



2008/2009  
ANNUAL REPORT  
Information and Privacy Commissioner  
of the Northwest Territories

ELAINE KEENAN BENGTS  
Information and Privacy Commissioner



**NORTHWEST  
TERRITORIES  
INFORMATION  
AND PRIVACY  
COMMISSIONER**

5015 - 47th Street  
P.O. Box 262  
Yellowknife, NT  
X1A 2N2

October 29, 2009

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 1<sup>st</sup>, 2008 to March 31<sup>st</sup>, 2009.

Yours very truly

Elaine Keenan Bengts  
Information and Privacy Commissioner  
Northwest Territories



## INDEX

	Page
Commissioner's Message	4
The Act	11
The Role and Mandate of the Information and Privacy Commissioner	13
The Review Process	15
Requests for Review	16
Protection of Privacy	17
The Year In Review	19
Making an Access to Information Request	21
Review Recommendations Made	22
Review Recommendation 08-069	22
Review Recommendation 08-070	24
Review Recommendation 08-071	26
Review Recommendation 08-072	28
Review Recommendation 09-073	29
Review Recommendation 09-074	31
Looking Ahead	34



## COMMISSIONER'S MESSAGE

The *Access to Information and Protection of Privacy Act* (the "ATIPP") of the Northwest Territories was passed in 1994, some 15 years ago, and came into force in 1997. This Act confirms the legal right of the people of the Northwest Territories to have access government information and provides the mechanisms to exercise that right. Furthermore, the Act requires Territorial government agencies to take positive steps to protect the personal information of individuals.

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

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

In the 15 years since this Act was passed, the world has changed. Technology has dramatically changed the way we do things and many of the basic assumptions which formed the underpinnings of the process are no longer accurate. The push toward the "paperless office", the amazing growth of data storage capabilities, the prevalence of e-mail as a means of communication and the ever growing use of mobile technologies...all of these have created new challenges in terms of the keeping of accurate and accessible records, as well as in term of ensuring that personal information is kept secure and used only for the purpose it is collected. However, the basic goals of the Act, which were to make government more open and transparent, and to make government officials and politicians more accountable to the people of the Northwest Ter-



ritories remain relevant today, perhaps even more so than when the Act was created. The means of meeting those goals, however, have changed.

In his 2008 Annual Report, Richard Thomas, the British Information Commissioner outlined his assessment of what successful access and privacy legislation will accomplish. He feels that success is established where it results in

- A society where information rights and responsibilities are respected by all.
- Organizations which inspire trust by collecting and using personal information responsibly, securely and fairly;
- People understanding how their personal information is used, are aware of their rights and are confident in using them;

The government should not keep information confidential merely because public officials might be embarrassed by disclosure, because errors and failures might be revealed, or because of speculative or abstract fears,.

President Barack Obama, January 22nd, 2009 Memo to the Heads of Departments and Agencies

- Public authorities who are open and transparent, providing people with access to official information as a matter of course;
- People who are aware of their rights of access to official information and are confident in using them.

These are laudable goals. Achieving this kind of robust system is possible, but only with diligence and hard work. It requires ongoing review of the legislation to ensure that it meets the ever changing realities of the technological world and government systems. It requires systems that adequately index, track and control electronic records of all kinds. It requires that there be well trained ATIPP Coordinators, drawn



from senior ranks of government who are capable of interpreting the Act, making the necessary decisions and applying policy. A good system would have all of the ATIPP Coordinators meeting regularly and working together as a network to ensure appropriate and consistent application of the Act in all public bodies. A comprehensive training program for all current and new public sector employees, with more advanced training for those whose responsibility it is to handle personal information on a regular basis, would be in place. All contractors would be made aware that records pertaining to the contract are all subject to the Act and would be clearly informed and educated about their obligations and responsibilities under the Act. There would be a comprehensive and practical manual that explains statutory requirements in plain language with

Citizens entrust their governments with power through elections, and with resources through the payment of taxes. Those who are entrusted with this power bear a responsibility not only to serve, but also to inform citizens and encourage the public to participate in their decisions and actions. - It is citizens, after all, who should ultimately be the source of power, as they bear the consequences of its abuse

Excerpt from the Web Site of Transparency International

checklists and precedents to assist when issues arise, and it would be referred to and used consistently to address access and privacy issues. We're not all the way there yet.

Perhaps the most significant element that is needed, however, is a modern and effective information management system, applicable and responding to the challenges of electronic record keeping together with strong policies about information management that are strictly enforced.



Information is a necessary commodity in today's world. Misuse or mismanagement of that information, however, can be a toxic liability. As noted by Richard Thomas, the British Information Commissioner in his 2009 Annual Report:

There needs to be clear responsibility for data minimisation – not collecting any more personal information than is needed and keeping it no longer than necessary. Data quality and data cleansing are likely to assume ever greater importance – ensuring the right information relates to the right person, that it is accurate and that it is kept up to date. Many organizations describe information as a valuable asset, as indeed it can be, if it is managed well. We have tried to get them to recognize that this

The stockpile of government information has been liquefied – broken down into a vast pool of elements whose significance, taken independently, is not easily grasped.

Excerpt from *Blacked Out: Government Secrecy in the Information Age* by Alasdair Roberts (New York: Cambridge

can also quickly turn into a major liability if the risks of poor data handling materialize. Real damage to people's careers, reputations, personal relationships, private lives and bank balances can follow if things go wrong. Real damage can also hit the reputation, the prosperity and the legitimacy of the organizations responsible.

A good information management system requires clear lines of accountability and responsibility, coherent policies and procedures, and rigorous enforcement of those policies. The system in place for paper records is, for the most part adequate to the task



of dealing with paper records. That system does not work nearly as effectively, however, when dealing with electronic records.

As noted by the former Assistant Information and Privacy Commissioner for Newfoundland and Labrador, Sandy Hounsel, in a paper prepared for presentation to the 5th International Conference of Information Commissioners:

A crucial aspect of the modern records management system is the explosion over the last number of years of electronic information. The modern workplace has become more and more digital and our reliance on elec-

There is no human institution but has its dangers. The greater the institution the greater the chances of abuse. Democracy is a great institution and, therefore, it is liable to be greatly abused. The remedy, therefore, is not avoidance of democracy, but reduction of possibility of abuse to a minimum.

Mahatma Gandhi

tronic records and databases is unprecedented. It is estimated that more than 90% of all records being created today are electronic.

There is no doubt that the advantages are numerous. We can search it, cut and paste it, update it in real time, e-mail it, automate it, audit it, secure it, and control it in ways that paper-based systems simply would not allow. Ultimately, this allows us to work faster, save money and accomplish much more with significantly less effort. ....

However, organizations often have difficulty cataloguing, organizing and preserving this information, while maintaining a reasonable ability to ac-





cess it. This is in part due to the failure of many organizations to properly recognize and manage the records management life cycle. This life cycle is equally relevant to both paper records and electronic records, a fact often overlooked by these organizations. More importantly, however, many organizations appear to be overwhelmed by the volume and variety of electronic records. The technology has simply surpassed the capacity to react appropriately.

I am increasingly concerned about the management of electronic records and, in particular, the management of e-mail communications. As far as I am aware, every employee is pretty much left to manage their own e-mail system in their own way. There

Accountability and transparency go to the core of representation, they shed light on power structures in democracy they can illuminate bias and self-interest, and most importantly, lack of them can destroy legitimacy.

A.N. Tiwari

Information Commissioner ,Central Information Commission, India

is no uniformity and there are no apparent policies beyond some very basic rules. Notwithstanding the rules, there is little or no monitoring of how individual employees manage their electronic records. The right to access to information is limited by the Government's ability to find the records. If the management of records is inconsistent, finding records will become a problem. I have already run into several situations in which the records clearly exist but the public body has been unable to locate them where they should have been filed or stored.



Having a good records management system is just as important to the electronic record as it is to the paper record and governments have to find a way to manage electronic records more effectively. This is not a problem unique to the Northwest Territories. It is, in fact, one of the primary issues being faced by all governments, large and small, in Canada and abroad. Without good records management practices, the ability to access to information becomes difficult and sporadic. Without the ability to access information from government, democracy is at risk. Good management of electronic records is undoubtedly a challenge, but it one that must be addressed.

Legislation is tested and improved as a result of usage, and without people using it, much of FOI is pointless. Whose role is it to educate the public? I would say it is the responsibility of every government agency and every public official who interacts with the public. FOI should be embedded into all of government's dealings with citizens.

Megan Carter, Director, Information Consultants Pty Ltd



## THE ACT

The Northwest Territories' *Access to Information and Protection of Privacy Act* (ATIPPA) came into effect on December 31st, 1996. It is applicable to all Territorial Government departments and certain government agencies specified under the regulations. It establishes rules outlining how Territorial government agencies collect, use and disclose personal information and how the public can gain access to government records.

A driver's license is proof that someone is allowed to drive a car. It is not a universal identity card. Nor is it an appropriate identifier for use in analyzing shopping return habits.

David Loukidelis

Information and Privacy Commissioner of British Columbia

The term “access to information” refers to the right of the public to have access to general records relating to the activities of government, ranging from administration and operations to legislation and policy. It is an important aspect of open and accountable government. Under the *Access to Information and Protection of Privacy Act*, the public is given the right to have access to “records” in the possession or control of a public body through an access to information request. Most government records are subject to the Act and are, therefore, required to be disclosed when a request for information is made, unless it is subject to one of the specific, limited exemptions from disclosure as provided for in the Act. The exceptions to the open disclosure rule function to protect individual privacy rights, allow elected representatives to research and develop policy and the government to run the “business” of government.



The Supreme Court of Canada has clearly stated that exceptions to disclosure provided for in access to information legislation should be narrowly interpreted so as to allow the greatest possible access to government records.

The Act also gives individuals the right to obtain information which government bodies collect about them and to request that corrections be made to that information. Even if the public body chooses not to make the correction requested, a notation must be made on the file that the request for a correction was made and the nature of the request.

General surveillance raises serious democratic problems which are not answered by the repeated assertion that those who have nothing to hide have nothing to fear. This puts the onus in the wrong place: it should be for states to justify the interferences they seek to make on privacy rights.

Thomas Hammarberg,

The Council of Europe's Commissioner for Human Rights

Privacy protection is the other part of the legislative equation, and refers to the safeguarding of personal information held by government. The Act provides rules for when and how government and government agencies can collect, use and disclose personal information and imposes obligations on public bodies to provide security to protect the personal information they have in their possession.



## THE ROLE AND MANDATE OF THE INFORMATION AND PRIVACY COMMISSIONER

The office of the Information and Privacy Commissioner (IPC) is created under the *Access to Information and Protection of Privacy Act*. 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 annually, and usually appears once a year in front of the Standing Committee on Priorities and Planning to discuss her report. The IPC is an independent officer who can be only be removed from office “for cause or incapacity” on the recommendation of the Legislative Assembly.

The second deadly sin is to pretend to Freedom of Information but to provide so many exceptions and derogations from the principle as to endanger the achievement of a real cultural change in public administration.

Justice Michael Kirby, High Court of Australia (then President of the NSW Court of Appeal),

The Information and Privacy Commissioner has several roles under the Act, including:

- independently reviewing the decisions and practices of government organizations concerning access and privacy and providing recommendations to public bodies with respect to those issues
- providing comment and advice on proposed government legislation and programs ;
- educating the public about the Act



When dealing with access to information issues, the Information and Privacy Commissioner has very limited power to make binding orders with respect to matters which come before her. Rather, in most cases her role is that of an ombudsman - she makes recommendations which are persuasive, but not binding. With respect to requests for access to information, recommendations are made to the head of the public body involved who must then make a final decision as to whether or not the information will be disclosed. If the person seeking the information is still not satisfied with the response received from the head of the public body after the review process has been completed, there is recourse to the Supreme Court of the Northwest Territories for a final determination of the matter.

You can put an amazing security system in place, but if nobody understands how to use it, it will go wrong. It's all about the human factor...

Security training can't just be about ticking the box, it's got to be about making sure that people understand the everyday rules, and why they are there. ... It has to be part of people's everyday lives, so that they can relate to what you are asking them to do.

Martin Smith, Chairman and Founder, The Security Company

The Information and Privacy Commissioner is also authorized under the Act to investigate complaints of breach of personal privacy. Upon completion of her investigation, the IPC will indicate whether or not it appears that the individual's privacy has been breached. Regardless of the finding, the IPC will normally make recommendations to the public body involved concerning systems, policies and procedures which might help to improve security and avoid inappropriate future disclosures. The public body must respond to the recommendations made within 60 days, but the Act does not provide for any appeal from the public body's response to a breach of privacy complaint.



## The Review Process

Requests for information must be made in writing and be delivered to the public body from which the information is sought. Although forms are available, requests for information do not need to be in any particular form. The only requirement is that the request be in writing. This would include a request made by e-mail but where a request is made by e-mail, it may not be considered complete until the public body receives confirmation of the request with the applicant's signature. Requests for information are subject to a \$25.00 application fee except in cases where the information requested is the applicant's own personal information. In such cases, there is no application fee, although there may be a fee for copying records in certain circumstances.

Although we have seen massive change in the capability of organizations to exploit modern technology that uses our information to deliver services, that has not been accompanied by a similar drive to develop new effective technical and procedural privacy safeguards,

Richard Thomas, UK Information Commissioner

When a request for information is received, the public body has a duty to identify all of the records which are responsive to the request and to respond to the request within 30 days. Once all of the responsive documents are identified, they are reviewed to determine if there are any records or parts of records which are exempt from disclosure under the Act. The public body must endeavor to provide the applicant with as much of the requested information as possible, while at the same time applying the limited exceptions to disclosure specified in the Act. Public Bodies are prohibited from disclosing certain kinds of records. In some instances, the Public Body has discretion to decide to either disclose the records or not. These discretionary exemptions require



the public body to consider whether or not to disclose the information, keeping in mind the purposes of the Act and the weight of court authority which requires public bodies to err on the side of disclosure.

Every person has the right to ask for information about themselves. If an individual finds information 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 be made on the file that the individual has requested a correction.

The impact of poor records management goes far beyond the government's access and privacy regime. Within government, the lack of accurate and authoritative information results in poor decisions, failed programs and lost opportunities... The failure to maintain and protect records with high legal and intellectual property value results in increased liability and financial loss. The premature destruction of records with long-term archival value contributes to our collective historical amnesia and the loss of valuable knowledge.

Hon. John Reid , Information Commissioner of Canada

Annual Report 2002/2003

## REQUESTS FOR REVIEW

Under section 28 of the *Access to Information and Protection of Privacy Act*, a person who has requested information from a public body, or a third party who may be affected by the disclosure of information by a public body, may apply to the Information and Privacy Commissioner for a review of the public body's decision. This includes decisions about the disclosure of records, corrections to personal information, time extensions, fees, and breaches of privacy. The purpose of this process is to ensure an





impartial avenue for review and independent oversight of discretionary and other decisions made by public bodies under the Act.

A Request for Review must be made in writing to the Information and Privacy Commissioner's Office within 30 days of receiving a decision from a public body under the Act. There is no fee for making a Request for Review.

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. In most access cases, the Commissioner will receive a copy of the responsive documents from the public body involved and will review the records in dispute. In some cases, it may be necessary for the Information and Privacy Commissioner to attend the government office to physically examine the public body's files.

Databases are not just lists, nor are they the digital equivalent of paper files. Structured databases enable the "querying" of data along novel lines, permitting machines to mine swaths of information, and from it to produce new information. The database state, therefore, is a machine bureaucracy that is actually run by machines. As such it promises to dehumanise both the public-service front line, and the people who rely on it most.

Becky Hogge, From: New Statesman, April 30, 2009

## **PROTECTION OF PRIVACY**

Part II of the *Access to Information and Protection of Privacy Act* sets out 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 also requires public bodies to ensure that they maintain adequate security measures to ensure that the personal information which they collect cannot be accessed by unauthor-



ized 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.

Under the amended *Access to Information and Protection of Privacy Act* the Information and Privacy Commissioner has jurisdiction to review privacy complaints where members of the public are concerned that their personal information has been improperly collected, used or disclosed by a public body. Once recommendations are made, the public body has ninety days to respond to the recommendations. There is, how-

I for one do not believe that a poor records management protocol is an appropriate enough reason to deny an applicant access to information that he or she is rightfully entitled to. This highlights the importance of handling all records, both electronic and paper, in a manner that is conducive to appropriate access, security and conservation.

Sandy Hounsel

Assistant Information and Privacy Commissioner for Newfoundland and Labrador

ever, no appeal available to the court unless the individual seeks to have a charge laid pursuant to section 59 of the Act.

In all cases, the IPC will assess whether or not there is any possibility that the matter might be resolved through mediation or other intervention without having to complete a full review. This is often all that is needed to resolve the matter to the satisfaction of the Applicant or Complainant. If, however, a mediated resolution does not appear to be possible, the matter moves into a more in depth review.



All of the parties involved, including the public body and any third parties whose information may be disclosed, are given the opportunity to make written submissions on the issues.

A learning process needs to be introduced rapidly, aimed at the youngest users who are at least aware of the risks inherent in their assiduous use of new communication technologies. If nothing is done today, could future generations claim tomorrow that their privacy is “safe”?

Excerpt from the Web Site “Protecting Privacy in a Borderless World”, 30th Annual Data Protection Commissioner’s Conference, Strasbourg, France, October 2008

## **THE YEAR IN REVIEW**

In the 2008/2009 fiscal year, the Information and Privacy Commissioner's Office opened 15 files in a number of different categories as follows:

Breach of Privacy Complaints	4
Requests for Review (Access)	9
Request for Comment	1
Breach of Privacy (Private Sector)	1



The Requests for Review received involved seven Public Bodies:

- Hay River Health and Social Services Authority 6
- Department of Justice 2
- Yellowknife Education District #1 1
- Education Culture and Employment 1
- Department of the Executive 1
- Department of Human Resources 1
- NWT Power Corporation 1

We still have public trust.. But, trust is not a renewable resource -- once it is lost it may not be regained.

Mary Lysyk, Policy Adviser for Health Canada

# MAKING AN ACCESS TO INFORMATION REQUEST

Applicant makes Request for Information from public body

Public body provides satisfactory response within 30 days

Public body fails to provide satisfactory response or fails to respond within 30 days

Applicant makes a Request for Review to the Information and Privacy Commissioner (IPC)

IPC Conducts informal mediation to resolve issue

If mediation successful, no further action

If mediation unsuccessful, moves to formal review

IPC may choose to go directly to formal review

IPC provides both Applicant and Public Body with the results of her review and makes recommendations

The head of the Public Body has 30 days to provide the Applicant and the IPC with a written indication of his decision with respect to the recommendations made.

Applicant may appeal to the Supreme Court of the Northwest Territories



## REVIEW RECOMMENDATIONS MADE

### Review Recommendation 08-069

In this case the complainant felt that someone working within the Government of the Northwest Territories had disclosed personal information about her. She had provided her personal information to a public body in support of an application for some funding. An acquaintance later told her that he had heard that she had applied for this funding and that she may have provided misleading information on her applica-

In terms of public awareness, all of the Canadian commissioners are currently working on a public awareness campaign aimed at young audiences, to help them understand the inherent risks to privacy and personal information that arise from using social networking sites.

Jennifer Stoddart, Privacy Commissioner of Canada in an address to the 30th Annual Data Protection Commissioners Conference , Strasbourg, France, October, 2008

tion. The Complainant knew that a close personal friend of her acquaintance worked at the public body involved and was convinced that that person had improperly disclosed the information in her application. She tried to address her concerns directly with the public body but was not satisfied with the outcome of those efforts and, as a result she filed a complaint with the Information and Privacy Commissioner.

At the conclusion of the IPC's investigation, she acknowledged that it was difficult in the circumstances to confirm with any certainty whether there had, in fact, a breach of an individual's privacy unless there was some means of confirming who had access to



her file and for what purpose. She noted that it will almost always come down to the Complainant's word against the employee's in such circumstances. She indicated that although it was impossible to determine absolutely that there had been an inappropriate disclosure of the Complainant's information, it was more likely than not that the public body's employee had inappropriately disclosed the Complainant's personal information. However, since that employee was no longer working with the public body, there were no specific recommendations made with respect to the employee. Rather, the Information and Privacy Commissioner made recommendations to assist the public body prevent similar disclosures in the future. Specifically, she recommended that the

In the north, where the low population base means that there is always going to be a high probability that public employees will be privy at some point to personal information of someone else that he or she knows, it is important to make sure that there are adequate safeguards in place to prevent improper use or disclosure of that information.

Elaine Keenan Bengts, Review Recommendation 08-069

public body develop a protocol to deal with complaints about possible breaches of personal information and that that protocol should include the ATIPP Co-Ordinator for the public body as an active participant in the process. Further, she suggested that the protocol include a requirement to keep a written record of the steps taken during the investigation of the complaint, the findings, and the steps to be taken to address any deficiencies.



### **Review Recommendation 08-070**

The Applicant in this case requested a review of the decision of the Department of Industry, Tourism and Investment to refuse access to a specific report. He also requested any correspondence, e-mails, briefing notes and other documents related to or discussing the contents of the report and, in particular, any document which discussed why the Government of the Northwest Territories decided not to make the report public.

Furthermore, each document must meet the three criteria for determining if it is privileged:

- (i) it must be a communication between solicitor and client;
- (ii) it must entail the seeking or giving of legal advice; and
- (iii) it must be intended to be confidential by the parties.

Elaine Keenan Bengts, Review Recommendation 08-70

The public body in this case made it clear from the beginning that they considered the record in question to be extremely sensitive and that they were not at all interested in disclosing it. In fact, they refused to provide the Information and Privacy Commissioner with a copy of the record, even in the face of those sections of the Act which give the IPC authority to review all records which are the subject of a review. The public body invoked every exemption they could think of under the act, including

- section 15 (solicitor/client privilege)
- section 14(1)(a) (advice prepared for or by a public body)





- section 13 (cabinet confidence)
- section 16 (disclosure prejudicial to intergovernmental relations)
- section 17 (disclosure harmful to the financial interests of the government)
- section 24 (disclosure harmful to the financial interests of a third party)

After reviewing the report, the IPC found that the report was subject to solicitor/client privilege and that the public body had fully considered and applied their discretion in refusing to disclose the record.

The IPC strongly criticized the public body, however, on their handling of this request and the disrespect shown to her office evidenced by their reluctance to provide her with a copy of the report which was the subject of the Access to Information Request.

Although I am pleased that the matter was eventually resolved, I do not anticipate that I will be asked to provide a solicitor's undertaking with respect to my review of records in future reviews, no matter how sensitive the information might be considered by the public body. Rather, I anticipate that all public bodies will respect the office of the Information and Privacy Commissioner and accept that the oath of office taken by the Commissioner and the provisions of the legislation by which the Commissioner is bound are sufficient to ensure that the substance of records received for the purpose of review will not be improperly disclosed by him/her.

Elaine Keenan Bengts, Review Recommendation 08-070

She pointed out that the Act gives the Information and Privacy Commissioner the right to review all records subject to the Act, while at the same time prohibiting the IPC from disclosing the contents of such records.

The recommendations made were accepted, though no comments were received with respect to the IPC's concerns about the manner in which the request was handled.



### **Review Recommendation 08-071**

This case dealt with another concern about a possible breach of privacy. The Complainant was concerned that his personal medical information had been shared inappropriately by the Workers Compensation Board (now the Workers Safety and Compensation Commission). The Complainant had filed a claim with the Workers Compensation Board (WCB) claiming post traumatic stress disorder as a result of an incident which had occurred approximately 8 years earlier at a remote work site while the Complainant was employed with “Employer A”. When filing his complaint, the Complainant mistakenly named his current employer rather than his former employer. In support of his claim, he had also submitted a chronology of his employment since the

It seems to me that the spirit and intention of the *Access to Information and Protection of Privacy Act* suggests that if an individual requests that a process for which he/she has given consent to the collection or disclosure of personal information be stopped, by implication the consent attached to the original request is also revoked. Thereafter, the WCB would have no right whatsoever to use or disclose the personal information of the claimant.

Elaine Keenan Bengts, Review Recommendation 08-071

incident which he says caused his disorder, naming several additional employers. The WCB conducted an investigation and, in doing so, they contacted a number of the Complainant’s former employers. The Complainant subsequently asked that his complaint be put on hold and the WCB initially complied but for some reason reinitiated the investigation some time later, without the knowledge of the Complainant. In reviving the investigation, the WCB contacted the Complainant’s current employer and asked a number of questions and, apparently, disclosed at least something of the nature of the Complainant’s claim. Unfortunately, the contact with his current employer coincided in time with a separate dispute the Complainant was having with that employer. This



exacerbated his problem with his current employer and he therefore asked me to review the situation. As a secondary issue, the Complainant, who had asked for access to his file, was concerned about a reference on the file to allegations made by his current employer of certain behavior by the Complainant.

Upon completing her investigation, the IPC was satisfied that the WCB was aware of its duty of confidentiality and its obligations not to use or disclose personal information except in accordance with legislation. She was not, however, entirely satisfied that these concepts were fully understood or that the processes in place were sufficient to meet those obligations.

It is imperative that institutions keep a record of the use and disclosure of personal information under their control. Except in limited circumstances, individuals have the right to know which documents containing their personal information are set to whom and when they are disclosed.

Robert Marleau, Interim Privacy Commissioner of Canada, Annual Report 2002/2003

She recommended that all Claims Managers be given basic training with respect to the privacy provisions of the *Access to Information and Protection of Privacy Act* so as to ensure that they fully understood their obligations to maintain the confidentiality of the personal information of claimants and others.

She further recommended that policies be created and adopted to require Case Managers to consult directly with the claimant before conducting an investigation to clarify any issues which appeared to need clarification, such as the identity of the employer with whom the complainant was working at the time of the incident leading to the claim.



Finally, she expressed concern that it did appear that certain of the Complainant's personal information had been improperly disclosed by the WCB to the Complainant's current employer. She recommended that the WCB take steps to recover the information improperly disclosed and that they should attempt to mitigate, as far as possible, any fallout as a result of the inappropriate sharing of information.

The recommendations of the Information and Privacy Commissioner were accepted.

It is agreed by all concerned that the personal information, that is a prognosis about the Complainant's medical condition, was never provided. There was, therefore, no "collection" of information. This ends the matter. If there was no collection of information, there is nothing to review.

Elaine Keenan Bengts, Review Recommendation 08-72

### **Recommendation 08-072**

The Complainant in this case requested that I review whether the Financial Management Board Secretariat (FMBS) properly collected his personal information. The Complainant was an employee of the Government of the Northwest Territories. He had been asked to provide confirmation from his doctor that he could perform the duties of his employment. The Complainant objected to the request.

The public body alleged that the Complainant's behaviour had been erratic, insubordinate and unprofessional and that he had been warned about his actions but that he refused to comply with direction given. He had been given time off for insubordination



and the Complainant himself claimed that he was suffering from stress related illness. As a result, the employer asked the Complainant to submit to a mental health evaluation so that the employer could determine whether any accommodations were required.

The Complainant objected to having the assessment, and eventually returned to work without the evaluation. The employer eventually decided that, as the Complainant had successfully returned to work without the need for accommodations, their request for the evaluation was redundant, and they withdrew the request.

The Information and Privacy Commissioner concluded that there had been no collection of personal information by the public body and, as a result, there could be no "improper" collection. She made no further recommendations.

I find that at least some of the severed information is the personal information of both the applicant and the third parties. Information and Privacy Commissioners throughout Canada have concluded, in such situations, that an individual's right to receive personal information about themselves is sometimes limited by the privacy considerations of third parties.

Elaine Keenan Bengts, Review Recommendation 09-073

### **Recommendation 09-73**

This case arose out of a Request for Information made by a former employee of a public body for an unedited version of a report prepared by an outside contractor in relation to a workplace harassment complaint made against the Applicant. The public



body had disclosed the record, but they had redacted much of the report such that the meat of it was not disclosed. The Applicant was also concerned that those portions of the report that he did receive were inaccurate and did not reflect the statements made by him to the investigator. Furthermore, he had not, he said, been given the opportunity to review and correct those portions of the report that reflected his statement to the investigator before the report was submitted to the public body. The public body was relying in section 14 and section 23 of the Act to justify their refusal to disclose the remaining portions of the report. Section 14 (1) gives a public body the discretion to refuse to disclose information where the disclosure could reasonably be expected to reveal advice, proposals, recommendations, analyses or policy options developed by

The question of whether information can or must be withheld from investigation-related records must be addressed on an exception-by-exception basis in the circumstances of each case. The sensitivity of workplace complaint investigations can be an appropriate contextual factor in such cases, but the same rules under the Act apply to such materials as apply to personal information in other records.

David Loukidelis, Order 01-53, BC Information and Privacy Commissioner

or for a public body. Section 23 prohibits the disclosure of personal information where that disclosure would constitute an unreasonable invasion of the privacy of a third party.

After reviewing the report and applying the relevant sections of the Act, the Information and Privacy Commissioner concluded that although some of the information in the report might have been protected from disclosure as being the personal information of third parties, and that disclosure would amount to an unreasonable invasion of their privacy, before refusing disclosure outright, the public body should have consulted with



the third parties to determine whether they would object to the disclosure pursuant to section 26 of the Act. She further recommended that much of the report be disclosed with the personal information severed.

The recommendations were accepted.

Although the Act does not impose a standard of perfection, it is well established that, in searching for records, a public body must do that which a fair and rational person would expect to be done or consider acceptable. The search must be thorough and comprehensive. The evidence should describe all potential sources of records, identify those searched and identify any sources that were not searched, with reasons for not doing so. The evidence should also indicate how the searches were done and how much time public body staff spent searching for records.

David Loukidelis, BC Information and Privacy Commissioner, Order 02-03

#### **Recommendation 09-074**

In this review, the Applicant was seeking information which the Department of Education might have about him with respect to his Student Financial Assistance or his Millennium Scholarship, during a certain time period. He was specifically interested in e-mails between certain named employees of the department. The public body responded to the request, but the Applicant was not satisfied with the results and requested that the public body search through its backup system to recover deleted e-mails.

The Public body took the position that they had done a thorough search in the first instance and had concluded that all relevant records had been provided. They declined to review the backup records as requested by the Applicant. It was their position that



section 7 of the Act required only that they make every “reasonable effort” to assist an Applicant and that that onus was met by searching the current records. They argued that to search backups would be extremely difficult and time consuming and that it was unlikely that any further records would be found in the backup system that weren’t discovered in the original search for a number of reasons, including the “standard policy” within the division for e-mail messages relating to clients to be saved either on the client record or by the officer working with the client. It was the public body’s position that unless the Applicant could provide some evidence to support his suspicion that the e-mail records he was seeking actually existed, searching the backup system went beyond what was reasonably required under the Act.

It seems to me that when an Applicant is asking a public body to search backup records, which would normally be considered above and beyond the normal search methods, there is an onus on that individual to provide something to support the need for that kind of search.

Elaine Keenan Bengts, Review Recommendation 09-074

The Information and Privacy Commissioner suggested that because the Act makes “reasonableness” the standard, there are no absolutes and each case must be taken on its own facts. What is reasonable in one case, on one set of facts and evidence, may not be reasonable in another case with another set of facts and evidence. In this case, it was her opinion that the department had met the standard of reasonableness for a number of reasons. Firstly, she was satisfied that the search of current and existing records had been thorough and wide ranging. Secondly, she was convinced from the details provided about the nature of the backup system by the public body that it was unlikely that any additional records would be found. Thirdly, although he had





been given the opportunity to do so, the Applicant had not provided her with any evidence, other than the Applicant's own suspicions, that other records existed. She recommended that no further steps be taken.

The recommendations were accepted.

La Forest J, with whom the majority of the Supreme Court of Canada agreed on this point, commented on the purpose of access to information legislation in *Dagg v. Canada (Minister of Finance)* [1997] 2 S.C.R. 403. He said:

The overarching purpose of access to information legislation is to facilitate democracy by helping to ensure that citizens have the information required to participate meaningfully in the democratic process and that politicians and bureaucrats remain accountable to the citizenry.

This important legislative purpose would be defeated if a public body could simply refuse to search its records on the basis of cost and labour.

Frank Work, Order F2007-028, Alberta Information and Privacy Commissioner



## LOOKING AHEAD

The *Access to Information and Protection of Privacy Act* has been in force now for some 13 years. Every year I make recommendations for change with a view to making the system more accessible, effective and efficient. There is always room for improvement, and the following recommendations are made with a view to continuing to improve the Act and strengthen it as a means to more open and accountable government.

Would we be happy under an efficient tyranny - one in which every movement and action of the citizen was recorded, analyzed, cross-checked instantaneously and no incident, no matter how trivial, ever forgotten?

Professor AS Douglas , London School of Economics, *Science Journal*, October 1970

### 1. **General Review of the Access to Information and Protection of Privacy Act**

Over the last 13 years, use of the Access to Information and Protection of Privacy Act has revealed some weaknesses and a need for clarification in some areas. The technology of today is entirely different than was contemplated when this Act was passed. The legislators of the day could not have anticipated the prevalence of e-mail as a means of communication or the significant move toward electronic records as being the primary method of record keeping. As with most legislation, there is a need to



evolve as things change and to address issues that come up from time to time. The increasing ability to retain ever greater amounts of information should bring with it increasing vigilance. A number of Canadian jurisdictions have recently done reviews of their Acts, and are making or have made amendments to address gaps in the legislation to address the new challenges of the electronic age. I would, therefore, recommend 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 21<sup>st</sup> century technologies and to addressing some of the issues which have been raised in my Annual Reports over the years.

In brief, Privacy by Design refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices (FIPs) into the design, operation and management of information processing technologies and systems.

Dr. Ann Cavoukian, Information and Privacy Commissioner, Ontario

## **2. Board and Agency Amalgamations**

This Government has proposed that a number of boards and agencies be amalgamated into a significantly smaller number of boards and agencies. As I understand the proposal, this may well involve the amalgamation of agencies with currently different mandates, such as education authorities and health and social services agencies. I have significant concerns about how this would impact on the privacy of individuals. There is very little information available about how these amalgamations would work, and what the long term vision for such agencies would be. How does the Government



intend these larger agencies to mesh with one another? There are significant privacy concerns and issues that would flow from such amalgamations, as these agencies all hold significant amounts of our personal information. Those privacy issues must be addressed at the implementation stage or they will undoubtedly become a problem down the road and will be far more difficult to correct at that point.

My counterpart in Ontario has advocated “Privacy by Design”. This concept was developed by Dr. Anne Cavoukian, the Information and Privacy Commissioner of Ontario to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems. This concept asserts that the future of privacy cannot be assured solely by compliance with regulatory frame-

Databases are not just lists, nor are they the digital equivalent of paper files. Structured databases enable the "querying" of data along novel lines, permitting machines to mine swaths of information, and from it to produce new information. The database state, therefore, is a machine bureaucracy that is actually run by machines. As such it promises to dehumanize both the public-service front line, and the people who rely on it most.

Becky Hogge, *New Statesman*, April 30, 2009

works; rather, privacy assurance must ideally become an organization’s default mode of operation. The first three fundamental rules of “Privacy by Design” are all focused on ensuring that privacy issues are addressed before implementation, and not after problems have occurred. To paraphrase from Dr. Cavoukian’s paper on the issue, she says:

Privacy by Design does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, Privacy by Design comes before-the-fact, not after.



2. Privacy is the default. No action should be required on the part of the individual to protect their privacy – it is built into the system, by default.
3. Privacy by Design should be embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

At the very least, it is in my opinion imperative that a full privacy impact assessment be done on the project before any steps are taken to move ahead with it . Moreover, when it does go ahead, it should incorporate Privacy by Design at the implementation stage.

Citizens entrust their governments with power through elections, and with resources through the payment of taxes. Those who are entrusted with this power bear a responsibility not only to serve, but also to inform citizens and encourage the public to participate in their decisions and actions. - It is citizens, after all, who should ultimately be the source of power, as they bear the consequences of its abuse.

Transparency International

### 3. **Municipalities**

This will not be the first time that I have recommended that municipalities should be subject to access and privacy legislation. Not only is it important that municipal authorities be accountable to the public through access to information rules, it is also important that municipalities have rules regarding how they gather, use and disclose personal information about individuals.



In my last Annual Report, I noted that the Northwest Territories was one of only five jurisdictions in Canada that did not include municipalities in their access and privacy legislation. That number is now down to one in four, and I understand that one of the remaining holdouts, the Yukon, is now considering the inclusion of municipalities under its Act. This is an issue of basic democratic imperatives. Openness and accountability are just as necessary at the municipal level as they are at the Territorial or Federal level. The concern, it appears, with including municipalities is the anticipated cost to the municipalities of inclusion. My colleague in Alberta, Commissioner Frank Work, has opined, and I agree, that the right of access to information is precious and that no government should ever oppose it or impede it on the basis that it is too expensive, too

The RTK [Right to Know] movement stands in a similar position. In the last decade the idea of transparency has seized public attention, and there have been great strides in persuading governments to acknowledge the right to information as a matter of principle. Compared to where we were only a few years ago, the prospect is spectacular. Nonetheless we are only in the foothills. Full realization of the RTI idea will require many more years of steady arching.

Professor Alasdair Roberts, Maxwell School of Citizenship and Public Affairs,  
Syracuse University

Paper delivered at the 5th International Conference of Information Commissioners

time consuming or only the "troublemakers" use it. It is fundamental. The right to ensure that our personal information which is gathered by governments will remain private is equally as important. It is time to take steps to do what is necessary to include municipalities under our legislation. Perhaps the government could look more closely at the suggestion that the Government of the Northwest Territories fund or share the



cost of a position for one person who would work with all municipalities to address ATIPP issues so as to alleviate the costs concerns raised by the municipalities.

This new approach starts at the top, with this commitment from me: From now on, our digital infrastructure -- the networks and computers we depend on every day -- will be treated as they should be: as a strategic national asset. Protecting this infrastructure will be a national security priority.

We will ensure that these networks are secure, trustworthy and resilient. We will deter, prevent, detect, and defend against attacks and recover quickly from any disruptions or damage.

President Barak Obama

#### 4. **Electronic Records Management**

I would also repeat my recommendation that more attention has to be focused on the management of electronic records. Almost all of what we do today is done electronically. This comes with the significant challenges of finding ways to catalogue, organize and preserve this information, while maintaining a reasonable ability to access it. It will become ever more important to properly recognize and manage the records management life cycle. In my reviews I am seeing the results of this challenge.

E-mail communications are a particular challenge and if records are to remain accessible and available on an access request, it is increasingly important that everyone who uses e-mail to do the business of public bodies (which, of course, includes every person employed in any public body) properly records and preserves those communications in accordance with good record management practices so that when a record needs to be found, it is filed in such a way that it can be easily identified as responsive



and can be found without difficulties. The alternative will result in a complete inability to fully track and account for records created and the inevitable result will be public bodies who lack credibility and are completely unable to account to the public for their actions.

So what? If you have nothing to hide, why should you worry about any of this? As Daniel Solove points out in "I've Got Nothing to Hide, and Other Misunderstandings of Privacy," privacy isn't a single right to hide what you don't want others to see, but rather one which involves many facets and which protects societal interests. Uninhibited surveillance powers would chill free speech and association, even if completely legal.

Chen Shen, The Peak (Simon Fraser University) Monday, July 6, 2009

## **5. Protecting our Children**

Today's young people are growing up in an era in which computers are central to their lives. Most of them are far more comfortable with a computer and know more about how they can be used than their parents will ever be able to. In Canada today, the computer, almost by definition, includes access to the internet. It is estimated that more than 80% of Canadian homes are connected to the internet in some way. This is our children's reality....they use the internet to communicate with each other, to socialize with their friends, to explore their world and the world of others, to inform their lives. And while the Internet provides a way for our kids to connect with their peers in ways we could have never imagined a generation ago, there are a whole new set of risks that arise. And although many children well versed with the internet may well recognize the risks associated with their online activities, they most often they lack the knowledge or the will to avoid or reduce those risks. More must be done to educate our young people and to provide them with the knowledge they need to protect them-





selves while they work in the wired world, not only from the obvious risks of pedophiles and identity theft, but also from the less obvious and perhaps more insidious risks that lurk on line. I would recommend that consideration be given to including in school curriculums specific information about electronic medium and strategies for protecting children from on-line risks, beginning at the elementary school level .

From the other direction, the Freedom of Information Act is a stark reminder that a defining feature of modern democracy is that those elected to power and their officials are accountable to the people. The public has the right to know what is done in their name and with their money.

Freedom of information brings greater public understanding and less scope for impropriety, for decisions or for activities behind closed doors which jeopardize public confidence.

Richard Thomas, UK Information and Privacy Commissioner, Annual Report, 2009

## 6. **The Role of the Information and Privacy Commissioner**

The workload of the office of Information and Privacy Commissioner is becoming more significant as the public becomes more familiar with the Act and their rights under it. Each year, the necessary time commitment becomes more significant. The number of Requests for Review, particularly on the privacy side, are increasing year by year and the issues are becoming more and more complex, sometimes requiring significant amount of research.

At the moment, the Information and Privacy Commissioner role is filled on a part time “as needed” basis. Essentially, however, what this means is that the office is reactive, rather than proactive and I am convinced that there is a need for the office to be able



to address issues that arise outside of the review process and activities that the office could, and should, be participating in to strengthen the ideals and objectives of the legislation. For example, it would, I think, be appropriate for this office to be able to contribute more significantly to “Right to Know Week”, celebrated annually at the beginning of October throughout the country. I often feel, as well, that I do not have the time necessary to devote to keeping informed about the issues, particularly on the privacy side of the equation. Because of the pace of technological change, it takes a significant commitment of time to stay abreast of developments as they relate to privacy is-

Democratic progress requires the ready availability of true and complete information. In this way people can objectively evaluate their government's policy. To act otherwise is to give way to despotic secrecy.

-Pierre E. Trudeau

sues, but that time is often not available when the position is “part time”. It therefore becomes more and more difficult to maintain an appropriate level of expertise on some of the privacy issues. Furthermore, if Health Privacy legislation is passed in the next few years, and if the Information and Privacy Commissioner is given oversight functions under that legislation, there will likely be a significant increase in the workload of the office. Another of the mandates of the Information and Privacy Commissioner is to provide a public education component. This aspect of the office is not being well met because of the shortage of time to develop and deliver effective programs.



All this is to say that it may be that it is time to consider a different approach to the office, perhaps by making it a half time or even a full time position so as to ensure that the Information and Privacy Commissioner has the dedicated time to commit to these other aspects of the job that are otherwise difficult to address. This is not a “legislative” issue, as the Act requires only that there be an Information and Privacy Commissioner. It is, however, an issue which must be reviewed in terms of whether or not the mandate can be effectively met by the current approach. Alternatively, it may be that the Information and Privacy Commissioner’s office should be staffed with an investigator (on contract or otherwise) to carry out some of the functions of the office, to assist in investigations, with technical issues or with a public education campaign. The reality is that the time commitment necessary to do an adequate job is growing and eventually it will be necessary to expand the resources dedicated to the office. I would recommend that, along with a review of the Act, there be a review of the needs of the office with a view to determining whether a new approach should be taken.

From the other direction, the Freedom of Information Act is a stark reminder that a defining feature of modern democracy is that those elected to power and their officials are accountable to the people. The public has the right to know what is done in their name and with their money.

Freedom of information brings greater public understanding and less scope for impropriety, for decisions or for activities behind closed doors which jeopardise public confidence.

As we move into a more mature business-as-usual phase, public sector culture must continue to shift in favour of openness being the norm. There is no need to wait for requests. These can be sporadic, burdensome and disruptive. I have frequently advocated the ‘crown jewels’ approach - public bodies need to show they recognise the imperative of accountability (and make lives easier for themselves) by identifying what absolutely has to be kept secret and then proactively publishing other official information as a matter of routine.

Richard Thomas, UK Information and Privacy Commissioner, 2009 Annual Report

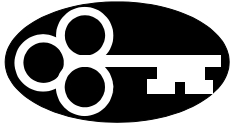


# RAPPORT ANNUEL 2008-2009

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

Elaine Keenan Bengts

Commissaire à l'information et à la protection de la vie privée



NORTHWEST  
TERRITORIES  
INFORMATION  
AND PRIVACY  
COMMISSIONER

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

Le 29 octobre 2009

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

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

**Objet : Présentation du rapport annuel**

Monsieur,

J'ai l'honneur de déposer mon rapport annuel devant l'Assemblée législative des Territoires du Nord-Ouest pour la période du 1<sup>er</sup> avril 2008 au 31 mars 2009.

Veillez 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



## INDEX

	Page
Message de la commissaire	47
La Loi	55
Rôle et mandat de la commissaire à l'information et à la protection de la vie privée	57
Processus de révision	60
Demandes de révision	61
Protection de la vie privée	62
Bilan de l'année	64
Recommandations relatives aux demandes de révision	65
Recommandation relative à la demande de révision n° 08-069	65
Recommandation relative à la demande de révision n° 08-070	67
Recommandation relative à la demande de révision n° 08-071	69
Recommandation relative à la demande de révision n° 08-072	71
Recommandation relative à la demande de révision n° 09-073	73
Recommandation relative à la demande de révision n° 09-074	73
Regard vers l'avenir	77



## MESSAGE DE LA COMMISSAIRE

La *Loi sur l'accès à l'information et la protection de la vie privée* (la « Loi ») des Territoires du Nord-Ouest a été adoptée en 1994, il y a environ 15 ans, et est entrée en vigueur en 1997. Elle confirme le droit légal de la population des Territoires du Nord-Ouest d'avoir accès aux renseignements du gouvernement et stipule les mécanismes permettant d'exercer ce droit. De plus, elle exige que les organismes du gouvernement territorial prennent des mesures positives pour protéger les renseignements personnels des particuliers.

La protection des données est cruciale pour le maintien des valeurs démocratiques fondamentales : une société de la surveillance risque de violer ce droit fondamental.

Thomas Hammarberg, commissaire aux droits de l'homme du Conseil de l'Europe

Durant les 15 années qui se sont écoulées depuis l'adoption de la Loi, le monde a changé. La technologie a changé notre façon de fonctionner de manière spectaculaire et bon nombre d'hypothèses fondamentales formant la base du processus ne sont plus valides. La tendance en faveur du « bureau électronique », la croissance prodigieuse des capacités d'emmagasinage des données, la prépondérance du courriel à titre de moyen de communication et l'utilisation toujours grandissante des technologies mobiles... tous ces éléments ont produit de nouveaux défis quant à la conservation de documents exacts et accessibles, ainsi qu'à l'assurance que les renseignements personnels sont sécurisés et utilisés seulement aux fins pour lesquels ils ont été colligés. Toutefois,



les buts fondamentaux de la Loi, qui étaient de rendre le gouvernement plus ouvert et plus transparent, et de rendre les fonctionnaires plus responsables à l'égard de la population des Territoires du Nord-Ouest, demeurent pertinents aujourd'hui, peut-être même encore plus qu'au moment de l'élaboration de la Loi. Les moyens pour atteindre ces buts ont changé, cependant.

Dans son rapport annuel 2008, le commissaire à l'information britannique, Richard Tho-

Le gouvernement ne devrait pas conserver des renseignements confidentiels pour la simple raison que des fonctionnaires pourraient être embarrassés par leur divulgation, parce que des erreurs et des échecs pourraient être révélés ou à cause de craintes spéculatives ou abstraites.

Président Barack Obama, 22 janvier 2009, note de service aux directeurs des ministères et agences

mas, a esquissé ce qu'une législation efficace en matière d'accès à l'information et de protection de la vie privée accomplira. Il estime que la législation est couronnée de succès quand il en découle :

une société où les droits et les responsabilités relativement aux renseignements sont respectés par tous;

des organismes qui inspirent la confiance en colligeant et en utilisant les renseignements personnels de manière responsable, sécuritaire et équitable;

une population qui comprend comment ses renseignements personnels sont utilisés, qui connaît ses droits et qui est confiante de pouvoir les exercer;

des pouvoirs publics ouverts et transparents, ayant comme pratique normale de donner accès aux renseignements officiels à la population;





une population qui connaît ses droits d'avoir accès aux renseignements officiels et est confiante de pouvoir les exercer.

Il s'agit là de buts louables. Il est possible d'édifier ce type de système robuste, mais seulement avec du zèle et un travail acharné. Cela exige une révision permanente de la législation, pour veiller à ce qu'elle reflète les réalités toujours changeantes de l'univers technologique et des systèmes gouvernementaux. Cela exige des systèmes pouvant indexer, retracer et contrôler des documents électroniques de toutes sortes. Cela exige la présence de coordonnateurs à l'information et à la protection de la vie privée émanant

Les citoyens confient le pouvoir et des ressources à leurs gouvernements, au moyen d'élections et de versement des impôts. Ceux à qui ce pouvoir est confié assument non seulement la responsabilité d'être au service des citoyens, mais aussi de les informer et d'encourager le public à participer à leurs décisions et à leurs mesures. - Après tout, ce sont les citoyens qui devraient être la source du pouvoir en dernier ressort, puisqu'ils supportent les conséquences de son abus.

Extrait du site Web de Transparency International

des échelons supérieurs du gouvernement qui soient capables d'interpréter la Loi, de prendre les décisions nécessaires et d'appliquer les politiques. Au sein d'un bon système, tous les coordonnateurs à l'information et à la protection de la vie privée se réuniraient régulièrement et collaboreraient en réseau pour veiller à l'application adéquate et systématique de la Loi dans tous les organismes publics. Un programme complet de formation pour tous les employés du secteur public, déjà en poste et débutant leurs fonctions, avec une formation plus approfondie pour ceux qui ont la responsabilité de traiter des renseignements personnels couramment, serait en place.



Tous les entrepreneurs seraient conscientisés au fait que les documents se rapportant au contrat sont tous assujettis à la Loi et seraient explicitement informés et éduqués au sujet de leurs obligations et de leurs responsabilités en vertu de la Loi. Il existerait un manuel pratique complet qui expliquerait les exigences de la Loi en langage clair et simple, avec des listes de vérification et des précédents afin d'aider lors des problèmes qui surgissent. Ce manuel serait consulté et utilisé constamment afin de régler des questions relatives à l'accès à l'information et à la protection des données. Nous n'en sommes pas encore tout à fait là.

Cependant, peut-être que l'élément le plus important s'avérant nécessaire serait un système de gestion de l'information moderne et efficace, applicable et réceptif aux défis de

Les réserves d'information gouvernementale ont été liquéfiées, fondues dans un vaste bassin d'éléments dont l'importance, prise de manière indépendante, n'est pas facilement comprise.

Extrait de *Blacked Out: Government Secrecy in the Information Age*, par Alasdair Roberts (New York : Cambridge University Press, 2006)

la tenue de dossiers électroniques, et doté de politiques de gestion des renseignements qui sont fermes et appliquées avec rigueur.

Dans le monde d'aujourd'hui, l'information est une denrée nécessaire. Toutefois, l'usage abusif ou la mauvaise gestion peut être une responsabilité empoisonnée. Comme l'a souligné Richard Thomas, le commissaire à l'information britannique, dans son rapport annuel 2009 :

Il doit exister une responsabilité claire sur la minimisation des renseignements – ne pas colliger plus de renseignements personnels qu'il n'est nécessaire et ne



pas les conserver plus longtemps que nécessaire. La qualité et le nettoyage des données vont probablement avoir une importance toujours plus grande – assurant que les bons renseignements se rapportent à la bonne personne, qu'ils sont exacts et qu'ils sont mis à jour. Bon nombre d'organismes décrivent les renseignements comme étant un bien de grande valeur, et ils peuvent certes l'être, s'ils sont bien gérés. Nous avons tenté de leur faire reconnaître que cela peut aussi rapidement devenir une grave responsabilité si les risques du traitement inadéquat des renseignements se matérialisent. Si les choses tournent mal, cela peut faire de véritables ravages à la carrière de certaines personnes, des réputations,

Il n'existe pas d'institution édiflée par les humains qui ne comporte pas de dangers. Plus l'institution est importante, plus les chances d'abus sont importantes. La démocratie est une grande institution et, par conséquent, elle est susceptible de subir de grands abus. Le remède n'est donc pas d'éviter la démocratie, mais d'en réduire la possibilité d'abus au minimum.

Mahatma Ghandi

des relations personnelles, des vies privées et des soldes bancaires. La réputation, la prospérité et la légitimité des organismes responsables peuvent également subir des dégâts importants.

Un bon système de gestion de l'information exige des lignes directrices claires sur la reddition des comptes et la responsabilité, des politiques et des procédures cohérentes et une application rigoureuse de ces politiques. Le système qui est en place pour les documents sur support papier est, pour la plupart, adéquat pour la tâche de traiter de tels documents. Il est loin de fonctionner aussi efficacement, cependant, pour le



traitement des documents électroniques.

Rappelons les propos de Sandy Hounsell, ancien commissaire adjoint à l'information et à la protection de la vie privée de Terre-Neuve-et-Labrador, dans une communication présentée à la 5<sup>e</sup> conférence internationale des commissaires à l'information :

Au cours des dernières années, l'explosion de l'information électronique est devenue un aspect crucial des systèmes modernes de gestion de documents. Le milieu de travail moderne s'est numérisé de plus en plus et notre

La responsabilisation et la transparence sont au cœur de la représentation, elles mettent en lumière des structures de pouvoir au sein de la démocratie, elles peuvent mettre à jour les partis pris et les intérêts personnels et, plus important encore, leur absence peut détruire la légitimité.

A.N. Tiwari

Commissaire à l'information, Commission de l'information centrale, Inde

niveau de confiance à l'égard des documents et des bases de données électroniques est sans précédent. On estime que plus de 90 % de tous les documents créés aujourd'hui sont électroniques.

Il ne fait aucun doute que les avantages sont nombreux. Nous pouvons faire des recherches dans les documents, en couper et coller des portions, les mettre à jour en temps réel, les envoyer par courriel, les automatiser, les vérifier, les sécuriser et les contrôler par des moyens que les systèmes sur papier ne peuvent tout simplement permettre. Au bout du compte, cela nous permet de travailler plus vite, d'épargner de l'ar-



gent et d'accomplir beaucoup plus avec bien moins d'effort. [...]

Toutefois, les organismes éprouvent souvent de la difficulté à cataloguer, organiser et préserver cette information tout en maintenant une capacité d'accès raisonnable. Cela est causé en partie par l'incapacité de plusieurs organismes de reconnaître et de gérer adéquatement le cycle de vie de la gestion des documents. Ce cycle de vie est tout aussi pertinent pour les documents sur papier que les documents électroniques, un fait souvent négligé par ces organismes. Toutefois, ce qui est encore plus important est que les organismes semblent être dépassés par le volume et la variété de documents électroniques. La technologie a tout simplement surpassé la capacité de réagir convenablement.

La législation est mise à l'épreuve et améliorée par l'usage et, si les gens ne s'en servent pas, l'accès à l'information est en grande partie inutile. À qui revient le rôle d'éduquer le public? Je dirais qu'il s'agit de la responsabilité de chaque organisme gouvernemental et de chaque fonctionnaire qui traite avec le public. L'accès à l'information devrait être inhérent à toutes les transactions d'un gouvernement avec ses citoyens.

Megan Carter, directrice, Information Consultants Pty Ltd

Je m'inquiète de plus en plus au sujet de la gestion des documents électroniques et, en particulier, de la gestion des communications effectuées par courriel. Autant que je sache, chaque employé est pratiquement laissé à lui-même pour gérer son système personnel de courriels à sa propre façon. Au-delà de quelques règles de base très simples, il n'y a aucune uniformité et aucune politique évidente. En dépit des règles, il y a peu ou pas de contrôle sur la façon dont les employés individuels gèrent leurs documents électroniques. Le droit d'accès à l'information est limité par la capacité du



gouvernement de trouver les documents. Si la gestion des dossiers est inégale, on aura de la difficulté à retracer des documents. J'ai déjà constaté plusieurs situations où il était clair que les documents existaient mais où l'organisme public avait été incapable de les retrouver à l'endroit où ils auraient dû être classés ou mémorisés.

Être doté d'un bon système de gestion de documents est tout aussi important pour les documents électroniques que ceux sur format papier. Les gouvernements doivent donc trouver une méthode plus efficace pour gérer les documents électroniques. Ce problème n'est pas particulier aux Territoires du Nord-Ouest. Il s'agit, en fait, de l'un des principaux problèmes avec lesquels tous les gouvernements sont aux prises, qu'ils soient grands ou

Un permis de conduire prouve que son détenteur a le droit de conduire une voiture. Ce n'est ni une pièce d'identité universelle ni un moyen approprié d'analyser les habitudes de retour de marchandises.

David Loukidelis

Commissaire à l'information et à la protection de la vie privée de la C.-B.

petits, situés au Canada ou à l'étranger. Sans de bonnes pratiques de gestion de documents, la capacité d'avoir accès à l'information devient difficile et sporadique. Sans la capacité, pour le gouvernement, d'avoir accès à l'information, la démocratie est menacée. La gestion efficace des documents électroniques est sans aucun doute un défi, mais il s'agit d'un défi qu'il faut réussir à relever.



## LA LOI

La *Loi sur l'accès à l'information et la protection de la vie privée* des Territoires du Nord-Ouest (la Loi) est entrée en vigueur le 31 décembre 1996. Elle a force exécutoire sur tous les ministères et certains organismes du gouvernement territorial précisés dans les règlements. Elle établit les règles des procédures selon lesquelles les organismes du gouvernement territorial colligent, utilisent et divulguent les renseignements personnels et selon lesquelles le public peut avoir accès aux documents du gouvernement.

La surveillance générale soulève des problèmes démocratiques graves que ne résolvent pas l'affirmation à répétition que ceux qui n'ont rien à cacher n'ont rien à craindre. Le fardeau est mal placé : c'est aux États qu'il devrait incomber de justifier leur ingérence dans les droits à la vie privée.

Thomas Hammarberg

Commissaire aux droits de l'homme du Conseil de l'Europe

Le terme « accès à l'information » désigne le droit d'accès du public aux documents généraux sur les activités du gouvernement, allant de l'administration et du fonctionnement à la législation et aux politiques. C'est là un aspect important d'un gouvernement ouvert qui répond de ses actes. En vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*, le public a le droit de consulter tous les « documents » en la possession ou qui relèvent d'un organisme public en faisant une demande d'accès à l'information. La plupart des documents du gouvernement sont visés par les dispositions de la Loi et doivent donc, par conséquent, être divulgués en cas de demande d'accès à l'information, sauf si un document est l'objet d'une des exceptions de divulgation spécifiques et limitées prévues dans la Loi. Les exceptions à la règle de divul-



gation ouverte servent à protéger les droits concernant la vie privée d'une personne, permettent aux représentants élus de rechercher et d'élaborer une politique et au gouvernement de diriger les « affaires » du gouvernement.

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 avec précision pour allouer le plus grand accès possible aux documents du gouvernement.

La Loi donne également aux individus le droit d'obtenir les renseignements que les orga-

On peut bien mettre en place un système de sécurité époustouflant. Mais si personne ne comprend comment l'utiliser, il déraillera. C'est là le facteur humain...

La formation à la sécurité ne peut se réduire à cocher une case, il faut qu'elle fasse en sorte que les gens comprennent les règles quotidiennes et leur raison d'être. [...] Il faut que cela fasse partie de la vie quotidienne des gens, pour qu'ils puissent faire le rapport avec ce qu'on leur demande de faire.

Martin Smith, président et fondateur, The Security Company

nismes gouvernementaux colligent à leur sujet et de demander que des corrections soient apportées à ces renseignements. Même si l'organisme public décide de ne pas faire la correction demandée, il faut noter au dossier qu'une demande de correction a été effectuée et décrire la nature de cette demande.

La protection de la vie privée est l'autre élément de l'équation législative et désigne la protection des renseignements personnels détenus par le gouvernement. La Loi pré-





voit des règles à suivre quant au moment et à la manière dont le gouvernement et ses organismes peuvent colliger, utiliser et divulguer des renseignements personnels et impose aux organismes publics l'obligation de prévoir les dispositifs de sécurité pour protéger les renseignements personnels qu'ils détiennent.

### **Rôle et mandat de la commissaire à l'information et à la protection de la vie privée**

Le Commissariat à l'information et à la protection de la vie privée (le Commissariat) existe en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée*. 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. Chaque année, elle rend des

Le second péché mortel est de prétendre à l'existence de l'accès à l'information tout en apportant un tel nombre d'exceptions et de dérogations au principe que cela compromet la matérialisation d'un véritable changement de culture dans l'administration publique.

Juge Michael Kirby, Cour suprême de l'Australie (alors président de la Cour d'appel de Nouvelle-Galles du Sud)

comptes à l'Assemblée législative des Territoires du Nord-Ouest et paraît habituellement une fois l'an devant le Comité permanent des priorités et de la planification pour discuter de son rapport. En tant que représentante indépendante, elle ne peut être destituée ou suspendue qu'en « raison de son empêchement » sur la recommandation de l'Assemblée législative.

La commissaire à l'information et à la protection de la vie privée joue plusieurs rôles en



vertu de la Loi, notamment :

- revoir de manière indépendante les décisions et les pratiques des organismes gouvernementaux concernant l'accès à l'information et la protection de la vie privée, ainsi que faire des recommandations aux organismes publics relativement à ces décisions et à ces pratiques;
- faire des commentaires et donner des conseils sur les lois et les programmes proposés par le gouvernement;
- éduquer le public au sujet de la Loi.

Même si nous avons constaté un changement massif dans la capacité des organisations à exploiter la technologie moderne qui utilise nos renseignements pour la prestation des services, il ne s'est pas accompagné d'une force motrice similaire pour élaborer de nouvelles mesures de protection de la vie privée efficaces sur les plans technique et procédural.

Richard Thomas, commissaire à l'information du R.-U.

En matière de résolution de problèmes d'accès à l'information, la commissaire à l'information et à la protection de la vie privée n'a qu'un pouvoir très limité de rendre des ordonnances exécutoires sur les affaires qu'on lui soumet. Dans la plupart des cas, son rôle s'apparente plus à celui d'un ombudsman. Elle présente des recommandations qui sont persuasives mais non exécutoires. En ce qui concerne les demandes d'accès à l'information, les recommandations sont présentées au responsable de l'organisme public impliqué, qui doit ensuite prendre une décision finale sur la divulgation ou la non-divulgation des renseignements. Si la personne qui voulait accéder à des renseignements n'est toujours pas satisfaite de la réponse du responsable de l'orga-



nisme public à l'issue du processus de révision, le recours est de faire appel à la Cour suprême des Territoires du Nord-Ouest, qui tranchera définitivement l'affaire.

La commissaire à l'information et à la protection de la vie privée est également autorisée, en vertu de la Loi, à faire enquête sur les plaintes pour atteinte à la vie privée. À la conclusion de son enquête, la commissaire indique s'il semble y avoir eu atteinte ou non

Les répercussions d'une mauvaise gestion des documents vont bien plus loin que les problèmes d'accès et de protection des renseignements personnels. Au sein même du gouvernement, le manque d'information exacte et sûre donne lieu à des décisions médiocres, à des programmes ratés et à des possibilités perdues. [...] L'incapacité à protéger des documents de grande valeur sur le plan de la propriété juridique et intellectuelle accroissent [sic] les problèmes de responsabilité et font augmenter les pertes financières. La destruction prématurée de documents à valeur archivistique contribue à notre amnésie historique et à la perte d'un savoir important.

L'hon. John Reid, commissaire à l'information au Canada

Rapport annuel du commissaire à l'information 2002-2003

à la vie privée de l'individu. Peu importe les résultats de son enquête, la commissaire formulera normalement des recommandations à l'intention de l'organisme public concerné sur les systèmes, les politiques et les procédures qui pourraient contribuer à améliorer la sécurité et éviter de futures divulgations inappropriées. L'organisme public doit réagir aux recommandations qui lui ont été adressées dans un délai de 60 jours, mais la Loi ne prévoit aucun appel au sujet de la réaction d'un organisme public en matière de plainte pour atteinte à la vie privée.



## Processus de révision

Les demandes d'accès à l'information doivent être faites par écrit et envoyées à l'organisme public auprès de qui l'information est recherchée. Bien que des formulaires soient disponibles, les demandes de renseignements n'ont pas à être présentées sur aucun formulaire particulier. La seule exigence est que la demande soit faite par écrit. Cela comprend une demande faite par courriel, mais une telle demande pourrait ne pas être considérée comme étant complète avant que l'organisme public ne reçoive confirmation de la demande signée par le requérant. Des droits de 25,00 \$ s'appliquent aux deman-

Les bases de données ne sont pas seulement des listes, ni l'équivalent numérique de dossiers sur support papier. Les bases de données structurées donnent la possibilité de « demander » des données selon de nouveaux paramètres, permettant à des appareils d'extraire des échantillons de renseignements et de produire de nouveaux renseignements à partir de cela. Par conséquent, l'état-base de données est un appareil bureaucratique qui est en fait dirigé par des appareils. En tant que tel, cela promet de déshumaniser à la fois la fonction publique de première ligne et les gens qui en dépendent le plus.

Becky Hogge, dans le magazine *New Statesman*, 30 avril 2009

des de renseignements, sauf si l'information demandée correspond aux propres données personnelles du requérant. Dans de tels cas, aucun droit ne s'applique, bien que des droits puissent être exigés pour copier des documents dans certaines circonstances.

Sur réception d'une demande de renseignements, l'organisme public a l'obligation de déterminer tous les documents éclairants pour la demande et de répondre à celle-ci dans un délai de 30 jours. Une fois que tous les documents éclairants ont été déterminés, ils sont examinés pour établir s'il y a des documents ou des parties de documents qui ne devraient pas être divulgués en vertu des dispositions de la Loi. L'orga-



nisme public doit s'efforcer de fournir au requérant le plus de renseignements possible, tout en respectant les exceptions de divulgation limitées qui sont désignées dans la Loi. Il est interdit aux organismes publics de divulguer certains types de documents. Dans certains cas, l'organisme public peut, à sa discrétion, décider de divulguer ou non les documents. Ces exceptions discrétionnaires exigent que l'organisme public considère s'il doit divulguer ou non les renseignements, en gardant à l'esprit les fins de la Loi et la force du pouvoir de la Cour, qui exige que les organismes publics pêchent plutôt par l'excès de divulgation.

Toute personne a le droit de demander des renseignements à son sujet. Si un individu

Pour ma part, je ne crois pas qu'un protocole médiocre de gestion de documents constitue une raison suffisamment appropriée pour refuser à un requérant l'accès à de l'information à laquelle il a légitimement droit. Cela fait ressortir l'importance de traiter tous les documents, tant électroniques que sur support papier, d'une manière qui se prête favorablement à l'accès, à la sécurité et à la conservation.

Sandy Hounsell

Ancien commissaire adjoint à l'information et à la protection de la vie privée de Terre-Neuve-et-Labrador

découvre des renseignements qui le concernent dans un document du gouvernement et qu'il croit que ces renseignements sont trompeurs ou incorrects, il peut faire une demande par écrit pour faire 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.

### **Demandes de révision**

En vertu de l'article 28 de la *Loi sur l'accès à l'information et la protection de la vie pri-*



vé, une personne qui a demandé des renseignements auprès d'un organisme public, ou une tierce partie qui peut être touchée par la divulgation des renseignements par un organisme public, peut s'adresser à la commissaire à l'information et à la protection de la

Un travail de pédagogie doit être rapidement initié en direction des plus jeunes, peu conscients des risques que présente leur fréquentation assidue des nouvelles technologies de communication. Si rien n'est fait aujourd'hui, les générations futures pourront-elles encore prétendre demain à une « bulle » de vie privée?

Extrait de « Protéger la vie privée dans un monde sans frontières », dans le site Web de la 30<sup>e</sup> conférence internationale des commissaires à la protection des données et de la vie privée, Strasbourg, France, octobre 2008

### Protection de la vie privée

La Partie II de la *Loi sur l'accès à l'information et la protection de la vie privée* décrit les règles régissant 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 aussi 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.

En vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* modifiée, la commissaire à l'information et à la protection de la vie privée a le pouvoir de revoir



les plaintes pour atteinte à la vie privée dans les cas où les membres du public s'inquiètent du fait que leurs renseignements personnels ont été inadéquatement colligés, utilisés ou divulgués par un organisme public. Lorsque les recommandations sont faites, l'organisme public dispose de quatre-vingt-dix jours pour y réagir. Toutefois, on ne peut faire appel devant la Cour, à moins que l'individu ne cherche à porter une accusation en vertu de l'article 59 de la Loi.

Dans tous les cas, la commissaire déterminera s'il y a ou non possibilité que la question soit résolue au moyen de la médiation ou d'une autre intervention sans devoir réaliser une révision complète. C'est là souvent tout ce qu'il faut pour résoudre la question à la satisfaction du requérant ou du plaignant. Toutefois, si une résolution par médiation ne semble pas possible, la question passe à une révision plus en profondeur.

Toutes les parties concernées, y compris l'organisme public et les tiers dont les renseignements pourraient être divulgués, ont la possibilité de faire des présentations par écrit concernant les problèmes.

Pour ce qui est de la sensibilisation publique, tous les commissaires canadiens travaillent actuellement à une telle campagne ciblant les jeunes publics, pour les aider à comprendre les risques inhérents à la vie privée et aux renseignements personnels qui découlent de l'utilisation des sites de réseautage social.

Jennifer Stoddart, commissaire à la protection de la vie privée au Canada, dans une allocution à la 30<sup>e</sup> conférence internationale des commissaires à la protection des données et de la vie privée, Strasbourg, France, octobre 2008



## Bilan de l'année

Durant l'exercice 2008-2009, le Commissariat à l'information et à la vie privée a ouvert 15 dossiers dans les diverses catégories énumérées ci-dessous :

- Plaintes pour atteinte à la vie privée 4
- Demandes de révision (concernant l'accès à l'information) 9
- Demandes de commentaires 1
- Atteintes à la vie privée (secteur privé) 1

Nous avons toujours la confiance du public. Mais la confiance n'est pas une ressource renouvelable. Lorsqu'on la perd, on ne peut pas la recouvrer.

Mary Lysyk, conseillère en matière de politiques pour Santé Canada

Les demandes de révision reçues ont touché les sept organismes publics suivants :

- l'Administration des services de santé et des services sociaux de Hay River 6
- le ministère de la Justice 2
- l'Administration scolaire de district n° 1 de Yellowknife 1
- le ministère de l'Éducation, de la Culture et de la Formation 1
- le ministère de l'Exécutif 1
- le ministère des Ressources humaines 1
- la Société d'énergie des TNO 1





## RECOMMANDATIONS RELATIVES AUX DEMANDES DE RÉVISIONS

### Recommandation relative à la demande de révision n° 08-069

Dans ce cas, la plaignante estimait qu'une personne travaillant au sein du gouvernement des Territoires du Nord-Ouest avait divulgué des renseignements personnels à son égard. Elle avait fourni ses renseignements personnels à un organisme public dans le cadre d'une demande de subvention. Plus tard, un de ses amis l'informa qu'il avait en-

Dans le Nord, où la faible population signifie qu'il existera toujours une probabilité élevée que les employés du gouvernement seront au fait, jusqu'à un certain point, des renseignements d'une autre personne qu'ils connaissent, il est important de s'assurer de la mise en place de mesures de protection adéquates pour prévenir l'utilisation ou la divulgation inappropriée de ces renseignements.

Elaine Keenan Bengts, recommandation relative à la demande de révision n° 08-069

tendu dire qu'elle avait présenté une demande pour cette subvention et qu'elle avait peut-être fourni des renseignements trompeurs dans sa demande. La plaignante savait qu'un ami personnel très proche de son ami travaillait à l'organisme public concerné et était convaincue que cette personne avait indûment divulgué les renseignements contenus dans sa demande. Elle essaya de régler la question directement avec l'organisme public, mais ne fut pas satisfaite de l'issue de ses démarches. Par la suite, elle déposa une plainte auprès de la commissaire à l'information et à la protection de la vie privée.



À la fin de son enquête, la commissaire admit qu'il était difficile, en ces circonstances, de confirmer avec certitude s'il y avait bien eu, en fait, atteinte à la vie privée d'une personne, à moins de disposer de moyens pour confirmer qui avait eu accès au dossier de la plaignante et à quelle fin. Elle souligna qu'il en revient presque toujours, en de telles circonstances, à la parole de la plaignante contre celle de l'employé. Elle indiqua que, même s'il était impossible de déterminer en toute certitude s'il y avait eu une divulgation induite des renseignements de la plaignante, il était plus que probable que l'employé de l'organisme public avait indûment divulgué ces renseignements personnels. Toutefois, comme cet employé ne travaillait plus pour l'organisme public, aucune recommandation

De plus, pour déterminer s'il est privilégié, chaque document doit respecter les trois critères :

- (i) il doit constituer une communication entre un avocat et un client;
- (ii) il doit impliquer qu'on demande ou qu'on donne des conseils juridiques;
- (iii) il doit être entendu comme étant confidentiel par les parties.

Elaine Keenan Bengts, recommandation relative à la demande de révision n°

spécifique n'a été formulée à son égard. La commissaire à l'information et à la protection de la vie privée a plutôt fait des recommandations pour aider l'organisme public à prévenir des divulgations similaires à l'avenir. Plus précisément, elle recommanda que l'organisme public établisse un protocole pour traiter les plaintes sur les manquements possibles à la confidentialité des renseignements personnels et que ce protocole devrait inclure le coordonnateur de l'information et de la protection de la vie privée de l'organisme public à titre de participant actif au processus. Elle suggéra de plus que ce protocole comprenne l'obligation de garder un dossier décrivant par écrit les mesures prises durant l'enquête sur la plainte, les résultats et les mesures prises pour résoudre les lacunes.



### Recommandation relative à la demande de révision n° 08-070

Dans ce cas, le requérant demandait une révision de la décision du ministère de l'Industrie, du Tourisme et de l'Investissement de lui avoir refusé l'accès à un rapport particulier. Le requérant avait aussi demandé accès à la correspondance, aux courriels, aux notes documentaires et aux autres documents associés au rapport ou qui en discutaient le contenu et, tout particulièrement, à tout document mentionnant pourquoi le gouvernement des Territoires du Nord-Ouest avait décidé de ne pas rendre le rapport public.

Bien que je sois heureuse que la question ait été réglée par la suite, je ne m'attends pas à ce qu'on me demande de fournir un engagement d'avocat relativement à l'examen de documents dans le cadre des futures demandes de révision, peu importe le degré de confidentialité que pourrait attribuer l'organisme public à cette information. Je m'attends plutôt à ce que tous les organismes publics respectent le Commissariat à l'information et à la protection de la vie privée et acceptent que le serment professionnel du commissaire et les dispositions de la loi qui le lient suffisent à garantir que la teneur des documents reçus aux fins d'une demande de révision ne sera pas indûment divulguée par le commissaire.

Elaine Keenan Bengts, recommandation relative à la demande de révision n° 08-070

Dans ce cas, l'organisme public avait clairement indiqué dès le départ qu'il considérait le document en question comme étant de nature extrêmement confidentielle et n'était pas du tout intéressé à le divulguer. En fait, il a refusé de fournir une copie du document à la commissaire à l'information et à la protection de la vie privée, en dépit des articles mêmes de la Loi donnant à la commissaire le pouvoir de prendre connaissance de tous les documents visés par une demande de révision. L'organisme public a invoqué toutes les exemptions en vertu de la Loi auxquelles il pouvait penser, dont :



- l'article 15 (privilege des communications entre client et avocat);
- l'alinéa 14(1)(a) (avis élaboré par ou pour un organisme public);
- l'article 13 (renseignements confidentiels du Conseil exécutif);
- l'article 16 (divulgarion risquant de nuire aux relations intergouvernementales);
- l'article 17 (divulgarion risquant de porter préjudice à l'intérêt économique du gouvernement);
- l'article 24 (divulgarion risquant de porter préjudice à l'intérêt économique de tiers).

Il me semble que l'esprit et la lettre de la *Loi sur l'accès à l'information et la protection de la vie privée* suggèrent que, si une personne demande qu'on mette fin à un procédé de collecte ou de divulgation de ses renseignements personnels auquel elle a donné son consentement, cela signifie que le consentement rattaché à la demande originale est également révoqué. Par la suite, la CAT n'aurait pas le moindre droit d'utiliser ou de divulguer les renseignements personnels du requérant.

Elaine Keenan Bengts, recommandation relative à la demande de révision n° 08-071

Après avoir pris connaissance du rapport, la commissaire a conclu que le rapport était visé par le privilège des communications entre client et avocat, que l'organisme public avait considéré la question à fond et qu'il avait usé de son pouvoir discrétionnaire en refusant de divulguer le rapport.

Toutefois, la commissaire a sévèrement critiqué l'organisme public pour le traitement de cette demande et le manque de respect à l'égard du Commissariat, comme l'attestait la réticence à lui fournir une copie du rapport qui faisait l'objet d'une demande d'accès à l'information. Elle fit remarquer que la Loi donne à la commissaire à l'information et à la protection de la vie privée le droit de prendre connaissance de tous les documents visés par les dispositions de la Loi, tout en lui interdisant en même temps de divulguer le contenu de tels documents.



Les recommandations formulées furent acceptées, bien qu'aucun commentaire n'ait été fait concernant les inquiétudes de la commissaire sur la manière dont la demande avait été traitée

Il est impératif que les institutions tiennent un relevé de l'utilisation et de la communication de renseignements personnels qui relèvent d'elles. Sauf dans un nombre de cas limité, les personnes ont le droit de savoir quels documents contenant leurs renseignements personnels sont envoyés, à qui ils sont envoyés et la raison pour laquelle ils sont communiqués.

Robert Marleau, commissaire à la protection de la vie privée du Canada, Rapport annuel au Parlement 2002-2003

### **Recommandation relative à la demande de révision n° 08-071**

Ce cas traitait d'une autre préoccupation relative à un cas possible d'atteinte à la vie privée. Le plaignant craignait que ses renseignements médicaux personnels aient été indûment divulgués par la Commission des accidents du travail (désormais la Commission de la sécurité au travail et de l'indemnisation des travailleurs). Le plaignant avait déposé une réclamation auprès de la Commission des accidents du travail (CAT) alléguant souffrir d'un trouble de stress post-traumatique à la suite d'un accident ayant eu lieu environ huit ans auparavant à un site de travail éloigné, alors qu'il travaillait pour l'« employeur A ». En déposant sa plainte, le plaignant avait indiqué le nom de son employeur actuel par erreur, au lieu de celui de son ancien employeur. Pour justifier sa réclamation, il avait aussi présenté une chronologie de ses emplois depuis l'accident qu'il affirmait avoir causé son problème, sur laquelle il a nommé plusieurs autres employeurs. La CAT fit enquête et, ce faisant, communiqua avec plusieurs des anciens employeurs du plaignant. Le plaignant demanda par la suite que



sa plainte soit mise en attente, ce à quoi la CAT se conforma en premier lieu. Toutefois, pour une raison ou une autre, elle reprit l'enquête plus tard sans que le plaignant le sache. En reprenant l'enquête, la CAT communiqua avec l'employeur actuel du plaignant pour lui poser de nombreuses questions et, apparemment, divulgua au moins quelques éléments sur la nature de la réclamation du plaignant. Malheureusement, la communication avec l'employeur actuel du plaignant coïncida avec un conflit distinct entre le plaignant et cet employeur. Cela exacerba le problème du plaignant avec son employeur actuel et il me demanda donc de me pencher sur la situation. À titre de problème secondaire, le plaignant, qui avait demandé à avoir accès à son dossier, s'inquiétait à propos d'u-

Toutes les parties concernées s'entendent pour dire que les renseignements personnels, en l'occurrence un pronostic sur l'état pathologique du plaignant, n'ont jamais été fournis. Il n'y a donc eu, par conséquent, aucune « collecte » de renseignements. Ceci clôt la question. Si aucune collecte de renseignements n'a eu lieu, il n'y a rien à revoir.

Elaine Keenan Bengts, recommandation relative à la demande de révision n° 08-072

ne mention portée à son dossier et relative à des allégations soulevées par son employeur actuel au sujet d'un de ses comportements.

Après avoir terminé son enquête, la commissaire était convaincue que la CAT connaissait son obligation de confidentialité et ses obligations de ne pas utiliser ou divulguer des renseignements personnels, sauf en se conformant à la législation. Elle ne fut pas entièrement persuadée, cependant, que ces concepts étaient entièrement compris ni que les procédés en place suffisaient à respecter ces obligations .

Elle recommanda que tous les gestionnaires des réclamations reçoivent une formation de base sur les dispositions relatives à la confidentialité de la *Loi sur l'accès à l'information et la protection de la vie privée* pour assurer qu'ils comprennent complètement



leurs obligations de préserver la confidentialité des renseignements personnels des requérants et des autres personnes.

Elle recommanda en outre que des politiques soient élaborées et adoptées pour exiger que les gestionnaires de cas consultent un requérant directement avant de mener une enquête pour clarifier les problèmes qui semblaient nécessiter des clarifications, comme l'identité de l'employeur du plaignant au moment de l'accident menant à la réclamation.

Enfin, elle s'inquiéta de l'apparence de divulgation indue de certains des renseignements personnels du plaignant par la CAT à l'employeur actuel du plaignant. Elle recommanda que la CAT prenne des mesures pour récupérer les renseignements indûment divulgués et tente d'atténuer le plus possible toute retombée de cette divulgation indue de renseignements.

Les recommandations de la commissaire à l'information et à la protection de la vie privée furent acceptées.

J'estime qu'une partie au moins de l'information supprimée constitue des renseignements personnels tant au sujet du requérant que des tiers. Dans de telles situations, les commissaires à l'information et à la protection de la vie privée de partout au Canada ont conclu que le droit d'un particulier d'obtenir des renseignements personnels à son égard est parfois limité par des facteurs sur la vie privée des tiers.

Elaine Keenan Bengts, recommandation relative à la demande de révision n° 09-073

### **Recommandation relative à la demande de révision n° 08-072**

Dans ce cas, le plaignant a demandé que j'examine si le Secrétariat du conseil de gestion financière avait correctement colligé ses renseignements personnels. Ce plaignant était un employé du gouvernement des Territoires du Nord-Ouest. On lui avait demandé de fournir une attestation de son médecin confirmant qu'il était en mesure de s'acquitter



des fonctions de son emploi. Le plaignant s'était opposé à cette demande.

L'organisme public alléguait que le comportement du plaignant avait été imprévisible, insubordonné et non professionnel, et qu'il avait reçu des avertissements sur ses actions mais avait refusé de se conformer aux directives données. Le plaignant avait été mis en congé pour insubordination et avait lui-même prétendu souffrir d'une maladie causée par le stress. En conséquence, l'employeur demanda au plaignant de subir une évaluation de santé mentale, de manière à pouvoir déterminer si des adaptations s'avéraient nécessaires.

La question de savoir si des renseignements peuvent ou doivent être supprimés des documents nécessaires à une enquête doit relever de l'exception et reposer sur les circonstances relatives à chaque cas. Le caractère confidentiel des enquêtes sur des plaintes en milieu de travail peut constituer un facteur contextuel approprié dans de tels cas, mais les règles qui visent de tels documents en vertu de la Loi sont les mêmes que celles qui s'appliquent aux renseignements personnels présents dans des documents d'autres types.

David Loukidelis, ordonnance n° 01-53, commissaire à l'information et à la protection de la vie privée de la C.-B.

Le plaignant s'opposa à l'évaluation et finit par retourner au travail sans subir d'évaluation. Finalement, l'employeur décida que, comme le plaignant était parvenu à reprendre ses fonctions sans avoir besoin d'adaptation, la demande d'évaluation de santé mentale était superflue et la retira.

La commissaire à l'information et à la protection de la vie privée a conclu que l'organisme public n'avait pas colligé de renseignements personnels et que, par conséquent, il n'y avait pu se produire de collecte « induite ». Elle ne formula aucune autre recommandation.





### **Recommandation relative à la demande de révision n° 09-073**

Ce cas découle d'une demande d'accès à l'information effectuée par un ancien employé d'un organisme public, afin d'obtenir la version inédite d'un rapport rédigé par un entrepreneur externe concernant une plainte pour harcèlement en milieu de travail portée contre le requérant. L'organisme public divulga le document, mais avait rédigé la plus grande partie du rapport de manière à ce que sa teneur ne soit pas divulguée. Le requérant s'inquiétait aussi que les parties du rapport qu'il avait reçues étaient inexactes et ne reflétaient pas les déclarations qu'il avait faites à l'enquêteur. Outre cela, il affirma ne pas avoir eu la possibilité de revoir et de corriger les parties du rapport reflétant ses dé-

Bien que la Loi n'impose pas de norme de perfection, il est bien établi que, lorsqu'il effectue des recherches pour trouver des documents, un organisme public doit adopter une marche à suivre à laquelle une personne juste et rationnelle s'attendrait ou qu'elle considérerait acceptable. La recherche doit être minutieuse et complète. Les preuves devraient décrire toutes les sources potentielles de documents, énumérer ceux qui ont fait l'objet d'une recherche et mentionner les sources qui n'ont pas fait l'objet d'une recherche et les raisons de cette absence de recherche. Les preuves devraient aussi faire état de la manière dont les recherches ont été effectuées ainsi que le temps consacré par le personnel de l'organisme public à la recherche de documents.

David Loukidelis, commissaire à l'information et à la protection de la vie privée de la C.-B., ordonnance n° 02-03

clarations à l'enquêteur avant que ce rapport soit présenté à l'organisme public. Pour justifier son refus de divulguer les parties restantes du rapport, l'organisme public s'appuya sur les articles 14 et 23 de la Loi. Le paragraphe 14 (1) donne à un organisme public le pouvoir discrétionnaire de refuser de divulguer des renseignements dans le cas où la divulgation risquerait vraisemblablement de révéler des avis, des propositions, des recommandations, des analyses ou des options de politiques élaborés par ou pour un organisme public. L'article 23 interdit de divulguer des renseignements personnels dans le cas où la divulgation constituerait une atteinte déraisonnable à la vie privée d'un tiers.



Après avoir pris connaissance du rapport et tenu compte des articles pertinents de la Loi, la commissaire à l'information et à la protection de la vie privée conclut que, bien qu'une partie des renseignements du rapport pouvait avoir été protégée contre la divulgation à titre de renseignements personnels de tiers, et que la divulgation correspondrait à une atteinte déraisonnable de leur vie privée, avant de refuser catégoriquement la divulgation, l'organisme public aurait dû consulter les tiers pour déterminer s'ils s'opposeraient à cette divulgation en vertu de l'article 26 de la Loi. Elle recommanda, en outre, qu'une grande partie du rapport soit divulguée, en supprimant les renseignements personnels.

Les recommandations furent acceptées.

Il me semble que, lorsqu'un requérant demande à un organisme public de faire des recherches dans des documents de sauvegarde, ce qui serait habituellement considéré comme dépassant de beaucoup les méthodes normales de recherche, il incombe à ce requérant de fournir des éléments pour justifier le besoin d'une recherche de ce type.

Elaine Keenan Bengts, recommandation relative à la demande de révision n° 09-074

#### **Recommandation relative à la demande de révision n° 09-074**

Dans cette demande de révision, le requérant recherchait des renseignements que le ministère de l'Éducation pouvait détenir à son sujet relativement à son aide financière à titre d'étudiant ou à sa bourse du millénaire pendant une certaine période. Il était tout particulièrement intéressé par des courriels entre certains employés du ministère dont il indiqua les noms. L'organisme public répondit à la demande, mais le requérant ne fut pas satisfait des résultats et demanda que l'organisme public fasse des recherches dans son système de secours pour récupérer des courriels qui avaient été supprimés.



L'organisme public adopta la position suivante : il avait effectué une recherche approfondie en tout premier lieu et concluait que tous les documents pertinents avaient été fournis. Il refusa de faire des recherches dans les documents de sauvegarde comme le demandait le requérant. À son avis, l'article 7 de la Loi exigeait seulement une « aide raisonnable » de sa part au requérant et que cette obligation avait été satisfaite par la recherche des documents actuels. Il avança que la recherche dans les documents de sauvegarde s'avérerait extrêmement difficile et exigerait beaucoup de temps, qu'il était improbable que de quelconques documents supplémentaires retrouvés dans le système de secours n'aient pas déjà été découverts lors de la première recherche pour plusieurs rai-

Dans *Dagg c. Canada (Ministre des Finances)* [1997] 2 R.C.S. 403, le juge La Forest a fait une remarque sur l'objet de la loi en matière d'accès à l'information avec laquelle la majorité des juges de la Cour suprême du Canada était d'accord. Il a dit :

La loi en matière d'accès à l'information a pour objet premier de favoriser la démocratie en aidant à garantir que les citoyens possèdent l'information nécessaire pour participer utilement au processus démocratique et que les politiciens et les bureaucrates demeurent redevables envers l'ensemble de la population.

Cet important objet de la loi serait mis en échec si un organisme public pouvait tout simplement refuser de faire des recherches dans ses documents à cause des coûts et de l'affectation de main-d'œuvre.

Frank Work, ordonnance n° F2007-028, commissaire à l'information et à la protection de la vie privée de l'Alberta

sons, dont la « politique courante » de la division voulant que les courriels concernant les clients soient sauvegardés soit dans le dossier du client, soit par l'agent qui traitait avec le client. L'organisme public était d'avis que, à moins que le requérant puisse fournir des preuves justifiant son soupçon que les courriels qu'il recherchait existaient véritablement, effectuer des recherches dans le système de secours dépassait les exigences raisonnables de la Loi.



La commissaire à l'information et à la protection de la vie privée avança que, comme la Loi établit que la norme est la « décision raisonnable », il n'y avait pas d'absolus et que chaque cas devait être tranché à partir de ses propres faits. Ce qui s'avère raisonnable dans un cas, selon les faits et les preuves qui l'entourent, peut ne pas l'être dans un autre, avec d'autres faits et preuves. Dans ce cas, la commissaire était d'avis que le ministère avait respecté la norme de la décision raisonnable pour de nombreuses raisons. Premièrement, elle était convaincue que la recherche effectuée dans les documents actuels et existants avait été approfondie et à grande échelle. Deuxièmement, elle était persuadée, grâce aux explications fournies par l'organisme public sur la nature du systè-

Serions-nous heureux sous un régime de tyrannie efficace – un régime au sein duquel chaque mouvement et chaque action d'un citoyen seraient instantanément consignés, analysés et contre-vérifiés et aucun incident, peu importe sa banalité, ne serait jamais oublié?

Professeur A.S. Douglas, London School of Economics,  
*Science Journal*, octobre 1970

me de secours, qu'il était improbable que des documents supplémentaires soient retrouvés. Troisièmement, bien qu'il eut bénéficié de la possibilité de le faire, le requérant ne lui fournit aucune autre justification que ses propres soupçons que d'autres documents existaient. Elle recommanda qu'aucune autre mesure ne soit prise.

Les recommandations furent acceptées.



## REGARD VERS L'AVENIR

La *Loi sur l'accès à l'information et la protection de la vie privée* est maintenant en vigueur depuis environ 13 ans. Chaque année, je fais des recommandations de changements afin de rendre le système plus accessible, plus efficace et plus efficient. Il y a toujours place à l'amélioration, et les recommandations suivantes sont formulées en vue de continuer à améliorer et à renforcer la Loi en tant que mécanisme produisant un gouvernement plus ouvert et plus responsable.

En bref, Privacy by Design désigne la philosophie et l'approche de la vie privée imbriquées dans les normes de conception de diverses technologies. Cela peut être réalisé en intégrant les principes des pratiques équitables sur la protection de l'information dans la conception, le fonctionnement et la gestion des systèmes et des technologies de traitement de l'information.

Ann Cavoukian, Ph.D., commissaire à l'information et à la vie privée de l'Ontario

### **1. Révision générale de la *Loi sur l'accès à l'information et la protection de la vie privée***

Au cours des 13 dernières années, le recours à la *Loi sur l'accès à l'information et la protection de la vie privée* a révélé des points faibles et le besoin de clarifier certains éléments. La technologie d'aujourd'hui diffère totalement de ce qui a été envisagé quand la présente Loi a été adoptée. Les législateurs de l'époque ne pouvaient prévoir la prépondérance du courriel comme moyen de communication ou l'importance de la tendance à adopter les documents électroniques comme principale méthode de tenue de dossiers. Comme pour la plupart des lois, il faut évoluer selon les réalités changeantes et résoudre les problèmes qui surgissent de temps à autre. La capacité grandissante



de conserver des quantités de renseignements toujours plus importantes devrait s'accompagner d'une vigilance accrue. Plusieurs provinces et territoires du Canada ont récemment révisé leurs lois et leur apportent ou leur ont apporté des modifications pour combler les lacunes de la législation, afin de relever les nouveaux défis de l'ère électronique. 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 21<sup>e</sup> siècle et pour remédier à certains des problèmes soulevés dans mes rapports annuels au fil des ans.

## **2. Fusions des conseils et des organismes**

Le présent gouvernement a proposé que plusieurs conseils et organismes soient fusionnés en un nombre considérablement plus petit de conseils et d'organismes. Si je comprends bien cette proposition, cela pourrait bien impliquer la fusion d'organismes dotés de mandats différents, actuellement, comme les administrations scolaires et les organismes de services de santé et de services sociaux. Je suis très préoccupée par les répercussions que cela pourrait avoir sur la vie privée des particuliers. Il existe très peu d'information quant à la façon dont ces fusions fonctionneraient et ce que serait la vision à long terme pour de tels organismes. Comment le gouvernement conçoit-il la façon dont ces plus grands organismes s'emboîteront l'un à l'autre? Ces fusions en-



traîneraient des préoccupations et des difficultés importantes en matière de protection de la vie privée, car ces organismes possèdent tous d'importantes quantités de nos renseignements personnels. Ces questions relatives à la protection de la vie privée doivent être réglées au stade de la mise en œuvre. Sinon, elles deviendront indubitablement un problème dans l'avenir, et il sera bien plus difficile d'y remédier à ce moment.

En Ontario, mon homologue a préconisé « Privacy by Design ». Ce concept a été élaboré par Ann Cavoukian, Ph. D. et commissaire à l'information et à la protection de la vie privée de l'Ontario, pour contrecarrer les effets toujours croissants et systémiques des technologies de l'information et des communications et des systèmes de données ré-

Les bases de données ne sont pas seulement des listes, ni l'équivalent numérique de dossiers sur support papier. Les bases de données structurées donnent la possibilité de « demander » des données selon de nouveaux paramètres, permettant à des appareils d'extraire des échantillons de renseignements et de produire de nouveaux renseignements à partir de cela. Par conséquent, l'état-base de données est un appareil bureaucratique qui est en fait dirigé par des appareils. En tant que tel, cela promet de déshumaniser à la fois la fonction publique de première ligne et les gens qui en dépendent le plus.

Becky Hogge, dans le magazine *New Statesman*, 30 avril 2009

seautés à grande échelle. Ce concept soutient que l'avenir de la protection de la vie privée ne peut être assuré uniquement par le respect des cadres de réglementation. La certitude de protéger la vie privée doit plutôt, idéalement, devenir le mode de fonctionnement par défaut d'un organisme. Les trois premières règles fondamentales de « Privacy by Design » sont toutes axées sur l'assurance que les questions relatives à la protection de la vie privée soient réglées avant la mise en œuvre et non pas après que les problèmes aient surgi. Reprenons les propos de Mme Cavoukian dans son article sur le sujet :



1. Privacy by Design n'attend pas que les risques visant la vie privée se matérialisent et n'offre pas non plus de recours pour remédier aux infractions à la vie privée lorsqu'elles ont eu lieu – il vise à empêcher qu'ils se produisent. Bref, Privacy by Design agit avant les faits, et non après.
2. La protection de la vie privée est le paramètre par défaut. Aucune mesure ne devrait être nécessaire de la part de l'individu pour protéger sa vie privée – cela est intégré au système, par défaut.
3. Privacy by Design devrait être intégré à la conception et à l'architecture des systèmes de TI et des pratiques entrepreneuriales. On ne l'ajoute pas après les faits comme mesure d'appoint. La conséquence est que la protection de la vie privée devient un composant essentiel de la fonctionnalité centrale qui est livrée. La protection de la vie privée est une partie intégrante du système, sans en diminuer la fonctionnalité.

Les citoyens confient le pouvoir et des ressources à leurs gouvernements, au moyen d'élections et de versement d'impôts. Ceux à qui ce pouvoir est confié assument non seulement la responsabilité d'être au service des citoyens, mais aussi de les informer et d'encourager le public à participer à leurs décisions et à leurs mesures. Après tout, ce sont les citoyens qui devraient être la source du pouvoir en dernier ressort, puisqu'ils supportent les conséquences de son abus.

Transparency International

À mon avis, il est au moins impératif qu'une évaluation intégrale de l'impact sur la vie privée soit effectuée sur ce projet avant que de quelconques mesures pour le faire aller de l'avant ne soient prises. Qui plus est, lorsque le projet se matérialisera, il devrait incorporer Privacy by Design dès le stade de la mise en œuvre.





### 3. Municipalités

Ce ne sera pas la première fois que j'aurai recommandé que les municipalités devraient être tenues de respecter la législation sur l'accès à l'information et la protection de la vie privée. Il est non seulement important que les administrations municipales répondent de leurs actes au public au moyen de règlements sur l'accès à l'information, mais aussi qu'elles aient des règlements sur leur méthode de collecte de renseignements personnels sur des individus, ainsi que sur leur utilisation et leur divulgation.

Le mouvement du « droit de savoir » se trouve dans une position similaire. Durant la dernière décennie, la notion de la transparence a captivé l'attention publique et de grands progrès ont eu lieu pour ce qui est de persuader les gouvernements de reconnaître que le droit à l'information est une question de principe. Comparativement au stade où nous en étions il n'y a que quelques années, la perspective est spectaculaire. Néanmoins, nous n'en sommes qu'au tout début. L'actualisation complète de la notion du « droit de savoir » exigera plusieurs autres années d'appui soutenu.

Professeur Alasdair Roberts, Maxwell School of Citizenship and Public Affairs,  
Syracuse University

Dans mon dernier rapport annuel, j'ai remarqué que les Territoires du Nord-Ouest étaient l'une des cinq seules autorités législatives du Canada à ne pas inclure les municipalités dans leur législation sur l'accès à l'information et la protection de la vie privée. Ce nombre a désormais baissé à quatre et je pense que l'un des derniers bastions, le Yukon, envisage désormais d'inclure les municipalités dans sa Loi. C'est là une question d'impératifs démocratiques fondamentaux. L'ouverture et la responsabilité sont tout aussi nécessaires au niveau municipal qu'elles le sont aux niveaux territorial ou fédéral. Il semble que ce qui est préoccupant, au sujet de l'inclusion des municipalités, est le coût prévu qu'entraînerait cette inclusion pour les municipalités. Mon collègue de l'Alberta, le commissaire Frank Work, a émis un avis avec lequel je suis d'accord indiquant que le droit d'accès à l'information est précieux et qu'aucun gouvernement ne devrait jamais s'y opposer ou l'entraver, sous le prétexte que cela re-



vient trop cher, que cela exige trop de temps ou que seuls les « fauteurs de troubles » s'en prévalent. Ce droit est fondamental. Le droit de s'assurer que nos renseignements personnels qui sont colligés par les gouvernements demeureront confidentiels est tout aussi important. Il est temps de prendre les mesures pour les démarches nécessaires à l'inclusion des municipalités à la Loi. Le gouvernement pourrait peut-être étudier de plus près la suggestion que le gouvernement des Territoires du Nord-Ouest assume ou partage les coûts d'un poste dont le titulaire travaillerait avec toutes les municipalités pour résoudre les problèmes relevant de la Loi, de manière à apaiser les inquiétudes des municipalités par rapport aux coûts.

Cette nouvelle approche débute par l'échelon supérieur, avec cet engagement de ma part : Dorénavant, notre infrastructure numérique – les réseaux informatiques et les ordinateurs dont nous dépendons chaque jour – sera traitée comme elle devrait l'être : une ressource stratégique nationale. La protection de cette infrastructure sera une priorité de la sécurité nationale.

Nous veillerons à ce que ces réseaux soient sûrs, fiables et résilients. Nous allons décourager les attaques, les prévenir, les détecter et nous défendre contre elles; et nous nous rétablirons rapidement des perturbations ou des dommages.

Président Barack Obama

#### **4. Gestion des documents électroniques**

Je réitérerais aussi ma recommandation selon laquelle il faut accorder plus d'attention à la gestion des documents électroniques. De nos jours, pratiquement tout ce que nous faisons l'est de manière électronique. Cela s'accompagne des défis importants de trouver des moyens de cataloguer, d'organiser et de conserver cette information, tout en maintenant une capacité raisonnable d'y accéder. Il deviendra même plus important encore de déterminer et de gérer le cycle de vie de la gestion des documents. Dans les demandes de révision qu'on m'adresse, je constate les résultats de ce défi. Les communi-



cations par courriel constituent un défi particulier. Pour garder les documents accessibles et disponibles en cas de demande d'accès à l'information, il devient de plus en plus important que tous ceux qui utilisent le courriel pour exécuter les tâches des organismes publics (ce qui, bien entendu, comprend chaque personne employée par un organisme public) consigne et sauvegarde ces communications conformément à des pratiques de gestion de documents exemplaires de sorte que, lorsqu'il faut trouver un document, il soit classé d'une façon qui permette de l'identifier facilement comme étant éclairant et de le retrouver sans difficulté. L'alternative entraînera une incapacité totale à contrôler et à justifier les documents créés et cela créera, inévitablement, des organismes publics qui manquent de crédibilité et sont tout à fait incapables de rendre des comptes au public sur leurs actions.

Et alors? Si vous n'avez rien à cacher, pourquoi devriez-vous préoccuper de quoi que ce soit? Comme le souligne Daniel Solove dans « I've Got Nothing to Hide, and Other Misunderstandings of Privacy », la protection de la vie privée ne constitue pas le droit de cacher ce que vous voulez dissimuler à autrui, mais plutôt un droit qui comprend bon nombre de facettes et qui protège les intérêts de la société. Même s'ils étaient tout à fait licites, des pouvoirs de surveillance incontrôlés réduiraient la liberté de parole et d'association.

Chen Shen, *The Peak* (Simon Fraser University), le lundi 6 juillet 2009

## 5. Protéger nos enfants

Les jeunes d'aujourd'hui grandissent à une époque où les ordinateurs jouent un rôle central dans leur vie. La plupart sont bien plus à l'aise avec un ordinateur et en savent plus sur la façon de les utiliser avec un degré d'aisance auquel leurs parents ne parviendront jamais. Aujourd'hui au Canada, l'ordinateur comprend presque par définition l'accès à Internet. On estime que plus de 80 % des foyers canadiens sont branchés à Internet d'une manière ou d'une autre. Cela est la réalité de nos enfants... ils utilisent Internet pour communiquer entre eux, pour échanger avec leurs amis, pour explorer leur univers et



celui des autres, pour guider leur vie. Même si Internet donne à nos enfants des moyens de communiquer avec leurs pairs que nous n'aurions jamais pu imaginer une génération auparavant, une toute nouvelle gamme de risques accompagne ce nouveau média. Et bien que bon nombre des enfants connaissant bien Internet soient en mesure de bien reconnaître les risques associés à leurs activités en ligne, ils ne possèdent pas, le plus souvent, les connaissances nécessaires ou la volonté d'éviter ou d'atténuer ces risques. Il faut en faire plus pour éduquer nos jeunes et leur faire acquérir les connaissances dont ils ont besoin pour se protéger quand ils travaillent dans l'univers branché, non seulement des risques évidents des pédophiles et du vol d'identité, mais aussi des risques moins évidents et peut-être plus insidieux que cache cet univers. Je recommanderais qu'on envisage d'inclure dans les programmes scolaires des renseignements précis sur les médias électroniques et des stratégies pour protéger les enfants des risques du monde branché, en commençant au niveau de l'école élémentaire.

D'un autre côté, la *Loi sur la liberté d'accès à l'information* est un rappel saisissant que l'un des éléments définitoires de la démocratie moderne est que ceux qui sont portés au pouvoir et leurs fonctionnaires sont responsables devant la population. Le public a le droit de savoir ce qu'on fait en son nom et avec ses deniers.

L'accès à l'information entraîne une augmentation de la compréhension du public et une diminution de la portée des actes répréhensibles par rapport aux décisions ou aux activités à huis clos qui mettent en péril la confiance du public.

Richard Thomas, commissaire à l'information et à la protection de la vie privée du R.-U., rapport annuel 2009

## **6. Rôle de la commissaire à l'information et à la protection de la vie privée**

La charge de travail du Commissariat à l'information et à la protection de la vie privée devient plus importante, car le public connaît mieux la Loi et les droits qui s'y rattachent. Chaque année, l'investissement en temps qu'exige ce travail devient plus important. Le nombre de demandes de révision, particulièrement en matière de vie privée, augmente



d'année en année, et les problèmes deviennent de plus en plus complexes, exigeant parfois des recherches considérables.

À l'heure actuelle, le rôle de la commissaire est une fonction à temps partiel, exécutée « au besoin ». Toutefois, ce que cela veut dire, essentiellement, est que le Commissariat assume un rôle plutôt réactif que proactif, et j'ai la conviction que le commissariat doit être capable de résoudre des problèmes qui ne relèvent pas du processus de demandes de révision et d'activités auxquels il devrait et doit participer, pour renforcer les idéaux et les objectifs de la législation. Par exemple, je pense qu'il serait approprié que le Commissariat soit en mesure d'apporter une contribution plus importante à la « Semaine du droit du savoir » qui est célébrée chaque année au début de l'automne dans tout le pays. J'estime aussi, souvent, ne pas disposer du temps nécessaire pour me garder au fait des enjeux, particulièrement pour ce qui est du volet de la protection de la vie privée. En raison du rythme de l'évolution technologique, les enjeux de la protection de la vie privée exigent un investissement de temps considérable, mais on ne dispose pas du temps nécessaire quand le poste est à « temps partiel ». Il devient par conséquent de plus en plus difficile de maintenir un niveau de connaissances approprié sur certains de ces enjeux. De plus, si la législation relative à la protection des renseignements personnels sur la santé est adoptée dans les prochaines années, et si cette législation prévoit des fonctions de surveillance pour la commissaire à l'information et à la protection de la vie privée, la charge de travail du Commissariat augmentera probablement de beaucoup. L'un des autres mandats de la commissaire consiste à offrir des activités d'éducation publique. Cet aspect du travail n'est pas bien respecté, à cause du manque de temps pour élaborer et offrir des programmes efficaces.

Tout cela pour dire qu'il est peut-être temps d'envisager une approche différente par rapport au Commissariat, peut-être en donnant au poste un statut mi-temps ou temps plein, afin d'assurer que la commissaire dispose du temps voulu pour réaliser ces autres as-



pects du travail qui sont, sinon, difficiles à accomplir. Il ne s'agit pas là d'une question « législative », puisque la Loi exige seulement la présence d'un commissaire à l'information et à la protection de la vie privée. Cependant, il s'agit d'une question qui doit être revue en évaluant si le mandat peut, oui ou non, être accompli efficacement selon l'approche actuelle. Autrement, nous en sommes peut-être au point où le Commissariat devrait être doté d'un enquêteur (à contrat ou d'une autre manière) pour accomplir certaines des fonctions du Commissariat, pour prêter assistance lors d'enquêtes, pour les problèmes techniques ou pour une campagne d'éducation publique. La réalité montre que l'investissement de temps nécessaire pour faire du bon travail augmente et que, éventuellement, il peut être indispensable d'augmenter les ressources allouées au Commissariat. Je recommanderais que, en plus de la révision de la Loi, on procède à une révision des besoins du Commissariat, en vue de déterminer s'il faudrait adopter une nouvelle approche.

Le progrès de la démocratie exige la disponibilité d'une information véridique et complète, qui permette aux citoyens de juger en connaissance de cause les politiques gouvernementales; autrement, c'est le règne de l'autocratie obscurantiste.

Pierre E. Trudeau