacun de ces employés a reçu une formation sur l'utilisation du système, y compris une séance d'information sur la confidentialité et ce qui constitue un accès approprié. De plus, tous les employés signent une entente de confidentialité au moment de leur embauche.

c) L'accès au système est contrôlé par l'utilisation des noms d'utilisateurs et des mots de passe individuels et uniques. Pour accéder au système de dossiers médicaux électroniques, l'utilisateur doit d'abord se brancher au réseau de l'ASSSSY, qui est également protégé par un nom d'utilisateur et un mot de passe. Il n'est pas possible d'accéder au système à l'extérieur du réseau de l'Administration des services de santé et des services sociaux de Yellowknife.

d) Les sessions individuelles « expirent » après une période d'inactivité déterminée.

e) L'accès au système est contrôlé par un paradigme « d'accès en fonction du rôle ». Les « rôles » sont définis par la description de poste d'un employé afin que, par exemple, un médecin puisse avoir accès au dossier au complet, mais que le réceptionniste puisse voir seulement des renseignements plus limités concernant le patient (son nom, son adresse, son problème médical, sa médication).

f) Il est possible de « verrouiller » les renseignements sur un patient afin qu'ils soient mis à la seule disposition de l'employé qui a créé le dossier, bien que cette fonction soit peu utilisée puisqu'elle est considérée comme allant à l'encontre des principaux objectifs du dossier medical électronique, qui est le partage efficace des renseignements visant à appuyer la prestation de soins de santé complets axés sur la collaboration.

g) Lorsqu'un employé quitte son emploi à l'ASSSSY, la révocation de l'accès au système des dossiers médicaux électroniques fait partie de la procédure de fermeture standard.

h) Le système de dossiers médicaux électroniques lui-même est conçu avec une fonctionnalité de vérification « solide » qui enregistre l'action et l'identité de l'utilisateur chaque fois qu'il accède au système. Cela permet l'examen des cas préoccupants qui pourraient survenir et l'établissement d'un protocole de vérification courant. Au moment de sa réponse (en juillet 2011), l'ASSSSY a indiqué qu'elle était « en train » de mettre en œuvre un processus de vérification courant des dossiers médicaux électroniques.

i) À moins qu'elle ne soit interdite par la législation au contraire, comme dans le cas de la législation relative à la protection de l'enfance, l'ASSSSY est d'avis qu'elle peut, à titre d'administration de la santé, partager au besoin des renseignements sur le client au sein de l'Administration, pour faciliter son fonctionnement, sans le consentement du client.

L'une des préoccupations spécifiques du plaignant était que le « Dossier des rendez-vous » qui se trouve sur la page récapitulative des rendez-vous médicaux de chaque dossier médical électronique est non seulement accessible, mais aussi inévitablement, par tous les 150 employés, indépendamment du « rôle » qui leur est confié. Ce dossier est disponible lorsque le résumé médical est consigné, lorsqu'un client est enregistré pour une raison quelconque et lorsqu'un membre du personnel note la visite. Les renseignements figurant sur cette page peuvent être assez délicats – par exemple, les éléments suivants pourraient bien y figurer :

- une grossesse;
- la consommation d'alcool et d'autres drogues;
- une dysfonction érectile;
- le dépistage du cancer;
- un avortement thérapeutique;
- un diagnostic psychiatrique – maladie affective bipolaire, schizophrénie, crises de panique;
- le dépistage d'infections transmissibles sexuellement.

En réponse à cet examen, l'ASSSSY a décidé qu'elle demanderait à son conseiller juridique un examen juridique du dossier médical électronique. Dans le cadre de cet examen juridique, le conseiller juridique a réalisé une évaluation des répercussions sur la vie privée et formulé de nombreuses recommandations que l'ASSSSY s'est engagée à suivre dans sa planification actuelle et future. On m'a remis une copie du rapport dans le cadre de mon examen.

Bien que le rapport préparé par le conseiller juridique de l'organisme public indiquait avec justesse que les tribunaux canadiens reconnaissent depuis longtemps les droits de la protection des renseignements personnels et que le « caractère privé de l'information » a été défini comme « le droit du particulier de déterminer lui-même quand, comment et dans quelle mesure il diffusera des renseignements personnels le concernant », on a constaté des différences importantes entre l'auteur du rapport et moi-même au sujet de ce que signifie exactement cet énoncé. L'organisme public était d'avis qu'il y a un consentement implicite qui permet à l'ASSSSY d'utiliser les renseignements personnels sur la santé des patients pour quel que motif de soins de santé que ce soit au sein de la clinique une fois que ces renseignements figurent dans leur système, allant des questions de counseling aux questions alimentaires en passant par les questions d'obstétrique ou même les questions touchant les services sociaux. À mon avis, toutefois, la législation actuelle permet à l'organisme public d'utiliser ou de divulguer les renseignements personnels obtenus du patient dans le seul but de traiter le problème spécifique énoncé. La législation actuelle permet seulement à un organisme public d'utiliser les renseignements personnels recueillis aux fins pour lesquelles ils ont été recueillis ou pour une utilisation conforme à ces fins. À moins qu'il n'y ait une législation particulière sur la protection des renseignements médicaux, la *Loi*, par conséquent, permet que des renseignements recueillis pour une infection de l'oreille du patient, par exemple, soient utilisés seulement pour fournir des soins médicaux concernant l'infection de l'oreille, sauf si le patient donne son consentement pour une plus large utilisation. Même si j'avais convenu de l'existence d'un certain paramètre au sein duquel un consentement implicite permettait de présumer qu'on peut utiliser des renseignements médicaux personnels parce qu'ils se rapportent à la fin pour laquelle les renseignements ont été recueillis, ce consentement implicite a une application assez limitée en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée.*

Selon les constats que j'ai établis en faisant ce rapport, j'ai exprimé de nombreuses préoccupations et soulevé une série de questions :

a) Il semble que les renseignements personnels sur la santé ne soient pas compartimentés, mais qu'ils soient plutôt généralement mis à la disposition de tous les « services » au sein des deux principales cliniques et que les patients ignorent comment leurs renseignements sont utilisés et partagés;

b) L'accès « en fonction des rôles » au système des dossiers médicaux électroniques semble avoir été défini afin de permettre l'accès au sein du système à autant de renseignements que possible au plus grand nombre de personnes que possible, mais cela ne respecte pas l'esprit ou l'objet de la *Loi*, dans sa version actuelle;

c) En fonction des renseignements fournis par l'organisme public, il semblait que, du moins dans une certaine mesure, la technologie régissait les solutions, au lieu du contraire. À mon avis, la technologie doit être en mesure de répondre aux besoins du système au lieu de laisser sa limitation définir les mesures de protection de la vie privée disponibles;

d) J'ai estimé qu'il reste beaucoup de travail à faire pour s'assurer que tant le public que l'ASSSSY comprennent parfaitement à la fois les avantages et les risques inhérents à un dossier médical électronique. Yellowknife est une petite ville et, inévitablement, au moins une des 150 personnes qui ont accès au système finira par avoir un certain lien avec chaque patient qui franchit la porte, que ce soit en tant qu'ami ou parent ou ami d'un ami ou d'un parent. J'ai aussi estimé qu'il était totalement inapproprié que le directeur des programmes sociaux ait un accès de haut niveau à tous les dossiers de l'ASSSSY, y compris les dossiers de counseling;

e) Le concept de « cercle de soins » doit être défini, et cette définition devrait être créée du point de vue du patient, et dans les limites imposées par la *Loi sur l'accès à l'information et la protection de la vie privée*, et non du point de vue de l'efficacité du système. Au moins jusqu'à ce que le public soit mieux renseigné sur le système, l'ASSSSY doit trouver des moyens pour protéger les renseignements personnels sur la santé « entre les services », afin que les renseignements recueillis aux fins de guérir une fracture à la jambe, par exemple, ne soient pas mis à la disposition des personnes œuvrant dans les services de counseling;

f) Le système des dossiers médicaux électroniques semble offrir seulement une approche du « tout ou rien » envers le masquage des renseignements. Les renseignements médicaux électroniques sont mis à la disposition de tout le monde dans le système (en fonction de leurs rôles) ou seulement de l'auteur. Aucune option n'est disponible qui permettrait d'interdire l'accès à une ou deux personnes au dossier d'un patient. Comme d'autres administrations l'ont découvert, c'est l'employé le plus curieux qui est le plus souvent la cause d'une utilisation ou divulgation injustifiée de renseignements personnels. Il doit y avoir une fonction qui permet au système d'« empêcher » certains individus d'accéder à certains dossiers. Non seulement le système doit avoir cette fonctionnalité, mais le public doit savoir que les « verrouillages » sont possibles, afin qu'il puisse les demander;

g) Plus d'une année après le lancement du système des dossiers médicaux électroniques dans les deux cliniques de Yellowknife, aucune vérification n'est effectuée ou la vérification effectuée est minime et ne tient pas compte des politiques ou des protocoles sous-jacents en place.

De nombreuses recommandations ont été faites compte tenu de ces préoccupations. Bien que les recommandations spécifiques formulées aient été, pour la plupart, acceptées par l'organisme public, l'ASSSSY n'a reconnu en aucune façon que son interprétation actuelle de la manière dont elle peut utiliser les renseignements personnels dans les deux cliniques de soins primaires est de quelle que façon que ce soit inappropriée ou contraire à la *Loi sur l'accès à l'information et la protection de la vie privée*. De même, elle ne s'est engagée en aucune façon à limiter l'échange de renseignements personnels sur la santé dans les cliniques entre les « services » ou les secteurs desservis.

L'objectif fondamental de la Loi reflète une philosophie générale de divulgation complète sauf si les renseignements font l'objet d'une dérogation en vertu d'un libellé législatif clairement délimité. La Loi comprend des dérogations particulières à l'obligation de divulguer, mais ces dérogations limitées ne masquent pas la politique de base selon laquelle la divulgation, et non le secret, est l'objectif dominant de la Loi. Les dispositions générales de la Loi sur la divulgation, jumelées à des dérogations particulières, prescrivent l'« équilibre » entre le droit à la vie privée d'une personne et la politique de base d'ouverture des dossiers des organismes et les mesures visant l'examen du public.

Tallis J.A., General Motors Acceptance Corp. du Canada c. Saskatchewan Government Insurance (Sask.C.A.), [1993] S.J. N° 301, p. 5

REGARD VERS L'AVENIR

La recommandation relative à la demande de révision n° 12-104 résumée dans la section précédente constitue, à mon avis, l'un des rapports les plus importants que j'ai rédigés depuis mon entrée en fonction. Bien que l'Administration des services de santé et des services sociaux de Yellowknife et tous les autres établissements de santé administrés par le gouvernement avec lesquels j'ai collaboré sont tout à fait conscients des préoccupations relatives à la vie privée et s'efforcent vraiment de « suivre les règles » de leur mieux, les règles ne sont pas bien définies et les dispositions sur la protection de la vie privée prévues dans la *Loi* ne sont tout simplement pas respectées. Dans plusieurs de mes recommandations précédentes, j'ai abordé le besoin d'une législation sur la protection des renseignements médicaux personnels. Je sais qu'on y travaille, mais près de cinq années se sont écoulées et rien n'indique encore que cette législation pourrait être présentée à une date quelconque. Il faut vraiment que cela devienne une priorité. Comme le rapport et les recommandations visant l'ASSSSY le démontrent, il est manifestement nécessaire de nous doter d'une législation dont les dispositions traitent des difficultés particulières du maintien de la confidentialité des renseignements médicaux personnels, tout en reconnaissant du même coup que la gestion convenable des dossiers électroniques peut considérablement améliorer la prestation des services de santé. Les dossiers médicaux électroniques doivent tenir compte du droit du patient « de déterminer lui-même quand, comment et dans quelle mesure il diffusera des renseignements personnels le concernant ». Il est également impératif d'éduquer le public sur les dossiers électroniques et la protection des renseignements médicaux, et ce, immédiatement. Avant qu'une nouvelle législation soit adoptée, il faudra organiser une consultation publique approfondie, à grande échelle et bien diffusée, non seulement pour jauger l'acceptation du public sur la législation proposée, mais aussi pour commencer le processus éducatif qui sera nécessaire pour que le public comprenne comment elle le touchera.

Sur un autre plan, je reçois de plus en plus de lettres de la part de personnes qui sont inquiètes de la façon dont les municipalités (administrations locales) recueillent, utilisent ou divulguent des renseignements personnels. Cette année, j'ai reçu deux plaintes au sujet de l'utilisation ou de la divulgation des renseignements personnels d'employés. Dans chaque cas, si les allégations des plaignants étaient fondées, et si la *Loi sur l'accès à l'information et la protection de la vie privée* s'appliquait, les violations seraient réelles et graves. J'ai tenté d'engager la municipalité en cause dans une discussion sur les politiques, les lignes directrices ou les pratiques exemplaires, mais n'ai obtenu aucune réaction à ma correspondance. En l'absence d'une législation sur l'accès à l'information et la protection de la vie privée visant les municipalités des TNO, celles-ci ne sont l'objet d'aucune contrainte législative, en dépit du fait qu'elles colligent et conservent toutes des volumes importants de renseignements personnels sur les citoyens et leurs employés. Il n'existe pas de mécanisme de surveillance et les citoyens ne disposent d'aucun recours lorsque les renseignements sont inadéquatement utilisés. Il n'existe pas non plus de règles permettant aux citoyens d'accéder aux renseignements que les municipalités produisent et colligent. Les trois territoires du Nord sont les seules et dernières autorités législatives à ne pas avoir de législation sur l'accès à l'information et la protection de la vie privée pour les municipalités. C'est là une question de responsabilité et il faut trouver le moyen de résoudre cette situation.

Pour conclure, je rappelle que la *Loi sur l'accès à l'information et la protection de la vie privée* est désormais en vigueur depuis 15 ans. Comme je le soulignais dans mes commentaires d'introduction, les principes sous-jacents de la *Loi* sont toujours très utiles. Le monde a subi des changements qui n'auraient jamais été envisageables en 1994, particulièrement pour ce qui est de la capacité de colliger, de conserver et de manipuler les données. La plupart des provinces et territoires canadiens, dont ceux qui ont adopté une législation plus récente que la nôtre, ont entrepris une révision générale de leur loi en matière d'accès à l'information et de protection de la vie privée, pour tenir compte de nouvelles réalités, remédier à des points faibles et clarifier certains autres points. Il est nécessaire d'évoluer en suivant les changements que connaît le monde de l'information. La capacité grandissante de conserver des

volumes de renseignements toujours plus importants devrait s'accompagner d'une vigilance accrue. Par conséquent, je recommanderais qu'une révision de la *Loi* soit ajoutée au programme législatif, en vue d'examiner si ses dispositions conviennent ou non pour faire face aux défis des technologies du XXI^{e} siècle et pour remédier à certains des problèmes soulevés dans mes rapports annuels au fil des ans.

La meilleure défense [pour une démocratie, pour le bien public] est l'agressivité, l'agressivité du citoyen engagé. Nous devons réaffirmer ce processus lent, coûteux en temps, inefficace et ennuyeux qui exige notre implication; on l'appelle « être un citoyen ». Le bien public n'est pas tangible. Il n'est pas statique. C'est un processus. Il s'agit du processus par lequel les civilisations démocratiques s'édifient.

- John Ralston Saul