RESPECTING PRIVACY IN E-GOVERNMENT

Jennifer Stoddart
President of the COMMISSION D'ACCÈS À L'INFORMATION
Bureau de Montréal
480, boul. St-Laurent, bureau 501
Montréal, Québec H2Y 3Y7 Canada
cai.communications@cai.gouv.qc.ca

Abstract: The topic of this paper addresses current privacy developments. The focus is on legal and other non-technical aspects, both from a Canadian and from an international perspective. Differences in approach between the European countries and the North-American part of the world will be highlighted.

Keywords: privacy, e-government, Quebec, Commission d'accès à l'information, Privacy Enhancing Technology

1. INTRODUCTION

The advent of electronic government, here as in the rest of the world, can bring citizens real advantages. In principle, e-government should lead to a greater participation of citizens in public life and the management of their society, not to mention the speed and accuracy with which government services could be delivered. It should allow a fairer and better-targeted distribution of services, supported by information that changes as fast as it is collected from users. Furthermore, the reduction of bureaucratic intervention in the citizens' transactions with government should minimize the curse of every public administration: the arbitrary exercise of discretionary power and discrimination.

Those are good reasons encouraging public administrations throughout the Western world to propose more and more comprehensive projects for government on-line.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35696-9_19
E. Nardelli et al. (eds.), *Certification and Security in E-Services*

But, as we know, such projects can involve real risks for privacy, and even lead to irreversible losses in the level of privacy protection we are accustomed to.

This is why organizations like the one I preside have a particular mandate to oversee and control, through notices, budding government on-line projects.

In my following remarks, I will first describe my organization's duties and then list a series of the criteria we use in assessing projects. I will conclude by citing a few examples of recent projects we were called upon to evaluate to illustrate concretely the application of the privacy concerns of the Commission d'accès à l'information.

2. ACCESS TO INFORMATION AND DEMOCRACY

As we all have heard: knowledge is power. Since the introduction of the new information technologies, knowledge is accessible to every citizen. Access to a broader source of information is a guarantee of democracy for all peoples. In the last 30 years of the 20th century, we saw a trend toward sharing the information hitherto in the possession of democracies, but unavailable to the public.

Thus, in the United States, a long tradition of democratization combined with an historic lack of trust in state authorities led to the adoption of the *Freedom of Information Act* in 1974[1]. At the same time, concern for access to information held by the state, notably within the European Union, Canada and especially Québec, only increased. Québec is a province of the Canadian federation that has a distinct culture. Québec also has a distinct legislation on access to information within its own jurisdiction.

In the early 80s, an inquiry commission on citizens' access to government information and the protection of personal information stressed the following point:

"Without access to facts, without information, freedom of opinion is devoid of substance. Knowledge conditions the exercise of the right of expression... The power of modern communication techniques and the State's broad use of these techniques easily lead to propaganda that is impossible for citizens, associations and even the best organized and wealthiest press organizations to counter."[2]

[1] Freedom of information Act and amendments of 1974 (P.L.93-501) (United States)

[2] Information et liberté, Rapport de la Commission d'étude sur l'accès du citoyen à l'information gouvernementale et sur la protection des renseignements personnels, Édition réalisée à la Direction générale des publications gouvernementales, Ministère des Communications, Government of Québec 1981, p.5

3. MANDATES AND DUTIES OF THE COMMISSION D'ACCÈS À L'INFORMATION.

The Commission d'accès à l'information is responsible for the enforcement of two Acts: the *Act respecting Access to documents held by public bodies and the Protection of personal information* and the *Act respecting the protection of personal information in the private sector.*

3.1 Public sector

In the public sector, departments, government organizations, municipalities, teaching institutions, and establishments of the health and social services network are subject to the Act respecting access, which includes two parts. The first part guarantees everyone the right of access to documents held by public bodies. The second part is intended to provide maximum protection to personal information held by the public administration. This second part of the Act also recognizes every citizen's right of access to and correction of his or her personal information.

3.2 Private sector

In the private sector, every goods and services company must comply with the *Act respecting the protection of personal information* wherever it collects, stores, uses or discloses personal data. To ensure control over his or her own information, any individual has a right to examine his or her file, notably through the right of access and the right of correction, and the right to have his or her own information removed from a list of names held or used by a company for the purpose of commercial or philanthropic canvassing.

3.3 Adjudicating function

As an administrative tribunal, the Commission reviews public administration decisions denying a person's application either for access to an administrative document or access to or the correction of his or her personal file. The Commission is also called upon to settle disagreements arising from the exercise of rights recognized by the Act respecting the private sector.

The Commission first attempts to settle these disputes through mediation. If it fails, the Commission allows the parties to submit their remarks orally or in writing, and makes a decision. This decision is final on points of facts;

points of law or jurisdiction may be appealed to the Court of Québec, with leave of a judge from that court.

3.4 Supervision and control function

The Commission also has a mandate to see that public and private organizations comply with their legal obligations in the collection, storage, use and disclosure of personal information. To this end, it may be called upon to authorize researchers to receive personal information, give opinions on agreements to exchange personal information, conduct investigations on its own initiative or upon a complaint, audit organizations for compliance with the Acts, and issue notices on bills or draft regulations that may impact established standards.

3.5 Advisory function

The Commission has finally set itself an objective to help implement concrete measures to ensure compliance with the spirit and letter of the law. This is where the Commission steps in to advise public and private organizations. This strategic function of the Commission is carried out in different ways: policy guidelines and evaluation of pilot projects especially on highly important issues like the new information technologies, genetics, biometrics, etc. As part of this function, the Commission attends conferences and seminars.

4. MEANS TO GUARANTEE THE RESPECT OF PRIVACY

At the time of writing, Japan's government faced fierce opposition from its people and many local authorities[3]. The source of this conflict is the introduction of a national identification system called Juki Net, which enables local authorities to identify every Japanese citizen on-line. To achieve this, a unique 11-digit number is attributed to each person.

While opponents of this system are worried about its potential hacking, their main concern is the threat it poses to their privacy; Juki Net is seen by many as a people monitoring system[4]. Many local authorities refuse to link

[3] Un nouveau numéro d'identité accueilli par des manifestations et des boycottages, by Miwa Suzuki of Agence France-Presse, La Presse, August 6, 2002.

[4] Japon : levée de boucliers contre le fichage numérique de la population, by Christophe Guillemin, ZDN and France, August 6, 2002.

up with the system while others, like Yokohama, Japan's second largest city[5], decide to register only those who wish to be entered in the system.

The mayor of Kokubunji even held a disconnection session at city hall and the mayor of another town North of Tokyo said "Juki Net was highly dangerous because a bill on the protection of personal information was still pending in Parliament."

Indeed, in 1999, when the Japanese government floated the idea of this system, they promised an Act protecting personal information would be passed beforehand[6].

Legislation is the primary tool for the protection of privacy, well ahead of any technological security tool. But this tool can only be effective if rooted in a society's culture and values. The Japanese example provides strong evidence. In spite of government guarantees that the system was fully secure[7], opposition is severe. Many Japanese citizens are calling for a law to protect personal data, not because they want information used by the State to be more secure, but to protect their privacy.

The passion characterizing the actions of opponents to the system shows the fondness of at least part of the population for this basic value of privacy. Time will tell if all of Japan's society rally to it.

In fact, many states have adopted legislation to protect their citizens' privacy or personal data over the past few years. While laws differ from one country to the next, the rules they propose are similar, dealing particularly with the collection, storage, purpose, use, and disclosure of personal information, and access to it by the person concerned.

The Commission's experience in the field teaches us that many data processors, at least in Québec, confuse confidentiality with the protection of privacy. Confidentiality is a security objective just like availability and integrity.

While confidentiality contributes to the protection of privacy, it does not per se guarantee it. This guarantee comes from the enforcement of all the rules set by law. The following example should help you see what I mean.

4.1 Québec health system

The Commission recently examined a system in the health area for the transmission of clinical data between a number of establishments offering short-term care to ambulatory patients. Thus, a patient receiving care from

[5] Yokohama, with a population of 3.27 million, is Japan's second most populated city (www.city.yokohama.jp).

[6] Japan national ID system raises privacy concerns, Kuriko Miyake, IDGNews Service, Itworld.com, 8-6-02.

[7] Juki Nnet goes online, Editorial, The Asahi Shimbun, Aug.6

several establishments is assured that an electronic file containing the information necessary for his or her treatments is made available to the caregivers he or she has to see in each establishment. The promoters of the project designed an architecture based on software making it possible to replicate data. Many security devices were put into place. At first glance, the law seemed to be respected. However, a further examination of the system's operation showed it replicated the data of all patients in all user establishments. Thus, a patient's record was found in the databases of establishments that provided care, but also in the databases of establishments he or she would not be visiting.

The Commission, in this case, determined that establishments not providing care to a patient could not keep his or her record. This shows that a secure system in which confidentiality is assured can contravene the rules for the protection personal information.

Yet, any system brought into service and any technology used need to comply with applicable laws. Once again, on-field experience shows that in many cases, the persons in charge of major developments have a hard time adapting personal information protection rules to their systems' operations. Very often this consideration is not examined in enough detail in the preliminary stages of development or when a technology or a system is purchased, the emphasis being laid more on costs and timetables as it were.

This has disastrous consequences. Imagine the embarrassing situation those responsible for a system that did not comply with the law would find themselves in once important contracts were signed or costly software purchased. To avoid such situations, the impacts of the introduction of a technology or a system on the privacy of citizens or potential users need to be thoroughly analyzed in this type of project.

The decision to go ahead with the project should only be made after such an analysis is performed. The project's ability to respect privacy or protect personal information as required by law should be examined, as well as the following areas. These should be seen as criteria likely to increase considerably the level of privacy protection:

- Criterion 1: Favour user anonymity.
- Criterion 2: Where anonymity is impossible, favour the use of pseudonyms.
- Criterion 3: Avoid the collection of additional personal data solely for security purposes.
- Criterion 4: Respect administrative boundaries between the various organizations.
- Criterion 5: Avoid centralization and the concentration of processing and data.

- Criterion 6: Avoid the spreading, duplication, replication and sharing of personal information.
- Criterion 7: Favour technologies that do not trace the actions of users and build profiles.
- Criterion 8: Consider balanced security measures that can achieve the required security objectives while respecting privacy.

Unfortunately, methods to conduct this type of analysis do not abound. Could government play a role in this regard? Should it require the use of such tools and promote their development?

5. E-GOVERNMENT

Before answering these questions, let me point out some issues that will lend more weight to my following remarks.

First, the difficulty for citizens to understand is what becomes of their personal information in a virtual world.

Secondly, the near-impossibility for citizens to understand, show and prove the logic of an illegal disclosure or a leak of personal information in such an environment.

Finally, the growing possibility a citizen may never know he has been the victim of an illegal disclosure or a leak of information.

In spring 2002, the Commission d'accès was invited to appear before a parliamentary committee studying a draft bill on the Québec health card. The bill, prepared by the Régie de l'assurance maladie du Québec, would provide for the introduction of an on-line system to check a patient's insurance coverage, the constitution of a shareable health record and the use of a microchip card. Without going into the details, I submit to you in passing that this bill would not satisfy one of the criteria designed to increase the level of privacy protection I mentioned earlier. *Criterion 5* requires avoiding centralization and the concentration of processing and data and this draft bill does the exact opposite. Where the shoe pinches even more is that I noticed during the parliamentary committee hearings that many experts had difficulty understanding the working of the proposed system and, as a result, deciding the positive and negative effects of its use. If privileged observers have such difficulty, imagine what it would be for an ordinary citizen. How can a healthy exercise of democracy be furthered in a context where many are unable to understand the essence of the fundamental changes proposed to us?

A government can decide to legislate to protect its citizens' privacy or let them worry about it. I don't think the latter approach is sufficient when a society is confronted with major technological changes that may often

impact citizens' privacy while they are unable to understand their functioning and effects.

As we have seen, many governments have done their legislative homework and met their citizens' wishes and aspirations. Yet, many surveys show the population continues to worry about privacy protection where technologies like the Internet are involved.

Generally, government legislates to protect citizens who are not in a position to understand the functioning of the complex systems in which their personal data reside. Government must also insure that the citizen, who has rights, can exercise them in case of illegal disclosure, leaks of personal information or other situations where he is wronged. In addition, government should not hesitate to submit the projects it promotes to a true public debate.

In the delivery of electronic services, government must itself be exemplary in protecting privacy. Government departments and organizations must be required to respect scrupulously the letter and spirit of the law.

The Commission d'accès recently issued an opinion on the government's Public Key Infrastructure (PKI) project. It should be pointed out this is an interim project; a permanent solution is being developed. This project needs to be corrected and improved to comply with the law. But even when this is done, irritants could remain concerning the respect of privacy. Let me cite as an example the requirement that a user state his or her identity to a non-government controller. This administrative choice alone, never mind other aspects of the project, is contrary to many of the criteria designed to increase the level of privacy protection. First, there is a contradiction with *criterion 1*; formal identification, by its very nature, is the antithesis of anonymity. Then, the collection of additional personal data by a third party for the purpose of security negates *criterion 3*. Finally, spreading personal identification data and repeating them in many places contravenes *criterion 6*.

Thus, in this project, it may be possible for its authors to respect the letter of the law, but hardly its spirit, which would require restricting to a minimum the collection and circulation of personal data.

A government should always choose those hardware and software technologies that are the least invasive of its citizens' and employees' privacy. This is why we should thoroughly analyze the impact of every government project on privacy and the protection of the personal data of citizens and those who will have to work with the proposed system and technology. As I said earlier, methods to analyze such matters are rather scarce.

A government surely could develop or help develop such methods. They should be based on proven international models, like the Common Criteria, while being flexible enough to take into account the differences between states in privacy and personal information protection legislation.

The type of analysis proposed here is highly important. States now acquire at great expense software whose sources they don't own. Very often the precise functioning of this software is known only to the product proprietaries. These programs process and handle a considerable amount of personal data. An expert from the Centre de bioéthique de l'Institut de recherches cliniques de Montréal recently wrote in *Le Devoir*[8]: "Indeed, the truth of the law (and the supremacy of the law) rests particularly on the principle that *nobody is supposed to ignore the law.* Government, which enacts a law's enforcement regulation, is supposed to know the law...But what about the computer system? What about computers, microchip cards or other devices that make them up? They are only machines. They ignore the law. Their truth resides in the programs they perform, mechanically, with an utter indifference for the law or their repercussions on citizens. An automatic teller or a microchip card, therefore, has their own truth, which may very well contradict that of the text of the law which allows them to exist."

A thorough analysis of the impacts of a new technology or system on privacy would enable governments to really know whether the technologies and systems they acquire or develop respect the letter and spirit of the laws for privacy protection.

Governments, I understand, want to provide a measure of security to transactions carried out in the virtual word. To do this, they must develop policies, and then choose security means and devices. While very often allied, privacy and security are sometimes at odds.

Some security devices require an additional collection of personal data, conduct automatic surveillance, trace transactions and generate files on user behaviour. Some reservation is called for in this respect. Governments must choose security means and devices that comply with the laws and reduce as much as possible the collection and generation of personal data. There is a category of products on the market under the general name of *Privacy Enhancing Technology*. Whether for security purposes or to satisfy other needs, governments would be well advised to promote the development of such products and acquire them.

6. PRIVACY ENHANCING TECHNOLOGIY

At present, some Privacy Enhancing Technology products are offered on the market as software allowing to surf the Net anonymously and making the management of personal data easier. While some of these products are known to be reliable and effective, others are criticized by privacy

[8] La démocratie aux prises avec le government électronique, Pierrôt Péladeau, Le Devoir, August 6, 2002.

advocates. Once again a thorough, independent analysis of these technological solutions would enable us to see things more clearly, and this, before any acquisition.

7. CONCLUSION

The protection of privacy and personal data cannot rely merely on the use of technologies ensuring security in a virtual world. This protection rather goes through the establishment of a legislative framework rooted in the society's culture and values.

The technologies used for the delivery of government services must respect these basic values. Given the wealth and complexity of software and hardware technologies on the market, it is surely not easy for a government or a state to see things clearly. This is why the development and use of methods to analyze their impact on privacy and the protection of personal data seem to me to be more necessary than ever, and this, before the introduction of any technology and system. The development and use of *Privacy Enhancing Technology* also seem to be a direction any government concerned with privacy protection should look at.

As for the organization under my responsibility, it will continue to be proactive and issue the necessary warnings when new technologies likely to have an impact on privacy are used or about to be used.

That's what we did a few months ago when we studied the issues raised by the use of biometrics and adopted a series of application principles, which organizations or companies planning to use these new technologies should take into account. These documents are available on the Commission's Web site (**www.cai.gouv.qc.ca**).