CHAPTER 5

THE KEY CONDITIONS FOR SUCCESS

Far from being a technological project, e-government focuses first and foremost on meeting the needs of Québec citizens: Technology is not an end in itself but rather a means of improving services. Everything must be done to help citizens develop the reflex of using on-line services and taking advantage of the new possibilities for expressing their democratic rights. If the government does not take concrete actions in this direction, e-government risks becoming an expensive and underused instrument. However, there are many factors that can influence citizens' support for this project (see Figure 9, page 111).

First, the strength of **political will and the governance structure** stemming from this will are key to the success of the e-government project. To highlight the importance of these key factors, they have been given a separate chapter in this report. In addition to accountability mechanisms, the proposed governance principles must therefore be considered as an integral part of the conditions necessary for success.

Second, the support of citizens rests primarily on the presence of a **climate of trust** associated with the delivery of e-services. This is a prerequisite if citizens and businesses are to use the e-services offered. The government must not only establish this climate of trust, but also implement the necessary means for maintaining it.

Clearly, given their multiplicity, it is difficult to determine exactly which factors influence the trust that citizens and businesses place in the use of on-line services and projects related to e-democracy. Nevertheless, the climate of trust that is key to developing the delivery of e-services successfully rests on the presence of the following two components:

1. Appropriate privacy protection mechanisms for the various types of e-services;
2. Secure mechanisms (assurance that a third party cannot interfere in the process).

These two factors must be supported by an institutional arrangement that ensures that information in computer systems is used and accessed only for justified reasons. Trust, therefore, will also depend on legal foundations that ensure, among others, the protection of personal information and privacy (see Figure 10, page 112). Accordingly, legislation must take into account the new realities of the virtual world and a networked State to enable the government to give citizens and businesses better services that incorporate the possibilities now available through ICTs.

The 2003 Québec study conducted by the *Centre francophone en informatisation des organisations* on the use of Internet services provides insight into a public concerned about an adequate level of security, the protection of personal information and the right to privacy. This constitutes a major obstacle to implementing the delivery of e-services. In fact, fears regarding privacy and security are the main reasons why citizens, businesses and self-employed workers do not use the government's Internet services (overall, these reasons were mentioned by 42% of citizens, 27% of businesses and 33% of self-employed workers).[31] The perception of citizens and businesses regarding the means made available to them by the government is therefore critical to the success of e-government. To dispel the fears associated with the use of these services, it is important that the new computer systems used to deliver e-services meet citizens' expectations precisely and concretely in terms of security, protection of personal information and the right to privacy.

---

[31] CEFRIO, NetGouv 2003, *Survey of Québec citizens, businesses and self-employed workers*, 2003, p. 10.

THE KEY CONDITIONS FOR SUCCESS (cont'd)

Third, the e-government project focuses on **simple access to government services**. With this in mind, it is important, as mentioned previously, that this e-government project not be reserved solely for citizens who have Internet access. It is therefore necessary to develop, parallel with the government's one-stop service portal, multiservice centres that provide access to all services offered by the government by telephone, mail or at service counters. The goal of the multiservice centres is to smooth the way for citizens in their dealings with the government, while taking into account citizens who do not have access to the Internet. However, this does not mean that the government is giving up on the goal of having all citizens gradually switch to e-services.

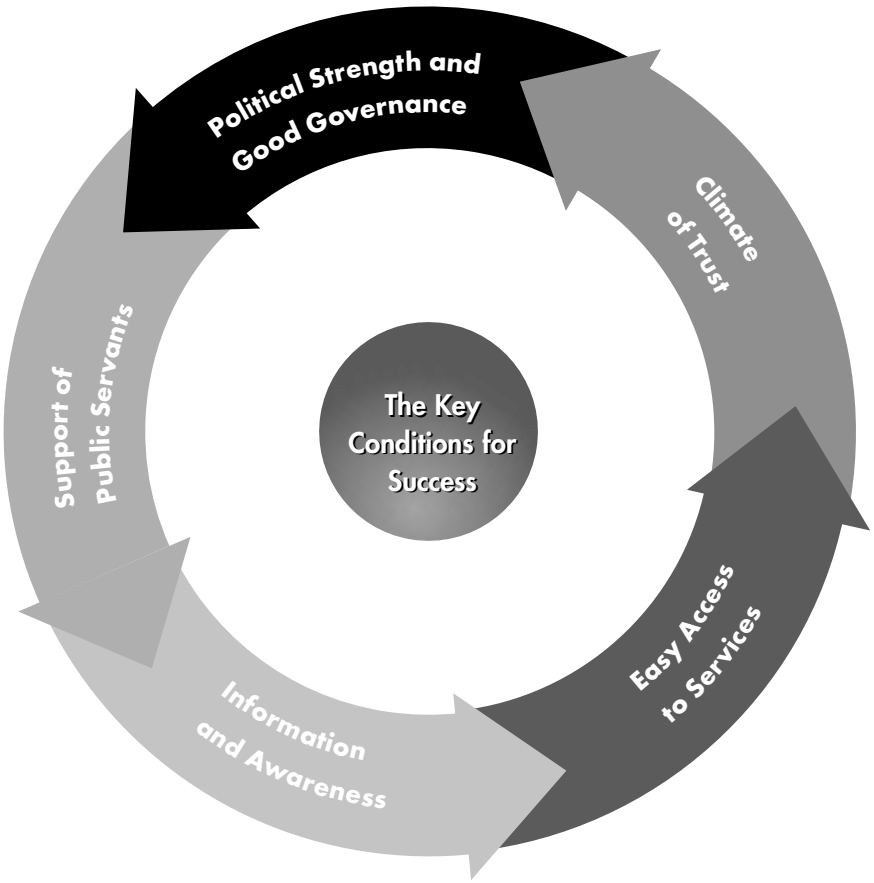
This is why the government must facilitate access to the Internet. Although recent surveys show that Québec leads the OECD rankings with respect to Internet access, it remains nonetheless that 40% of Quebecers do not have access to the Internet,[32] be it for socioeconomic, demographic or geographic reasons. It is the government's responsibility to combat this digital divide by favouring the possibility of free Internet access in public libraries, for example, and by supporting citizens unfamiliar with the new technologies to help them acquire the necessary skills. To this end, the establishment of partnerships with community groups would be a preferred approach to facilitate the acquisition of skills by citizens. Some achievements worthy of note show this to be the way of the future. The generalization of broadband or high-speed Internet access is also a factor to be considered in the democratization of access to government services. Moreover, clientele with special needs, especially those with motor, cognitive or sensory disabilities, must also be taken into account in the overall government approach.

Taxpayers' money risks being invested needlessly if the reflex to use e-services for dealings with the State does not develop. Fourth, therefore, the government must provide adequate information so that **citizens and businesses are informed about and aware of the new possibilities offered by ICTs**. The government must show that using these new methods to deliver services translates into real gains in efficiency. The delivery of e-services will enable citizens and businesses to save time, energy and, in the long term, money, and will also enable decision-makers and managers of public programs to make better decisions, thanks to a supply of quality, "just-in-time" information. The tangible improvement of services must guide the government in its strategy to develop e-government. When establishing the implementation schedule, priority must be given to projects with gains in efficiency that can be easily measured. A vast advertising campaign must be set in motion as quickly as possible so that citizens accompany the government every step of the way toward establishing e-government. The main government partners must be directly involved in this advertising campaign, in particular, those, like CEFRIO, that specialize in the appropriation and transfer of information and communication technologies.

[32] According to the most recent CEFRIO results, 60% of Quebecers are "connected" (NetTendance 2003).

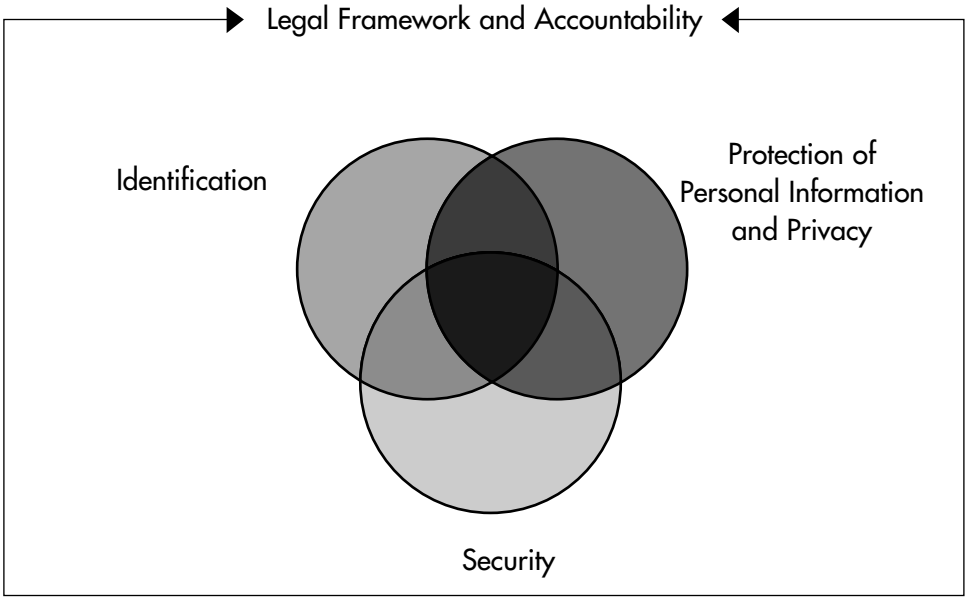
Lastly, other key factors in the success of e-government include **raising awareness among public servants and gaining their support** for the project. The implementation of e-government will have a major impact on the work of public servants and will, in many cases, bring added value to their jobs. It is crucial that government employees be directly involved in the project from the outset and view it not as an imposition, but rather as an opportunity.

Figure 9: Conditions for the Success of E-Government



1. Establishing a Climate of Trust

Figure 10: The Key Elements in Establishing a Climate of Trust



1.1 The Legal Foundations of a Climate of Trust for E-Government

In 2001, in response to the new realities of ICTs, the government adopted the *Act to establish a legal framework for information technology.*[33]

> "[this *Act*] specifies the rights regarding documents on paper and other media as those which depend on information technologies. It makes adjustments to several basic notions of Québec civil law in order to make it fully compatible with the secure use of information technologies.
>
> The *Act* has a general application: Any situation not covered by specific rules in specific laws are governed by the principles stipulated in the *Act to establish a legal framework for information technology*.

[33] R.S.Q, Chapter C-1.1.

The *Act* stipulates rules regarding the establishment of documents on various media, the transfer of information in a document to a different medium, the conditions for the integrity of the documents throughout their life, the relationship between a person and a document, and certification. It sets out specific protections for personal information and provides details on accountability conditions for service providers."[34]

The *Act* places Québec in a leading position in terms of a legal framework. Québec's legislation on information and communication technologies is a legal solution that satisfies many of the concerns of the Working Group on Electronic Commerce of the United Nations Commission on International Trade Law (UNCITRAL), which is currently preparing the "Preliminary Draft Convention on [International] Contracts Concluded or Evidenced by Data Messages." This group is particularly concerned about the creation of separate legal systems for paper documents and electronic documents, as well as the erosion of national rights. The Québec solution, which stems from the application of the principles of neutrality and functional equivalence proposed by UNCITRAL, also offers the freedom of choice and interchangeability of the supports and technologies sought after by the stakeholders involved in international trade, while maintaining the applicable legal system. This solution was presented by the Québec section of the Canadian delegation participating in the UNCITRAL task force on electronic commerce during its recent work in 2004 and was favourably received. As a result, the *Act to establish a legal framework for information technology* is now a precedent in this matter.

By identifying the various issues and possibilities related to new information and communication technologies, the *Act* is the first major step toward implementing true e-government.

However, the e-government project can only be successful if the entire legislative corpus is adapted at two levels:

- All of the laws must respect the legal framework set out by the framework *Act*, in particular with regard to technological neutrality;
- It is important to adopt the necessary legislative changes in order to facilitate the adoption of transactional-type measures.

a) Respect for the Concept of Technological Neutrality

The *Act to establish a legal framework for information technology* introduces the principle of technological neutrality, i.e., that the expression of a standard must not presuppose a specific medium (paper or electronic). However, many components in the current legislation do not meet this criterion of neutrality: Having been drafted before the use of ICTs became a reality, many laws include provisions that presuppose the use of a paper medium. For example:

---

[34] *Conseil du Trésor, Autoroute de l'information*, http://www.autoroute.gouv.qc.ca/loi_en_ligne/loi/index.html [on-line], site consulted March 31, 2004.

THE KEY CONDITIONS FOR SUCCESS (cont'd)

- Several provisions stipulate specific times for consulting documents (consultation of a log during "regular" office hours, for example). The possibility of consulting these documents on-line renders the stipulation of consultation hours obsolete;

- Other legislative provisions deal with physical presence during meetings (annual meeting or board meeting, for example). It is appropriate to question whether a physical presence is actually necessary, or if the use of ICTs could permit new forms of presence (videoconferencing, for example);

- The reference to appended or attached documents can infer a temporal component (this may be interpreted as requiring items to be sent concomitantly or simultaneously). The new possibilities related to sending documents in electronic format require a review of the concept of appended or attached documents. The legislation must enable a mixture of document formats sent as part of the same process; it should be possible to attach paper documents to electronic documents and send them at the same time.

According to the *Act*, people cannot be obliged to use a specific technological medium for sending or receiving documents unless specifically stipulated by law or in an agreement. In fact, Section 29 stipulates as follows:

Acquisition of a Support
A person may not be required to acquire a specific medium or technology to transmit or receive a document, unless such requirement is expressly provided by law or by an agreement.

Receiving Support
Similarly, no person may be required to receive a document in a medium other than paper or by means of technology that is not at the person's disposal.

Choice of Support
A product or service or information on a product or service that is available in more than one medium may be obtained in any such medium at the option of the recipient of the product or service.[35]

Pursuant to the principle of neutrality, the *Act* permits the use of technologies for the application of all laws. The principle of neutrality not only assures that future developments take citizens' choices into account, but also provides a guarantee of increased security, since in the event of a technological breakdown, the interchangeability will permit the use of paper documents and vice versa. Occasionally, there may be obstacles preventing the application of this principle, such as when a law requires the exclusive use of a specific support or technology. Accordingly, the entire legislative corpus must be reviewed to determine whether legislative provisions that are not technologically and legally neutral should remain, be deleted or be modified.

---

[35] *Act to establish a legal framework for information technology*, 2001, R.S.Q., chapter C-1.1, c. 32, Sect. 29.

The legislator must therefore draft enabling legislation for this *Act* that would ensure the implementation of the principles of technological media support and legal neutrality and be functionally equivalent in all Québec legislation. A team of lawyers at the *Ministère de la Justice* is already working on a draft bill, which should be tabled in spring 2005. The draft bill will set the technological and legal standards to be applied in all e-service projects.

Considering the impact of the *Act*'s enabling legislation, the government should advance the presentation of the legislation by allocating the necessary resources and ensuring that the *Act* takes into account the reality of the development of e-government.

b) Adoption of "Transactional Laws"

A transactional law is one that can be administered on-line through the delivery of e-services. The nature of transactional laws is one of the major components that will allow for the implementation of various features contributing to the creation of true e-government in Québec. The desire to make laws transactional requires finding solutions to specific problems.

The difficulties appeared following the desire to ensure that the *Cooperatives Act*, sponsored by the MDER and adopted in December 2003, can be managed transactionally. Although these difficulties may be specific to the *Cooperatives Act*, they can be generalized to all transactional laws that the government wishes to adopt.

Furthermore, as part of the work to implement a business portal, a task force led by the *Ministère de la Justice* identified nine problems to be resolved to enable business people to perform on-line transactions with the government (see insert below). These problems are similar to those raised in the process to adopt the *Cooperatives Act*. Following an analysis, the team of lawyers determined that, for all departments, close to 500 measures related to these issues would require legislative or regulatory amendments to permit transactions on-line.

Difficulties Related to Adopting Transactional Laws

Many components included in traditional legislation can be problematic in a virtual world:

- Various signature requirements;
- Payment method (when payment by credit card is not an option);
- Capacity (physical or legal person);
- Documents to be provided;
- Number of copies to send;
- Medium, layout and format of the application;
- Concordance of requirements;
- Requirement of a seal;
- Method of sending the application.

Accordingly, the entire legislative corpus must be reviewed based on the new realities specific to a virtual environment.

- ***Relaxing of Administrative Processes***

Updating laws and regulations to enable their application via information and communication technologies is designed to simplify the government's actions regarding the choice of methods to use at the administrative rather than the legislative level. However, the relaxation of the legislative corpus will not resolve every problem related to the application of laws. Moreover, if the processes used to administer a law are heavy and complex, they will not automatically be changed by the introduction of technologies. The introduction of information and communication technologies necessarily requires a review of the management processes, since those applicable to paper may be obsolete, in addition to being incompatible with the use of electronic methods. Although a review of the legislative corpus is necessary to enable it to incorporate the new technologies fully, this cannot occur without a review of the administrative processes and an integrated management of paper and information and communication technologies.

This work is all the more important since certain administrative formalities that are relatively easy to apply in the real world take on a far more complex dimension in the virtual world. For example, there is the multiplication of signatures required. It is essential to determine whether these signature requirements are necessary.

Further reflection is needed on the implications of the desire to make laws transactional. For example, a ruling must be made on how to **authenticate** electronic documents; this must be easily identifiable. Clear parameters must be established in this regard, for example, with respect to the validity of an electronic seal. Moreover, we must find a way to guarantee the **integrity** of technological documents in order to ensure their preservation.

RECOMMENDATIONS

5.1 We recommend that the entire legislative corpus be updated in order to ensure that respect for the principle of technological neutrality continues at an accelerated pace.

5.2 We recommend that provisions be made to table the enabling legislation for the *Act to establish a legal framework for information technology* in the near future.

5.3 We recommend that a team of lawyers review the regulations, instructions and management processes stemming from the application of laws and regulations to adapt them to the delivery of e-services.

1.2 The Basic Principles for the Protection of Personal Information and Privacy Under E-Government

The Charter of Human Rights and Freedoms states that "Every person has a right to respect for his private life" (Section 5). It is this premise that provides the foundation for the protection of personal information and the right to privacy in Québec.

Nonetheless, the challenge of the dazzling rise of new information and communication technologies since the 1970s and the repercussions of these technologies in terms of the protection of privacy is a pressing reality that the government must take seriously by constantly examining the impact of new technologies on the right to privacy. This said, it is imperative that the Québec government equip itself with clearly defined legal and institutional mechanisms that must then be consolidated to guarantee its citizens that personal information used when delivering e-services is protected against any infringement on their right to privacy. These mechanisms must also be defined so they can be adapted to rapidly changing technologies.

The government must promote an approach in which the technological systems and organizational rules used minimize the possibility of a breach of privacy. In other words, rather than trying to control possible violations of the right to privacy, the government must take the necessary steps to ensure such eventualities simply do not occur. Lastly, the government must also promote the deployment of awareness-raising and training programs that enable users to fully absorb the risks related to the protection of personal information in the use of technological systems.

Before formalizing the steps to be taken by departments and agencies in developing and deploying e-government projects, the principles for the protection of personal information should be clearly stated. It is important that citizens and public administrators alike understand and assimilate these principles.

First, a distinction must be made between the protection of personal information and the right to privacy, on the one hand, and the security of information and network systems that transmit this personal information, on the other. Computer systems that process personal information necessarily require security measures. However, security alone does not in itself guarantee adequate protection of personal information–a computer system can be very secure without actually protecting the right to privacy.

The OECD has established guidelines governing the protection of privacy and the cross-border flow of personal data.[36] These guidelines have been developed around the following eight principles:

1. **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, such data should be accurate, complete and kept up to date.
3. **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification Principle stated above if it is not a) with the consent of the data subject, or b) by authority of law.

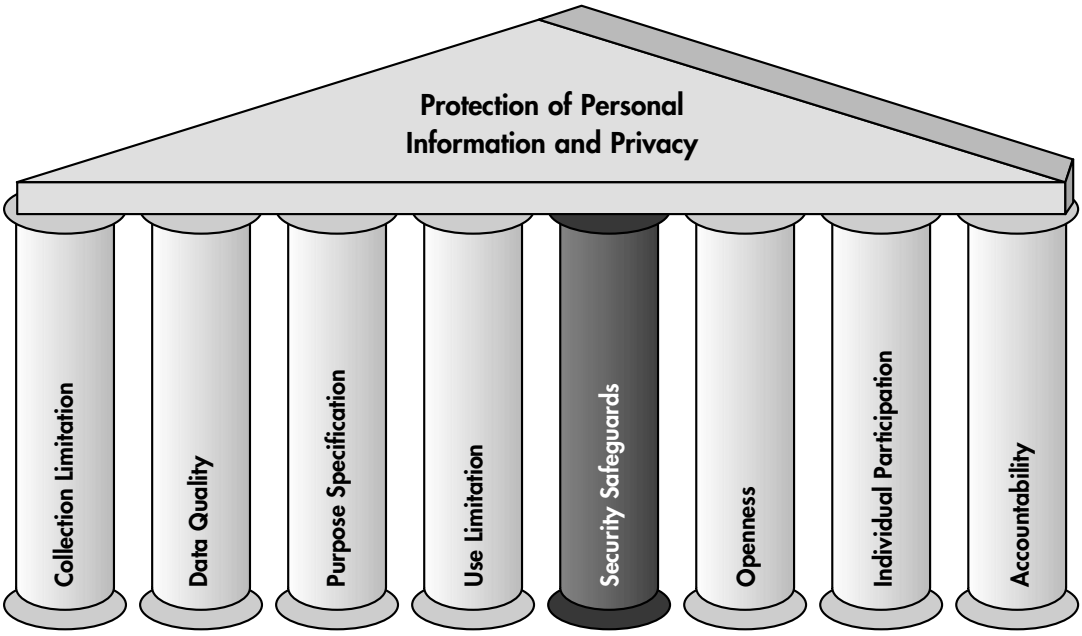
---

[36] *OECD, Privacy Online: OECD Guidance on Policy and Practice Guidelines, 2003, p. 11.*

THE KEY CONDITIONS FOR SUCCESS (cont'd)

5. **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure.
6. **Openness Principle:** There should be a general policy of openness about the developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle:** Any individual should have the right to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him or to have communicated to him; and to be given reasons if a request is denied and to be able to challenge such denial; and to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.
8. **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

Figure 11: Guidelines Governing the Protection of Privacy



This list of eight principles clearly shows that computer system security is only one factor among many that guarantee the protection of personal information. As stated by the *Commission d'accès à l'information* (CAI): "The concept of the protection of personal information and the right to privacy goes beyond the simple notion of secure exchanges."[37] The principle of security is necessary, but not sufficient.

The increasing number of attacks on computer systems and the growing spread of ever-more sophisticated viruses are confirmation of these concerns and of the popular belief that a secure system alone cannot guarantee the protection of personal information. Computer systems thus deployed are much more like electronic access systems in which it is easy to compile data (logs) on all user activities which can subsequently be tied to the real identity of the users. In this situation, privacy protection issues are, by default, largely pushed aside or marginalized.

In addition to respecting the principles of computer security, the government must also, in designing computer networks, ensure that other principles guaranteeing the protection of personal information and the right to privacy are respected at all times. The protection of personal information must be the rule and must allow for a clear definition of needs in terms of networks and computer infrastructure. Adopting this perspective makes it possible to strike a balance between security and the protection of privacy.

Lastly, the government must take the necessary measures to promote better accountability on the part of stakeholders in the e-government project, including citizens who use e-services. In fact, a computer system can only assure the protection of personal information and security if risk management is taken into account at all levels by making both service providers (public servants) and people receiving services accountable.

a) The Legal Situation in Québec Regarding the Protection of Personal Information Under E-Government

Before dealing with the potentially necessary changes to the protection of privacy under e-government, the principles of the protection of personal information as stated by Québec legislation must be clearly defined.

First, what constitutes personal information must be clarified. As stipulated in the *Act respecting access to documents held by public bodies and the protection of personal information* (hereinafter called the *Act respecting access*), personal information comprises any type of nominative information concerning a physical person that can be used to identify that person. For example, the name of a physical person is not in itself personal information, but can become so when associated with other nominative information about this individual, or if it can be used to identify other nominative information.

---

[37] *Commission d'accès à l'information*, 2002 five-year report. *Une réforme de l'accès à l'information: le choix de la transparence*, November 2002, p. 85.

Furthermore, the *Act respecting access* stipulates that all personal information collected (when this is necessary) and held by the D/As in compliance with the law must be treated as confidential. The personal information held by a D/A cannot be released without consent of the person concerned, except in specific cases defined by the *Act*. Two such exceptions are the communication of information between D/As (according to defined conditions)[38] and research authorizations. The CAI explains that "exchanging personal information without people's consent is to undermine one of the pillars of the protection of personal information, hence the implementation of exceptional and limiting mechanisms when an agency wishes to proceed in this manner."[39] Lastly, the Act stipulates the conditions the D/As must observe throughout the useful life of personal information (collection, conservation, communication and destruction).

b) Adaptation of Current Legislation to the New Context of E-Government

In the context of the implementation of e-government, it is appropriate to ask whether the current legal framework ensuring the protection of privacy must be reformulated to regulate more efficiently the circulation of information needed for the smooth and efficient delivery of government e-services. In fact, some specialists agree in saying that the future development of integrated on-line public services for citizens and businesses, as well as their smooth operation, rests essentially on the use and the increased exchange of personal information between the various stakeholders. According to these specialists, the information and its exchange is vital to enable the government to optimize the quality of services. It is therefore a question of customizing services for citizens and businesses.

• *The Exchange of Personal Information Within an Increasingly Integrated Electronic Administration*

The *Centre de recherche en droit public* at the *Université de Montréal* (CRDP) has looked into adapting the legislative framework necessary for the new realities specific to the emergence of information and communication technologies and the new possibilities of delivering e-services. The CRDP stated that the goal is to implement "an adequate legal framework that enables the controlled exchange of personal information between D/As for the purposes of enabling the delivery of e-services to citizens on the basis of information held by several D/As." The specialists of the centres also state that "the strengthening of privacy protection [is possible] through a better targeting of protection mechanisms." In short, it is necessary to "[…] protect privacy better

---

[38] The communication of personal information between D/As without the consent of the person in question can be done under the following conditions: Information is necessary for carrying out an act (Section 67); information is necessary for establishing conditions of employment (Section 67.1); information is necessary for the discharge of duties (Section 67.2); information is necessary for the implementation of a program (Section 68); information is necessary for the pairing or matching of files (Section 68.1). For the last two points, a written agreement must be obtained and an opinion from the CAI must be established. If this opinion is negative, the agreement can be submitted to the government for approval. These documents must be tabled before the National Assembly and published in the Official Gazette of Québec.

[39] CAI, 2002 five-year report. Une réforme de l'accès à l'information: le choix de la transparence, November 2002, p. 79.

without preventing the circulation of information needed for the delivery of e-services."[40] Faced with such a situation, the government must establish an innovative legal framework to enable the secure exchange of personal information between multiple D/As, while ensuring optimal protection of the information throughout its exchange, use and conservation.

The current regime of agreements duplicate or copy personal information exchanged under such agreements into the various databases of the D/As concerned. The duplication of this personal information increases the risks related to a breach of privacy, although these risks were present before the advent of agreements established with the CAI. Previously, the same personal information would have been collected by each individual D/A, resulting in an overall reduction in the efficiency of the public administration and the delivery of services in general. Currently, a citizen's change of address is exchanged daily between the D/As participating in the relevant agreement and is thereby copied into the various databases.

The current system could be improved through a variety of actions, such as reducing the number of locations where personal information is stored. D/As that need this information in the application of their programs could access it without actually keeping it. Agreements could provide for these possibilities. The D/As that acquire personal information would then be responsible for its use and for respecting the associated confidentiality criteria. There is no intention of creating a central database for storing all nominative information, but rather one for minimizing the duplication and excessive collection of information. Access rights governed by a regulatory framework or agreements among the relevant D/As will be provided.

As established by the CAI, the principle of compartmentalization limits the circulation and communication of personal information to a specific organization. The CAI also states that although not spelled out in the *Act respecting access*, this principle is inferred from the legislative text (Section 59). On this point, the CAI indicates that the principle of compartmentalization of personal information in the public administration is the best guarantee for the protection of privacy and for minimizing the possibility of creating a "Big Brother" state. Improvements to the current situation that minimize the duplication of personal information, while allowing for access to it within the framework of e-services, would not call into question the logic behind the principle of compartmentalization. In fact, the personal information would be stored only where it is to remain, i.e., a database under the responsibility of a D/A, and not duplicated or freely exchanged between various D/As. The personal information would only be released or made accessible to other D/As when permitted by law or under an agreement which would have to be made pubic. Access to this personal information would be strictly controlled within a well-defined framework.

In support of these legal and structural foundations, modern privacy-enhancing technologies, such as those presented later in this chapter, could facilitate the exchange of personal information while ensuring its protection. It appears that modern cryptology can offer tools that ensure the secure exchange of personal information in compliance with the rules governing the protection of personal information and privacy. This assertion is an observation based on years of research in cryptology.

---

[40] CRDP, *Les modifications à apporter aux cadres administratifs et juridiques afin de favoriser le développement de l'administration électronique dans le respect de la vie privée* (prepared for *le Secrétariat du Conseil du trésor*), *Université de Montréal* (Faculty of Law, December 2003, p. 1.

THE KEY CONDITIONS FOR SUCCESS (cont'd)

• *Various Degrees of Sensitivity of Personal Information*

Specialists point out the significant importance of designing a legal framework in which personal information can be assigned varying degrees of protection depending on its sensitivity. This sensitivity, which takes into account circumstances, can change at any time during the life of the person in question. Information can become more sensitive depending on the prevailing circumstances. To quote Pierre Trudel, "even if all information concerning a person has a similar status, it does not all involve the same risks and stakes."[41] On this point, the CSRI explains that:

> "For example, a person's address is often widely available in a telephone book. However, in certain circumstances, the publication of an address can present a risk to that person's safety, in which case adequate protection must be provided."[42]

Consequently, personal information can become extremely sensitive for certain individuals or groups of individuals, which results in the need for a change in the degree of protection of this information. On this point, the focus must be placed on the citizen's consent and choice whenever possible. In other cases, institutional mechanisms must be provided.

Current legislation does not distinguish between or judge the sensitivity of personal information, but it is clear that additional protection measures must be provided in certain circumstances. In addition, provisions concerning the protection of personal information in sectorial laws, such as the *Act respecting health services and social services* or the *Act respecting the ministère du Revenu,* establish rules concerning certain personal information that are much stricter than those in the *Act respecting access*. Nevertheless, it is important that the computer systems developed for delivering e-services incorporate features that provide variable levels of protection that can be changed according to the sensitivity and use of the information in question. To this end, the law should acknowledge this requirement.

• *Principle of Purpose of Specification*

Specialists agree in saying that the purpose of specifications must better correspond to the realities of e-government. According to the current design, it is agreed that personal information cannot be used for purposes other than those for which it was initially collected. However, to meet the new realities generated by e-government and specifically to avoid wasting time through the multiple collection of information, the D/As must be able to offer value-added services that were not covered in the D/As' enabling legislation. In such cases, the principle of purpose is not respected, since the personal information used was not collected for the purpose of providing a value-added service. The legal framework must define or permit this possibility.

---

[41] Trudel, Pierre, Améliorer la protection de la voie privée dans l'administration électronique: pistes afin d'ajuster le droit aux réalités de l'État en réseau, CRDP, Faculty of Law, *Université de Montréal*, p. 41.

[42] SCT, Brief by the *Comité stratégique des ressources informationnelles* as part of the general consultation on the document entitled: Une réforme de l'accès à l'information: le choix de la transparence submitted to the *Commission de la culture*, September 2003, p. 6.

This type of service can be provided in a context in which, where possible, the free consent of a citizen is requested. The *Act to establish a legal framework for information technology* recognizes the validity of the equivalence of a signature on technological documents as the guarantee of an element of consent (Section 39). In this context, when a citizen wishes to have on-line access to a value-added service, it suffices to ask whether he/she authorizes the D/A to disclose his/her personal information to another D/A for the latter to be able to provide this service. This consent can be direct or indirect, i.e., it can be induced when a citizen simply requests the service depending on the type of transaction. The implementation of such mechanisms would make it possible, on the one hand, to respect the basic principles of the protection of personal information and, on the other, to benefit from the possibilities offered by new information and communication technologies in order to improve services to citizens.

RECOMMENDATIONS

5.4 We recommend that the government continue its reflections on establishing a legal framework that both respects the basic principles of the protection of personal information and facilitates the development of e-government.

5.5 We recommend that the government take all appropriate measures, such as training and awareness-raising programs, to make members of the public service and citizens accountable for the risks related to the use of e-services.

1.3 The Organizational and Technological Methods Enabling the Respect for the Basic Principles of the Protection of Personal Information and Privacy

To ensure that the basic principles and the legal obligations concerning the protection of personal information are respected in the development, deployment and operation of the computer systems through which this information is processed, clearly defined and entirely transparent mechanisms must be strengthened and consolidated. Such institutional mechanisms or means are of two types: Organizational and technological.

• *The Organizational Method*

The CAI has provided the D/As with a *Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information* (Guide for the protection of personal information in the development of information systems)[43] for use in assessing the measures adopted to protect personal information in technological projects. This guide is clearly a first step in the right direction in terms of protecting personal information in the context of the deployment of new technologies.

---

[43] *Commission d'accès à l'information, Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information: À l'intention des ministères et organismes publics*, Version 1.0, December 2002.

THE KEY CONDITIONS FOR SUCCESS (cont'd)

However, in light of consultations and developments in other countries, it appears that the Guide must be further developed. In this regard, the *Direction de soutien en accès à l'information et en protection des renseignements personnels* of the MRCI has just published the *Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes informatique par les organismes publics*.[44]

This document includes concrete, detailed rules on the steps to follow to ensure that the drafting, development, modification, implementation and commissioning of computer systems continuously respect the principles and legal obligations for the protection of personal information and privacy. It focuses on the electronic and administrative components of an information system. It covers all personal information recorded on electronic and other media and includes the administrative processes pertaining to this system. It does not include the operation and implementation phases.

Notes

The *Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes informatiques par les organismes publics*

The *Modèle de pratiques* aims to facilitate integration of the protection of personal information (PPI), while improving the quality of the process implemented across projects. The model is intended as a benchmark for public agencies to facilitate respect for the principles and legal obligations of privacy protection in the development of projects, irrespective of their size or type. It can also be applied to any program or service that uses personal information. By using this model, stakeholders are able to share a common vocabulary and determine activities to be implemented, as well as the targeted results in terms of privacy protection.

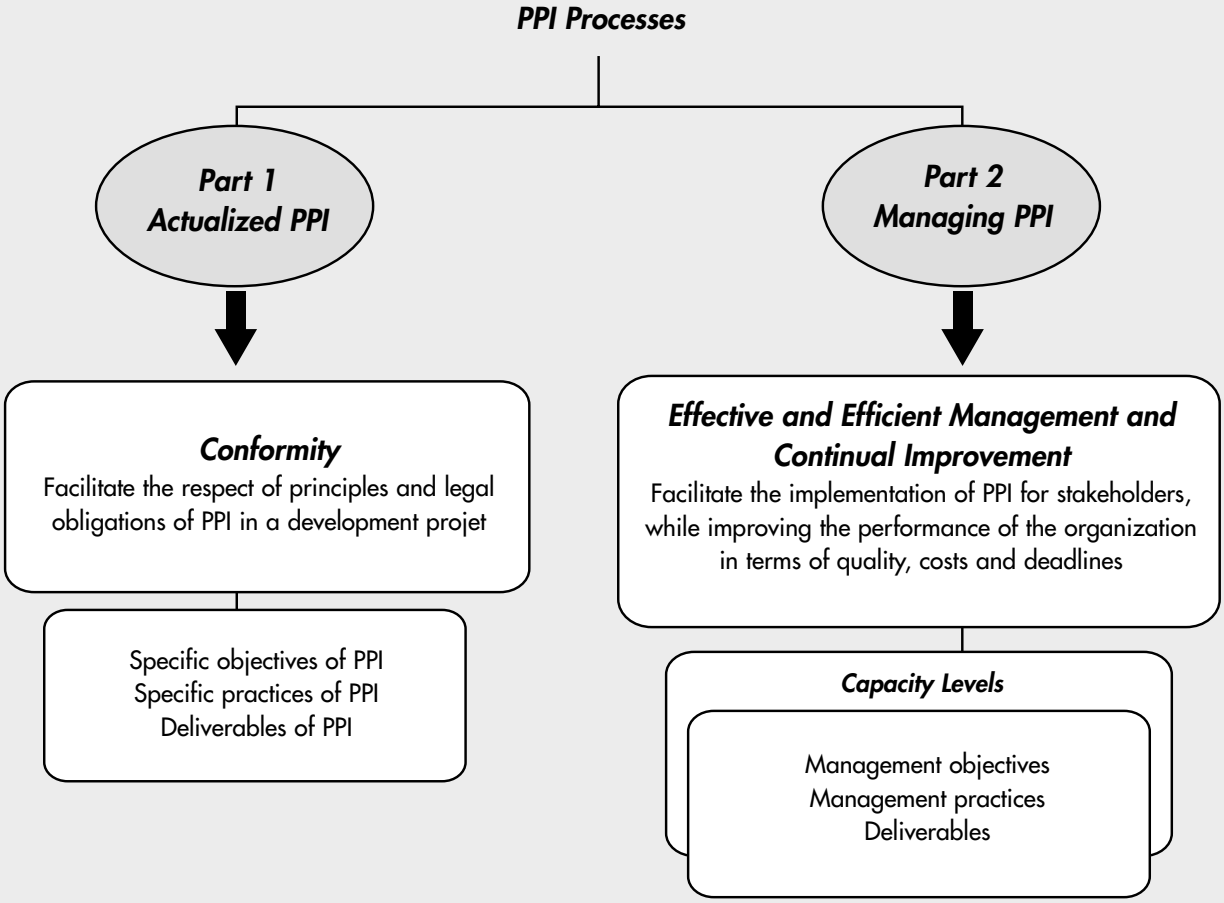
The MRCI's approach is to provide tools that enable public agencies to assume their responsibilities in the development of projects stemming from the *Act respecting access*. Use of the model is currently voluntary, and it must be adapted to the specific situation.

The figure on the following page illustrates the PPI process in development projects as proposed in the *Modèle*.

---

[44] *Government of Québec, Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics*, Version 1.0, Publications du Québec, 2004.

The *Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes informatiques par les organismes publics* (cont'd)



THE KEY CONDITIONS FOR SUCCESS (cont'd)

This practice model is necessary to ensure that following their implementation, projects do not present a risk to the protection of personal information. In fact, all too often, this issue emerges following the analysis of existing computer systems, by which time it is already too late! For example, in Québec, the CAI's opinion of the government's interim public key infrastructure[45] was given after its development. An upstream project assessment on the risks associated with the protection of privacy would no doubt have avoided the criticisms raised by the CAI in its opinion.

In addition to this practice model, a privacy impact assessment grid must also be developed as quickly as possible. This assessment is deemed necessary before starting the implementation stage of the computer systems and networks. The CAI itself stipulates "[that] it is important that the privacy protection aspect of technological projects be assessed before their implementation."[46] Several assessment grids have already been developed, specifically in Canada and France. In Québec, progress in this direction has already been made by the MRCI.

The D/As are obliged to conduct these assessments, which must be made public. In fact, the perception of risk is a social construct resulting from cultural, historical and situational factors. For this reason, transparency of the process is central to the public's trust, and the public must be able to debate it as needed. Moreover, the systems used must be shown to guarantee the right to privacy. An assessment deemed unsatisfactory would therefore have the effect of obliging the stakeholders in the project to correct or improve the systems accordingly. Conversely, a positive assessment would give the green light for the implementation of the project, subject to government approval when required.[47] In such cases, the opinions issued by the CAI would constitute important input for the government's authorization of the implementation stage. For all projects, the CAI, the agency responsible for monitoring the law, would have the latitude to conduct monitoring or issue opinions or recommendations to ensure that the projects developed by the D/As remain in compliance with the law throughout their development and use. Lastly, the minister responsible for applying the legislation governing the protection of personal information would play an advisory and supporting role in helping the D/As to conduct risk assessments and apply the *Modèle de pratiques*. He could also check the compliance of the implementation process for each risk assessment according to the criteria established. Responsibility for checking and monitoring the systems must nonetheless fall under the responsibility of D/A personnel (see Figure 12, page 127).

Having clear rules and involving the department and agency personnel responsible for the protection of personal information (PRPPI) at the project's design stage will facilitate their work, as well as the work of people who have to develop the systems that respect privacy.

Therefore, in order to solidify the structural mechanisms aimed at better protecting personal information, it is crucial to involve the D/A personnel responsible for protecting personal information (PRPPI) from the start, i.e., at the project design stage. Formal communication channels must be established, both to inform the PRPPI of

---

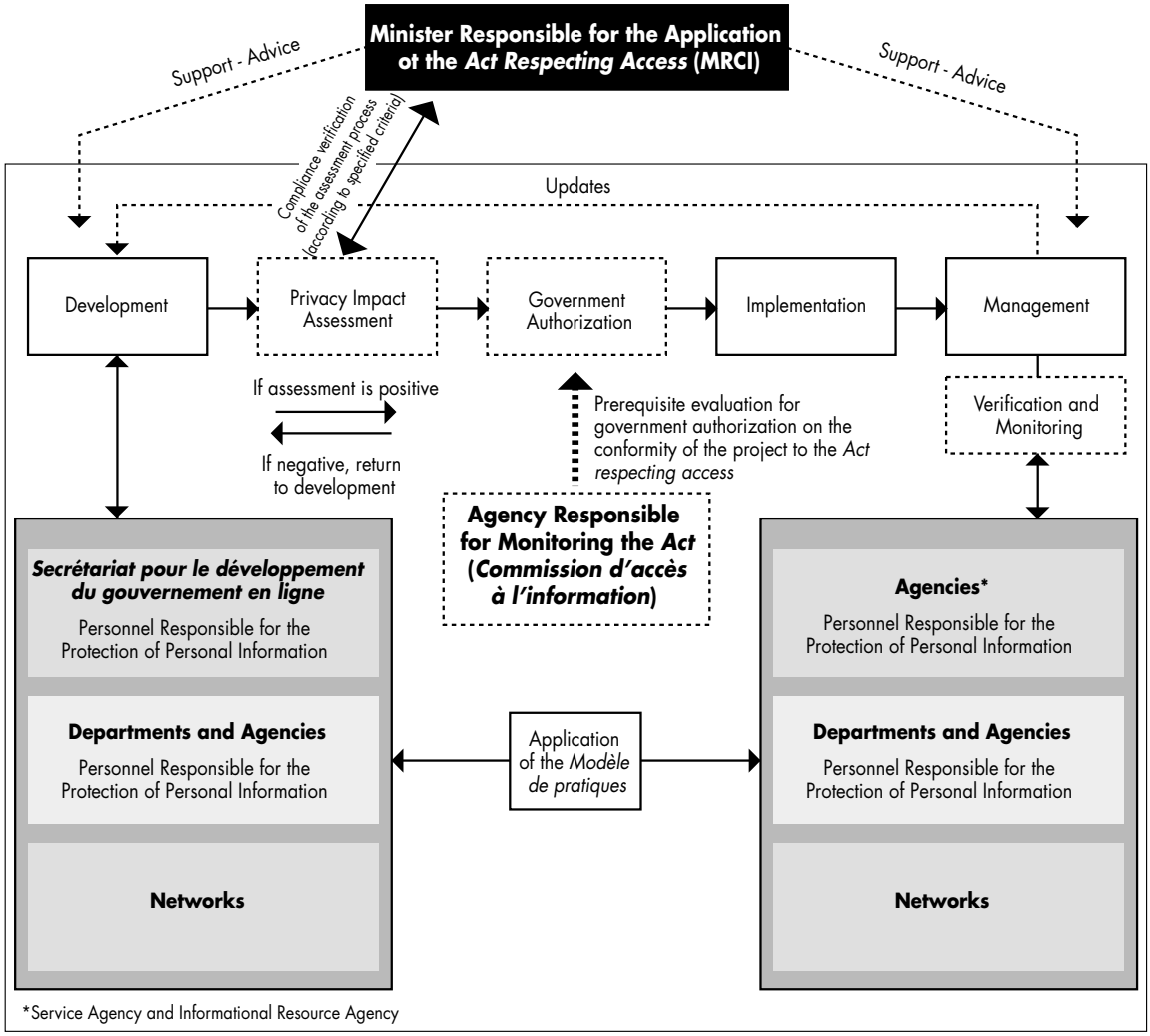
[45] *Commission d'accès à l'information, Avis de pertinence sur la solution intérimaire de l'infrastructure à clés publiques gouvernementale du Secrétariat du conseil du trésor*, File 01 11 07, August 2001.

[46] *Commission d'accès à l'information*, 2002 five-year report. *Une réforme de l'accès à l'information: le choix de la transparence, Document complémentaire de la Commission d'accès à l'information sur la consultation publique de la Commission parlementaire*, October 30, 2003, p. 27.

[47] The parameters used to determine which projects are to be submitted for government approval must be established.

developments in progress and to facilitate discussions between D/A personnel directly involved in the projects and with the PRPPI. In performing their work, the PRPPI should be supported at all times by the minister responsible for applying the legislation governing the protection of personal information. However, to fulfill these tasks and for these discussions to be productive, it is imperative that the minister responsible for applying the legislation governing the protection of personal information, the PRPPI and the agency responsible for monitoring the *Act*, i.e., the CAI, have access to the opinions and advice of specialists and experts, such as computer technicians and cryptologists. The rapid development of ICTs and their impact on the protection of privacy will require an increasingly significant use of experts to examine the possible risks related to the protection of personal information and privacy in Québec.

Figure 12: The Structural Elements Ensuring Respect for the Protection of Personal Information



THE KEY CONDITIONS FOR SUCCESS (cont'd)

Even when technological measures are implemented, they are still subject to human factors, which the government cannot totally prevent. It is therefore important to focus attention on management and administrative rules that necessarily mold behaviours and decisions concerning technological systems. The awareness-raising and training programs thus play a major role in the respect for organizational rules. On this point, the CAI notes in its November 2002 report that despite attempts at improvement, there is still much to be done for the protection of personal information to be clearly incorporated into the administrative procedures and structural culture of Québec departments and agencies.[48] Not only must there be specific rules on this matter, but training and awareness-raising programs for public servants must also be implemented to ensure that these rules are understood, assimilated and applied in compliance with the spirit of the law.

RECOMMENDATIONS

5.6 We recommend that the new *Modèle de pratiques de protection des renseignement personnels dans le contexte du développement des systèmes d'information par les organisms publiques* be implemented in all public agencies to ensure respect for the guidelines and legal obligations regarding the protection of personal information.

5.7 We recommend that a privacy impact assessment grid be developed as quickly as possible.

5.8 We recommend that D/A personnel responsible for protecting personal information actively participate in developing on-line projects and that they be supported in their work by the minister responsible for applying the legislation governing the protection of personal information.

5.9 We recommend that the minister responsible for applying the legislation governing the protection of personal information, the PRPPI in the D/As and the agency responsible for monitoring the law have access to technological or any other expertise that could help them in their work.

5.10 We recommend that the minister responsible for applying the legislation governing the protection of personal information actively participate in e-government projects by providing support and advice on the implementation and management of privacy risk impact assessments.

5.11 We recommend that D/A personnel responsible for protecting personal information establish, with the participation of the agency responsible for applying the legislation governing the protection of personal information and the CIO, awareness-raising and training programs for the stakeholders in e-government development projects such that the principles and legal obligations regarding the protection of personal information are understood, assimilated correctly and applied uniformly by all public and private agencies.

---

[48] *Commission d'accès à l'information, Rapport quinquennal 2002. Une réforme de l'accès à l'information: le choix de la transparence*, November 2002, p. 83.

- ***The Technologies***

The government must also implement institutional mechanisms, and even laws, to promote the use of specific technologies for protecting personal information and privacy. Accordingly, the technologies used must not only guarantee the protection of personal information, but must also, insofar as possible, favour the development of an environment in which the protection of personal information is strengthened.

To this end, the Dutch Minister of Justice stated, in discussing Dutch law on the protection of privacy, that:

> "[…] current IT capabilities to abuse personal data necessitate a search for supplementary possibilities to ensure personal data are treated properly and accurately. Consider partial or complete 'anonymizing,' for instance, by eliminating from personal data their identifying characteristics, or protecting them against use by certain applications/users, or by limiting their use to certain purposes. In this perspective, Amendment 22 of the Lower House to Article 13 of the Bill added that the prescribed security measures must also focus on the prevention of unnecessary collection and further processing of personal data. This will provide a legal foundation for the application of privacy-enhancing technologies. Such rules respond to the restrictions on developing information technologies."[49]

The literature on privacy-enhancing technologies (PETs) and cryptographic specialists mention a range of technological instruments that could ensure protection of privacy. Unfortunately, these instruments are still very poorly known and not yet adequately developed in the market.

In the context of the implementation of e-government, PETs seem to have all of the features necessary both to guarantee and strengthen the protection of personal information. They ensure better protection of the right to privacy by restricting the use of personal information to only those situations where it is actually necessary, but without limiting the performance of computer systems or the management of the delivery of e-services. The addition of PET functionalities to conventional systems has not reduced the performance of these systems.[50] In fact, the use of these technologies can significantly promote the respect for the principles of the protection of privacy in the government by guaranteeing that personal information is processed correctly. However, adding privacy-enhancing technologies (PETs) to current systems can be complex and expensive. We only need recall the costly review of thousands, indeed millions of programming codes on the eve of the millennium to check whether the systems were ready for the Y2K bug. Accordingly, it is crucial to consider the integration of privacy-enhancing technologies right from the outset.

---

[49] Dutch government, Parliamentary Document 25 892 # 92c, parliamentary year 1999-2000, Memory of Reply to First Chamber regarding the WBP, p. 16. Article 13: "The responsible party shall implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim to prevent unnecessary collection and further processing of personal data." http://www.cbpweb.nl/

[50] Borking, J. & C. Raab, "Laws, PETs and Other Technologies for Privacy Protection", *The Journal of Information, Law and Technology*, Vol. 1, 2001.

Privacy-Enhancing Technologies

One of the innovative privacy-enhancing technologies is the digital credential. A digital credential can be viewed as the digital equivalent of a passport. It can contain arbitrary attributes (e.g., name, citizenship, age, address, public key, pseudonyms, etc.) certified by an issuer, and therefore offer the same functionalities as a conventional identity or attributes certificate (X.509 certificates).

A digital credential differs from a conventional certificate in two ways:

- First, the credential is issued blindly (*blind signature*) such that the certificate issuer cannot recognize the credential once it is issued. Accordingly, even if during subsequent uses the user identifies himself to the certificate issuer, the latter is unable to track the use of the digital credential. It can, nonetheless, check the authenticity and integrity of the digital credential, as can the bodies (D/As) delivering the services, but without revealing the identity of the person to whom the said certificate was issued.

- Second, the user can selectively reveal certain properties of the attributes on his digital credential. He can opt to reveal only certain attributes (show only his citizenship, while hiding other attributes), show that an attribute respects a certain criterion (that his age is over 18, without revealing his exact age) or confirm that an attribute does not have a given characteristic (that his name does not appear on a blacklist, but without revealing it). In all of these situations, the user never has to identify himself formally.

These two properties make digital credentials excellent tools for building an access control infrastructure that preserves the users' right to privacy while eliminating the possibilities of tracking.

Other modern technologies can also be used for better protection of privacy without reducing the performance of the computer systems and networks.

- Certain modern encryption tools can be used, such as zero proof knowledge, to compare or corroborate personal information without disclosing the content, which people may wish to keep secret. These techniques could be used by public servants to ensure that citizens are eligible for a program without having to disclose their personal information.

- The transmission of a shared secret is another technological method that meets authentication objectives—the citizen shares secret information with all the D/As in such a way that, individually, none of them can discern or reveal this information. This technique could be used to corroborate identity during a specific exchange of personal information between D/As, such as a change of address.

- When personal information is required from one or more databases to several D/As in order to provide an integrated or value-added service, cryptographic search techniques can be used to extract from these databases only the information necessary for the delivery of services without revealing or permitting access to all of the information in the various databases on the individuals in question.

- A particularly useful technique for e-democracy and access to information is the one that permits a search for information within a database, the purpose of whitch is unknow to the database administrator or any other third party. For example, citizens or interest groups may want to search through public government information without informing others ot their actions.

For more information on these technologies, please see the references at the end of this report or the PET projects currently underway:

- CAFE: http://www.semper.org/sirene/projects/cafe/
- CYBERVOTE: http://www.eucybervote.org/main.html
- PISA: http://www.pet-pisa.nl/pisa_org/pisa/index.html
- SEMPER: http://www.semper.org/
- RAPID: http://www.ra-pid.org
- FIDIS: http://csrc.lse.ac.uk/research/fidis.html
- PAMPASt: http://www.pampas.eu.org

The Underdevelopment of Privacy-Enhancing Technologies

The literature on the subject and the testimony of specialists in the field mention numerous reasons for the underdevelopment of privacy-enhancing technologies. First, in a context in which governments' legal frameworks do not require or promote the implementation of privacy-enhancing technologies, the demand for these new technologies is not felt. A legal framework promoting privacy-enhancing technologies would stimulate the private sector to develop these technologies. Second, the development of these technologies is being held back by various market forces in the software industry. The specific characteristics of the software market, specifically the current near-monopoly situation, is likely largely responsible for market failures. In effect, concentration in

THE KEY CONDITIONS FOR SUCCESS (cont'd)

the programming sector is such that the suppliers control the market with respect to price and the development of technologies used. According to many specialists in the field, this situation means that the software marketed is often little more than simple upgrades aimed at resolving bugs identified in the previous versions. In terms of innovation, the cost of developing new computer technology often exceeds the returns. Also, the industry is no longer dominated by "start-ups" and innovation, as was clearly the case at the start of the new economy. In this context, *The Economist* states that research and development in the software industry is far more an issue of production than innovation. Referring to statements by George Gilbert (co-founder of the TechStategy Group), the article's author reports that the bulk of efforts are focused on maintenance, upgrades and resolving software bugs (*The Economist*, November 17, 2003).

For example, public key infrastructures (PKI), which are widely used by governments and organizations around the world, and whose primary function is to ensure secure transactions between users in an insecure environment (i.e., the Internet), do not necessarily meet the privacy protection needs of e-government. In fact, an impressive number of specialists, in particular privacy protection commissioners in many countries (including the CAI in Québec, the Information and Privacy Commissioner (IPC) in Ontario and the Office of the Federal Privacy Commissioner (OFPC) in Australia) have shown that the PKIs in their traditional systems can pose potentially high risks for privacy protection by enabling, through their operations, numerous functions that can be used for profiling, tracking, revealing information, etc. The presence of these elevated risks must be managed by appropriate legal and regulatory frameworks. However, the fact that the application of these measures is generally quite expensive must be taken into consideration.

Accordingly, the cost of developing and marketing new products specifically for the purpose of privacy protection seems too high for industry giants. In order to market these software products, the clientele would require further education, specifically on the new information and communication technologies.

* For example, Clarke, R., Conventional Public Key Infrastructure: An Artifact Ill-fitted to the Needs of the Information Society, prepared for submission to the Research Track - IS in the Information Society, Eur. Conf. on Inf. Syst. (ECIS 2001), Slovenia, Version of November 13, 2000 (http://www.anu.edu.au/people/Roger.clark/II/PKIMisFit.html); Brands, S., Rethinking public key infrastructures and digital certificates; building in privacy, MIT press, August 2000; Radicchio, PKI and the protection of data and privacy, White paper WP-LEG-003, version 1.0, 2000 (www.radicchio.org).

RECOMMENDATIONS

5.12 We recommend that the minister responsible for applying the legislation governing the protection of personal information, in collaboration with the CIO, make designers and network and infrastructure managers aware of the new privacy-enhancing technologies.

5.13 We recommend that the government encourage and support research and development in privacy-enhancing technologies.

5.14 We recommend that the government look into the possibility of establishing a legal framework to ensure that the technologies comply with the imperatives regarding the protection of privacy (privacy-compliant and privacy-enhancing technologies).

1.4 Toward a Culture of Security

The protection of personal information is the outcome of numerous components, security being just one of them. However, security also includes many other components. As part of the new virtual reality in general, and the implementation of e-government in particular, the security aspect takes on significant importance.

The digital age has introduced a whole new set of risks in the transmission of information. The explosion in the number of Internet users around the world[51] and the ease of sharing knowledge that can be used for cyber-crime increase the vulnerability of computer systems. Hence, the increased importance placed on computer and network security is justified.

> "Information security protects information against a wide range of threats so as to ensure the continuity of activities, minimize the damage caused and maximize the return on capital invested and business opportunities."[52]

Most stakeholders–businesses, individuals and the government itself–do not seem to be fully aware of the issues related to information security, relying for the most part on the efficiency of common tools such as firewalls and antivirus software. And yet, systems are becoming increasingly complex and involve interconnected networks and infrastructures. The risks are therefore considerable: Loss of information, breach of confidentiality and, above all, lack of citizens' faith in ICTs. Lastly, the financial losses resulting from computer security incidents can result in not insignificant costs for the economy.

---

[51] 630 million Internet users according to data compiled at the World Summit on the Information Society (2003).

[52] *Secrétariat du Conseil du Trésor, Gestion de la sécurité de l'information, première partie: code de bonne pratique pour la gestion de la sécurité de l'information,* BS 7799-1, 1999.

THE KEY CONDITIONS FOR SUCCESS (cont'd)

For example, *Canadian Healthcare Technology Magazine* states that:

> "15% of Canadian hospitals admitted having had their computer security breached in the past year. In addition, 57% of institutions surveyed said that some of their employees bypassed the computer security systems because they found them too time consuming. Moreover, more than one-third of hospitals surveyed had no disaster recovery plan in the case of loss of information, nor a backup plan that would enable a continuation of activities in the event of a computer failure."[53]

For all these reasons, computer security in Québec is a major issue for everyone involved. It is therefore imperative that measures be taken to develop a security culture in Québec. This security culture rests primarily on awareness-raising and accountability of everyone involved at every level, including the citizens who use e-services. A computer system can only be secure provided the risks are managed at every level and the rules of good practice are respected by all. System administrators must also be credible and reliable. The users in the public administration and in the general population must also know these rules and the risks associated with the use of computer systems. To do so, the government must develop relevant programs or awareness-raising and training mechanisms.

At its 1,037th session in July 2002, the OECD established nine guidelines for the security of information systems and networks, which can be summarized as follows:[54]

1) **Awareness:** The stakeholders must be made aware of the need to ensure the security of information systems and networks and of the actions they can take to strengthen security.

2) **Responsibility:** The stakeholders are responsible for the security of information systems and networks.

3) **Response:** The stakeholders must act promptly and in a spirit of cooperation to prevent, detect and respond to security incidents.

4) **Ethics:** The stakeholders must respect the legitimate interests of other stakeholders.

5) **Democracy:** The security of information systems and networks must be compatible with the fundamental values of a democratic society.

6) **Risk Assessment:** The stakeholders must conduct risk assessments.

7) **Security Design and Implementation:** The stakeholders must integrate security as a central component of information systems and networks.

8) **Security Management:** The stakeholders must adopt a comprehensive approach to managing security.

9) **Reassessment:** The stakeholders must examine and reassess the security of information systems and networks and introduce the appropriate changes to their security policies, practices, measures and procedures.

---

[53] *Canadian Healthcare Technology Magazine*, 2002.

[54] OECD, *OECD guidelines for the security of information systems and networks: Towards a culture of security*, July 2002.

Figure 13: Guidelines for the Security of Information Networks and Systems

The application of these guidelines in the delivery of e-services is more than satisfactory for establishing and maintaining the public's trust in and support for new technologies and, in particular, the use of these technologies to implement a project such as e-government.

As such, these guidelines would also be able to satisfy the ultimate goals that security specialists indicate as required of a computer system:

1. **Availability:** Property whereby information or an information system is accessible or available at any time or when needed.

2. **Integrity:** Property whereby data or information can be edited or changed by authorized persons only.

3. **Confidentiality:** Property whereby data or information, such as personal information, can be accessed by authorized persons only.

4. **Authentication:** Action used to establish the validity of a person's identity or an e-document or Internet site.

5. **Irrevocability:** Property whereby information, an action or a document is irrefutably and clearly attributed to its author or to the device that generated it.

Specifically, authentication and irrevocability present major challenges within the framework of e-government in which transactions will increasingly be carried out in a virtual forum from which physical contact has been eliminated. In fact, on-line identification of citizens is a major issue in the delivery of e-services. Accordingly, the government must establish mechanisms to ensure that these ends are achieved, thereby smoothing the delivery of e-services.

Several years ago, the Québec government initiated actions to ensure the security of technological systems within the public administration. This resulted in the creation of institutional mechanisms, specifically the *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernemental*, which came into effect in November 2000.[55] This directive sets guidelines for security management to be applied by the D/As and the responsibilities of the D/As in terms of security. Although this initiative has proven successful, closer follow-up is needed, since the guidelines do not seem to be uniformly applied by all D/As. The programs must also be improved and strengthened in this respect. Also, it would be appropriate to review this directive to ensure the security of both digital information and information on paper.

The Québec government has also implemented mechanisms for managing security and has developed a set of measures aimed at ensuring the protection of digital information and the availability of public services. The CERT/AQ, whose role is to support the D/As in managing security incidents, is one of these measures. Furthermore, the CERT/AQ maintains a security watch and is able to call in experts in this field. This measure must be encouraged and strengthened. Nonetheless, these services are only available to government departments and agencies–citizens, businesses and network organizations, both in health and education, do not have access to them.

- ***A Preferred Avenue: Institute for Security of Information Systems and Networks of Québec***

Given this shortcoming and the importance of security in establishing a climate of trust in developing e-government, it seems necessary that an external agency, one that has already established its credibility, be used to promote the project and raise awareness among the stakeholders and the general public in the application of security guidelines. This external agency could act as a lever for cooperation between the various stakeholders, both in the private and public sectors, to ensure that the exchange of information on threats and system vulnerabilities is carried out correctly and efficiently. Moreover, this external agency would be well placed to assess the systems and the administrative organization needed to certify and confirm that they respect appropriate practices. An analogy can be drawn between the need for certification and accounting processes–individuals are responsible for keeping their own books, but an accountant certifies the accuracy of the books and the accounting practices.

To counter growing security concerns, the *Centre de recherche informatique de Montréal* (CRIM) is proposing the creation of the ***Institute for Security of Information Systems and Networks of Québec*** (ISIQ) under a public-private partnership.

---

[55] *Secrétariat du Conseil du trésor, Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale,* November 23, 1999.

Such an institute would be intended as a catalyst for services, expertise and the best security practices for digital information. Its mission would be to promote and coordinate actions aimed at ensuring the security of digital information in Québec society. Its scope of action would be determined by four main principles, i.e., prevention and awareness-raising, detection of and reaction to emergency situations, technology watch and research, and support for delivering services. More specifically, the ISIQ could become the agency that would provide Québec with certification programs founded on international standards based, among others, on the OECD guidelines for the security of information systems and networks.

RECOMMENDATIONS

5.15 We recommend making computer and network security a government priority in order to position Québec as a leader in computer security.

5.16 We recommend that the CIO ensure the general application of the *Directive sur la sécurité de l'information numérique et des échanges électroniques.*

5.17 We recommend that the government support the creation of the *Institute for Security of Information Systems and Networks of Québec* as proposed by the CRIM (*Centre de recherche en informatique de Montréal*) as an avenue of interest to promote and support.

5.18 We recommend that the CIO implement awareness-raising and training programs on computer security for all parties directly involved in the e-government project.

1.5 Identification

In the context of developing e-government in which the government is increasingly called on to offer interactional, transactional and integrated services, the identification of users becomes a major issue. In a virtual world where services are delivered remotely and where there is no physical interaction, a positive identification process for users is essential to ensure that the person sitting at the computer is eligible for and entitled to receive an e-service. In its annual report, the *Commission d'accès à l'information* says: "Remote identification presents a higher risk of error than face-to-face identification. This additional risk must be considered."[56]

To ensure that users of services are indeed who they claim to be, the service provider that already holds personal or other identifying information on the users, for example, the personal access code used by the MRQ, need only compare this information with that provided by the users. This type of procedure is commonly known as a "shared secret." However, when the service provider holds no personal or identifying information

[56] CAI, 2002 five-year report. Une réforme de l'accès à l'information: le choix de la transparence, November 2002, p. 86.

about the users, mechanisms must be available to obtain reasonable guarantees as to the users' identity. Section 38 of the *Act to establish a legal framework for information technology* sets out identification objectives in a virtual world:

"The link between a person and a technology-based document, or the link between such a document and an association, a partnership or the State, may be established by any process or combination of processes to the extent that it allows:

1. The identity of the person or the identification of the association, partnership or the State and, where applicable, their location, to be confirmed, and allows their link with the document to be confirmed;

2. The document to be identified and, if need be, allows its origin and destination at any given time to be determined."

The degree of certainty regarding the eligibility or identity of the person with whom the service provider is in contact is proportional to the sensitivity of the information exchanged–the more confidential the information exchanged, the higher the need for certainty regarding the person's identity, and the greater the need for security of the means employed to confirm that person's identity, and, therefore, the higher the cost.

The main challenge in establishing an electronic identification process consists in implementing a system that is as simple as possible to use, while minimizing the risks of disclosing personal information.

Canadian E-Pass Project

The e-pass project aims to give all Canadian citizens a unique digital identifier to enable them to use transactional services that involve the exchange or transfer of personal information without compromising their right to privacy. The e-pass is based on an average security identification process, following which a public key is issued to the citizen. By using this public key and a password (private key), the citizen can then identify himself to each department or agency with which he conducts business. In the coming years, the federal government intends to make this infrastructure available to the provinces for use in their own delivery of transactional services to citizens. As with the SQAG, this system is perfectible in terms of privacy protection.

- ***Current Situation***

The Québec government has designed an identification system called the *Service québécois d'authentification gouvernementale* (SQAG). The objective is to deploy an identifier, usable by any government department, that provides an acceptable level of certainty and that can move toward higher levels of certainty. The SQAG was also designed to be compatible with the authentication system developed by the federal government. This could eventually give citizens and businesses access to both federal and provincial government e-services using the same identifier. Identity verification is carried out by the first department or agency contacted by the citizen to obtain an on-line service with shared secrets (exchange of personal information concerning the requestor held by both the latter and the service provider). At the request of the department or agency providing the service, a certificate provider then issues an identifier containing only a pseudonym which does not directly reveal the holder's identity. The departments and agencies can then make the link between a certificate and a citizen without having access to the personal information used in establishing his/her identity. The transaction logs associated with the use of a certificate are kept by the certificate provider, which is unable to determine the identity of the certificate holders, since the information on their identity is kept by another body.

The SQAG is also introducing several measures to minimize the possibilities of tracing and profiling, one of these being to give citizens the option of using several identifiers.

The SQAG, while still in the development stages, represents a promising avenue with respect to protecting privacy and largely resolves the issue of on-line identity authentication.

- ***A Perfectible System***

Some analysts who have examined the SQAG and other similar systems based on the use of X.509 certificates, which include Entrust technology (www.entrust.com), are nonetheless critical regarding the risks related to the protection of personal information. The implementation of an organizational framework makes it possible to manage the risks related to privacy protection. This is all the more important when the technology does not in itself counter a number of these risks, some of them quite high. This type of management structure often requires heavy investment, both in terms of funding and human resources.

For example, the *Registre des droits personnels et réels mobiliers*, whose structure is based on a standard public key infrastructure, carries risks with regard to users' privacy. However, these risks are relatively well controlled through the use of appropriate management administrative measures.

In fact, when issuing certificates, the certificate provider can use standard network functions to easily identify the user's IP address (see insert on the next page). Even if the D/A acts as an intermediary between the certificate provider and the user, the IP address is revealed on redirection through the user's browser. Accordingly, the certificate provider can geographically locate the receiver of the pseudonym, which easily enables it to determine the address. It could then use this information and match it with the pseudonym(s) it knows to create user profiles. Furthermore, the fact that the user can opt to use the same pseudonym for all of his e-services further increases the risk of profiling.

Notes

What Is the IP Address?

To use an analogy, the IP address works in basically the same way as a postal code in a regular mailing address. The IP address comprises four groups of numbers that identify each computer on a network so they can communicate with each other. An IP address has a 32-bit representation and is written in the form of four bytes separated by periods (e.g., 192.168.10.66).

Because they eliminate such risks, modern cryptographic techniques are a promising avenue for the future in dealing with these concerns. Since these technologies are not yet fully developed and accessible, it is still important for the government to encourage their development as quickly as possible so that it can incorporate them into the design of its on-line identification and authentication solutions. For example, the blind signature and restrictive blind signature would prevent, with a high degree of certainty, the certificate provider from being able to use standard network functions, such as the IP address, to establish profiles on the recipients of pseudonyms. In fact, because of modern cryptographic techniques, the certificate provider is totally unable to find out the pseudonym it issues. Only the users know the pseudonyms, and only the departments and agencies can match pseudonyms with individuals' internal files. In this case, the D/As need only verify the authenticity of the certificate (the signature) with the certificate provider.

In conclusion, it appears that the risks related to the profiling of users' information are not totally eliminated with the SQAG. The SQAG currently being developed by the Québec government should include additional features that would enhance the application of privacy guidelines.

RECOMMENDATION

5.19 We recommend continuing the development of the SQAG while maintaining current efforts to reduce the risks related to the protection of personal information as much as possible and to ensure harmonization and compatibility with the federal government's actions in terms of issuing certificates.

2. Simplifying Access to Government Services

In general, the goal of e-government is to simplify access to government services by focusing on multiservice centres, promoting free network access, expanding the broadband network and taking into consideration the specific needs of people with motor, sensory or cognitive disabilities (see Figure 14, page 149).

2.1 Focusing on Multimodal, Multiservice Centres

As previously mentioned, e-government must consider people who cannot or do not wish to use a computer or the Internet. They too must have access to the new services developed. Accordingly, multiservice centres must be developed parallel to call centres. The Communication-Québec network and the network of local employment centres (LECs) provide a good starting point for housing these multiservice centres. However, agreements between the two departments concerned must be made as quickly as possible to enable the rapid establishment of the multiservice centres.

• *The New Role of the Public Servant*

The implementation of multiservice centres, be it a service counters or a single telephone number, requires the full support of the public servants involved. In fact, the work of public servants will be decompartmentalized to enable them to answer any queries or requests from citizens which go beyond the strict boundaries of a department or agency.

To properly implement this project, the Québec government should look at the remove experience of *Service New Brunswick*, which has had great success in setting up multiservice centres similar to those proposed in the report for Québec. The public servants who greet and serve citizens were closely involved in the project from the outset. In general, these public servants consider that the broadening of their tasks stemming from a decompartmentalization of the services provided enables them to meet the needs of citizens more efficiently, since they are now able to follow requests through the various government bodies from start to finish. These broader responsibilities give public servants a feeling of accomplishment and greater motivation.

2.2 Promoting Free Access to the Network

In any democratic society, access to information must be viewed as a right, just like any other basic right. Over the years, the Internet has become one of the main vehicles for information. For many people, "[…] the social appropriation of technologies must be seen as the right to access technologies, like any other right, such as education, communication, information, etc."[57]

Clearly, private enterprise has developed the Internet access market, demanding fees to connect to the network. This situation has resulted in competition that has proven beneficial to citizens, with the cost of access in Québec being among the lowest in the world. Nonetheless, it remains that a responsible government must help citizens who do not have the means or who have other financial priorities to access the network by increasing free public access workstations. An individual's personal financial situation should not prevent him/her from accessing the Internet.

---

[57] *Communautique, Inforoute Points d'accès,* November 2003, p. 6.

THE KEY CONDITIONS FOR SUCCESS (cont'd)

Accordingly, between 1995 and 1998, the *Fonds de l'autoroute de l'information* granted $7 million to install over 1,120 workstations in 831 public libraries across Québec. Today, every independent public library and most libraries affiliated with a regional centre are now connected to the Internet (most connections are dial-up; the need for communities to have high-speed connections is discussed in the following pages). The public library network can also help citizens unfamiliar with new information technologies in accessing the Internet. In effect, the library staff could become resource persons and thus assist users unfamiliar with surfing the Internet and the delivery of government e-services.

Other initiatives, primarily conducted by community action groups, are already underway to make free public Internet access stations available to Quebecers.[58] For example, the *Communautique* group has set up 98 Internet access stations across Québec. This network, in addition to offering users free access to terminals connected to the Internet, has a mission to raise awareness and educate its clientele about using ICTs. The work of this group is founded on a strategy of having a presence in the community over many years: Managers must know their potential clientele to earn the community's trust. This community presence must therefore be based on a medium-term strategic plan, which is only possible if the recurrent funding for these organizations is assured for several years.

In this context, it is preferable that the government develop a partnership with community organizations to make training and free Internet access available to citizens who need it. It should also work with the federal government in an effort to strengthen and streamline services.

In addition to supporting non-profit organizations, the Québec government must simultaneously increase the availability of free Internet access, possibly through its multiservice centres. This initiative, based on an existing network, would be inexpensive and contribute to facilitating initiation to ICTs.

---

[58] The experiment appears to show that interactive terminals, viewed for some time as the way of the future, are not the solution. In the opinion of Bell Canada, which conducted the trial, the installation of public interactive terminals is unpopular (people are unfamiliar with this type of interface and decline to use it) and very expensive (since the main feature of the terminals is their availability in public spaces, they are subject to breakage and vandalism). Lastly, it appears that users of Internet services are less inclined to send sensitive information over an interactive terminal, placing greater trust in a standard computer terminal.

RECOMMENDATIONS

5.20 We recommend setting up a partnership program with community groups to offer all citizens real access to the Internet and to take the necessary steps to ensure these partner groups have access to recurrent funding for their medium-term survival.

5.21 We recommend implementing a training program for resource persons who will provide support to users in libraries, community access centres and government multiservice centres.

5.22 We recommend promoting initiatives aimed at making free public Internet access workstations available to all citizens at municipal libraries and government service centres, among others.

2.3 Extending the Broadband Network

For the largest possible number of Quebecers to benefit from the e-government project, the government has the responsibility to expand access to the high-speed network to the whole of Québec. Increasingly, access to broadband services is necessary to be able to profit from the full potential of services offered on the Internet. According to a recent study by Statistics Canada, broadband service "enables applications that are simply not possible with "dial-up" Internet access, which use a telephone line and standard modem."[59] The same applies for any application that requires video (used mainly by institutions for telemedicine and distance learning, for example).

The Québec Liberal Party's action plan adopted in September 2002 also stresses the need for high-speed connection: "In this new age, a high-speed Internet connection is as essential as electricity or the telephone. […] Equal access to technologies must become a basic principle in the development of Québec society."[60] In his inaugural address on June 4, 2003, the Premier declared: "We are going to connect the regions. Before the end of this mandate, high-speed access will be available in every region of Québec."

In this same study, Statistics Canada reports that "nearly half (49%) of all Canadian households that use the Internet regularly had a high-speed Internet connection in 2001," which places Canada among the countries with the highest rate of broadband use in the world (Korea ranks first, Canada second and Sweden third in terms of the proportion of high-speed users vs. the total population). Québec is lagging behind the rest of Canada, with only 42% of households having a high-speed connection. The same study showed that in 2002, "58% of businesses using the Internet had broadband technologies."

---

[59] Statistics Canada, *High speed on the Information Highway: Broadband in Canada, Connectedness series*, September 2003.

[60] http://www.plq.org/tousdocuments/planaction.pdf, p. 33.

THE KEY CONDITIONS FOR SUCCESS (cont'd)

Many technologies can now provide a broadband or high-speed connection,[61] the main ones being a cable modem, digital Internet access line (offered by telephone service providers) and satellite. Whereas the latter is still very expensive and not available everywhere in Québec,[62] cable and digital access require that cable and telephone companies upgrade their existing basic infrastructure. However, such an upgrade involves investments that only become profitable once a certain number of subscribers has been reached. For this reason, telephone and cable companies are not yet able to provide high-speed Internet access throughout Québec, even though their basic infrastructure covers the entire province (particularly telephones). Accordingly, in 2001, only 27% of small communities[63] with access to cable also had access to cable Internet.

The telecommunication companies interviewed estimate that over 90% of Quebecers are able to access high-speed Internet. Although this proportion is encouraging, the government still has a responsibility toward the remaining portion of the population that does not have access to these services, all the more so since it is often this most remote population that could benefit to the greatest extent from these services (for example, distance learning or the delivery of government e-services).

To extend access to high-speed Internet to all remote regions, the National Broadband Task Force proposes "*infrastructure support*, where incentives are offered to broadband providers to expand service and *community aggregation,* to pool the demand of various groups that could potentially benefit from broadband services."[64] Several programs meeting these objectives have already been set up in Canada. For example, in Alberta, the *SuperNet* program, which relies on a public-private partnership, has enabled 422 remote communities to get an Internet connection for an investment of $193 million. The federal government plans to invest $105 million over three years as part of the pilot program called Broadband for Rural and Northern Development,[65] which aims to extend the broadband network to remote communities by funding up to 50% of the necessary infrastructure costs, with the remaining portion funded by service providers and the communities themselves.

---

[61] Statistics Canada reports that the National Broadband Task Force established a high-speed connection as one that has a minimum bidirectional transmission speed of 1.5 Mbps.

[62] The Hughes Aircraft satellite, marketed by several companies in Canada, is positioned above the U.S. This means that the further north one goes, the more difficult signal access becomes, being almost impossible at the latitude of Lac-St-Jean. A second type of satellite link is possible (used by telephone and television companies), but its cost is too high to be a potential solution, except for extremely remote locations (Source: *Conseil du Trésor).*

[63] By small communities, Statistics Canada means census divisions outside of the census metropolitan areas and census agglomerations (fewer than 10,000 residents).

[64] Statistics Canada, High Speed on the Information Highway: Broadband in Canada, Connectedness series, September 2003, p. 21.

[65] To date, Québec has submitted 33 projects to the program, three of which have been accepted for a total subsidy of $4.8 million.

In Québec, the *Villages branchés* program involves a partnership between school boards, municipalities, private firms and the government in order to extend high-speed Internet access to remote regions. By connecting schools and municipal buildings to the broadband network, the program provides leverage to accelerate the deployment of private sector infrastructure. In this way, it meets one of the needs raised by the CANARIE group[66] regarding the development of solutions that permit access to high-speed Internet. The group promotes initiatives that enable citizens or municipalities to manage their own Internet connection by building their own infrastructure to enable them to connect to an existing network.

Villages branchés du Québec Program

The *Villages branchés* program connects school boards to municipalities, with the external connections provided by the government's current service networks, such as the *Réseau d'information scientifique du Québec* (RISQ), the *Réseau de télécommunication multimédias de l'administration publique* (RETEM) and the *Réseau de télécommunication socio-sanitaire* (RTSS). The use of fibre optics is explicitly promoted by the program. By analogy with the housing sector, the project funding model is like a condominium, where each partner contributes to the implementation of the infrastructure. The program assumes two-thirds of eligible expenses, with the remaining one-third being covered by the eligible organizations. The *Ministère de l'Éducation* and the *Ministère des affaires municipales, du sport et du loisir* commit the initial amounts and are subsequently reimbursed if the projects are approved under the program. Each project is subject to a preliminary study before any application is submitted to the *Villages branchés* program. These studies are subsidized by the *Fonds de l'autoroute de l'information* up to a maximum of $25,000.

By the end of 2003, 14 projects had been completed for a total investment of $71 million. Of this amount, $39 million came from the *Villages branchés* program and $32 million was directly invested by the developers and private partners. At the same date, a further 46 projects were under consideration, for a total potential investment of $107 million by the State and $80 million by the developers and private partners. The government has just granted $150 million to the program to implement the projects submitted. Eventually, the completion of these projects will enable the connection of some 800 municipalities across Québec.

By facilitating the deployment of a basic infrastructure between the target institutions, the program minimizes the investment needed from private developers to connect businesses and private households to the broadband network. "The telecommunication companies that join in the projects funded by the program […] can benefit by adding transmission capacity which they could use to serve companies and households in the regions in question. […] This private investment would not be possible without the cost sharing between the public and private sectors enabled by the program."

Source: *Secrétariat du Conseil trésor*, internal document, 2004

[66] CANARIE Inc. is a non-profit organization supported by its members, project partners and the federal government. The organization's mission is to accelerate the development and use of high-speed Internet in Canada by facilitating the widespread adoption of faster, more efficient networks and by getting the next generation accustomed to advanced products, applications and services. (Taken from the organization's Web site. For more information, go to http://www.canarie.ca)

RECOMMENDATIONS

5.23 We recommend that the government, in partnership with telecommunication networks present in Québec, ensure that high-speed Internet access becomes a reality for almost all Quebecers by the end of 2007.

5.24 To reflect government priorities, we recommend that all citizens be given regular progress reports on the deployment of broadband in Québec.

2.4 Acknowledging People with Motor, Sensory or Cognitive Limitations

The e-government project aims to improve the services to which all Québec citizens and businesses are entitled. Above all, people with motor, sensory or cognitive limitations must not be left behind by the project, especially since the Internet can, for this specific clientele, be a particularly rich sea of information, as well as a way to communicate with others in similar situations. The Internet not only provides a more practical way of accessing government services, but also opens up possibilities that would otherwise be inconceivable. "For people without disabilities, technology makes things convenient; for people with disabilities, it makes things possible."[67] However, Internet access for these specific clienteles is only possible insofar as the relevant technical elements and specific orientations are considered and incorporated into formal rules.

In relation to Bill 155 on the exercise of the rights of the disabled, the *Comité d'adaptation de la main-d'œuvre* (CAMO) stressed in its brief "[that it] is clear that without a formal commitment on the issue [access to information and communication technologies] by the Québec government, the digital divide facing the disabled will continue to widen and will soon resemble a real chasm.[68]

---

[67] Treviranus, J., *Expanding the Digital Media in More Human Directions*, 2000, cited in *Comité d'adaptation de la main-d'œuvre (CAMO) pour personnes handicapée.*, Bill 155, an Act amending the Act to secure the handicapped in the exercise of their rights and other legislative provisions, Brief submitted by the *Comité d'adaptation de la main-d'œuvre pour personnes handicapées*, 2003, available at www.camo.qc.ca/camo/proloi155.htm (February 2004), p. 9.

[68] *Comité d'adaptation de la main-d'œuvre (CAMO) pour personnes handicapées*, Bill 155, an Act amending the Act to secure the handicapped in the exercise of their rights and other legislative provisions, Brief submitted by the *Comité d'adaptation de la main-d'œuvre pour personnes handicapées*, 2003, available at www.camo.qc.ca/camo/proloi155.htm (February 2004).

a) A Step in the Right Direction

The federal government has included specific accessibility criteria in the Common Look and Feel standards and guidelines,[69] for example, by providing subtitles, a telephone helpline, etc. Departments are required to follow these standards. The Ontarians with Disabilities Act, 2001[70] includes provisions on the accessibility of Web sites.

In Québec, the *Ministère des Relations avec les citoyens et de l'Immigration* has set up the *Cadre de diffusion de l'information gouvernementale sur l'Internet*,[71] which offers several minimum guidelines for accessibility. It appears, however, that these are not systematically applied.

In fact, according to a recent study[72] that analyzed some 50 Québec government sites, the vast majority (94%) have a degree of accessibility ranging from zero to poor. The *Cadre de diffusion* should be enhanced to include full instructions on accessibility standards and techniques.

The Technical Components Related to Web Site Programming and Accessibility

The ability of people with motor and sensory limitations to access Internet sites is closely related to programing components and can easily be taken into account in the initial programming of the sites. The most frequently encountered errors were:

- Errors in HTML or CSS coding;
- Lack of textual equivalents for the images;
- Use of overly small font or insufficient contrast between text colour and background colour;
- Missing or poorly used headers;
- Use of Java script (partially supported by adaptation technologies);
- Script inaccessible by the keyboard;
- Windows opening without warning;
- Change of language not identified;
- Poorly associated or missing form labels.

---

[69] Treasury Board of Canada Secretariat, Common Look and Feel, available at http://www.cio-dpi.gc.ca/clf-nsi/index_e.asp (February 2004).

[70] Ontario government, Ontarians with Disabilities Act, 2001, Chapter 32, Laws of Ontario 2001.

[71] The *Ministère des Relations avec les citoyens et de l'Immigration, Cadre de diffusion de l'information gouvernementale sur Internet*, available at www.webmaestro.gouv.qc.ca/ress/Cadre/cadre.htm

[72] Jean-Marie D'Amour, *Rapport synthèse sur l'évaluation sur l'accessibilité des sites Web québécois et canadiens francophones*, 2003, available at www.accessibiliteweb.org [on-line] consulted February 20, 2004.

b) Use of Simplified Language

Making information on the Internet accessible also means that texts must be simplified and lightened for them to be understood by as many people as possible, including people with limited cognitive abilities. It is important to note the alarming statistics on illiteracy in Québec. Given this situation, the user-friendliness of Web pages is critical in receiving the support of users (use of signs and pictures to explain actions, for example). Moreover, the level of language must be understood by as many users as possible and satisfy the need for fast, even instantaneous, communication inherent in Internet actions. Although great strides have been made in recent years on these two points (user-friendliness and level of language), there is still room for improvement, for example, concerning the length and complexity of contractual clauses found on many sites during transactions.

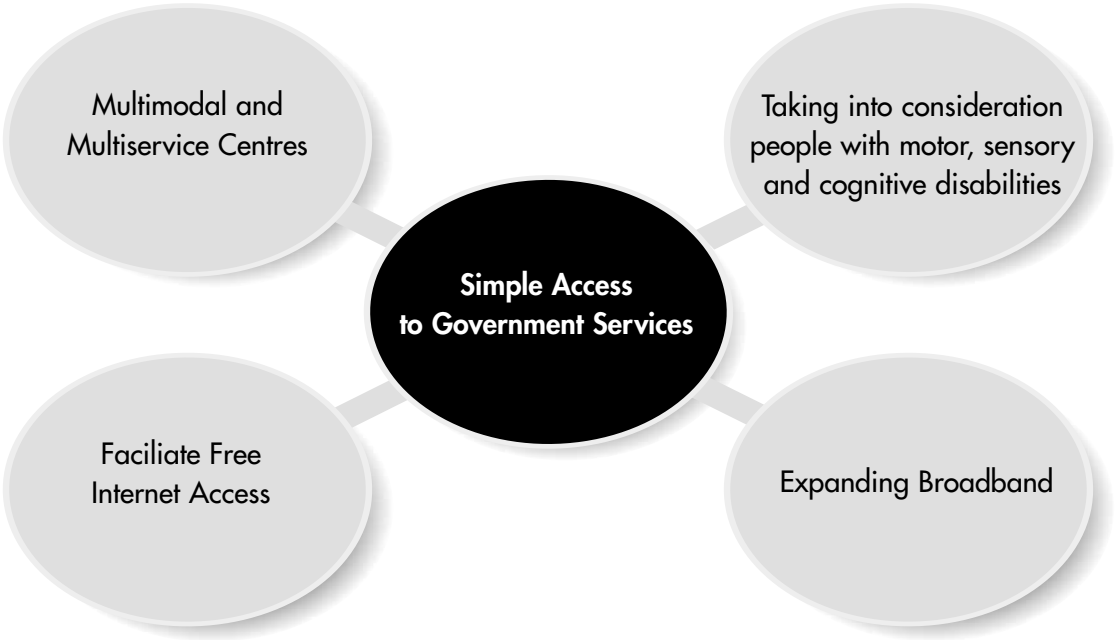
RECOMMENDATIONS

5.25 We recommend drafting and adopting a policy on Internet access for people with disabilities and amending the *Act to secure the handicapped in the exercise of their rights* accordingly.

5.26 We recommend adopting a policy on the rules for lightening texts on departments' Web sites.

5.27 We recommend that the *Cadre de diffusion de l'information gouvernementale sur Internet* be enhanced to include full instructions on accessibility standards and techniques, and that measures be taken to ensure it is systematically applied by government Webmasters.

Figure 14: How Can Access to Government Services Be Simplified?



3. Informing the Public and Raising Awareness about New Ways of Interacting with the State

The success of the e-government project rests primarily on meeting citizens' needs. The government must ensure citizens support the project by making the services known to them and convincing them of the benefits of using ICTs in their dealings with the government (see Figure 15, page 152). To implement such a strategy, the government must mount a large-scale communication campaign. The government's partners must be directly involved in this awareness-raising campaign.

Once the main projects are in place (one-stop government portal, "My Gov. Info." citizen's page and e-democracy initiatives), it would be useful to launch a major publicity tour throughout every region of Québec. A detailed publicity plan should be drawn up and implemented to target all necessary clientele and identify ways to showcase the benefits related to e-government.

Making E-Services Known to Citizens

A publicity plan will have to be drawn up to ensure that the e-government project and its main applications are known and understood by all Quebecers. Citizens and businesses must consider the possibilities offered by new technologies and develop a reflex to use them, without which the project risks being little more than an initiative with technological spin-offs.

The new information and communication technologies have many advantages and could be used to benefit citizens in the awareness-raising effort for the e-government project. For example, if a cost-benefit analysis is favourable, every Québec household could be given an interactive CD-ROM to guide them through their first experience with transactional e-services. This CD-ROM could be provided through the government's multi-service centres. Citizens could also be offered e-training.

RECOMMENDATIONS

5.28 We recommend mounting a vast communication campaign throughout every region of Québec, including an awareness-raising tour in the regions.

5.29 We recommend using tools stemming from new technologies to guide citizens through their initial transactions on e-government sites.

3.1 Promoting Quebecers' Adoption of New Technology by Making the Internet a Source of Value-Added Information

The Internet cannot and must not be viewed solely as a network linking millions of users to each other. The "wiring" is clearly important, but the content even more so. Quebecers must develop the reflex of making the Internet their first reference tool, whether for a government service or to find information on a broad range of subjects. Not until this reflex is well established will the possibilities offered by e-government be used to their full potential. For its part, the government must not only encourage citizens to use the Internet to look for information, but also facilitate the posting of content that is useful to Quebecers.

Initiatives to Post Content on the Internet

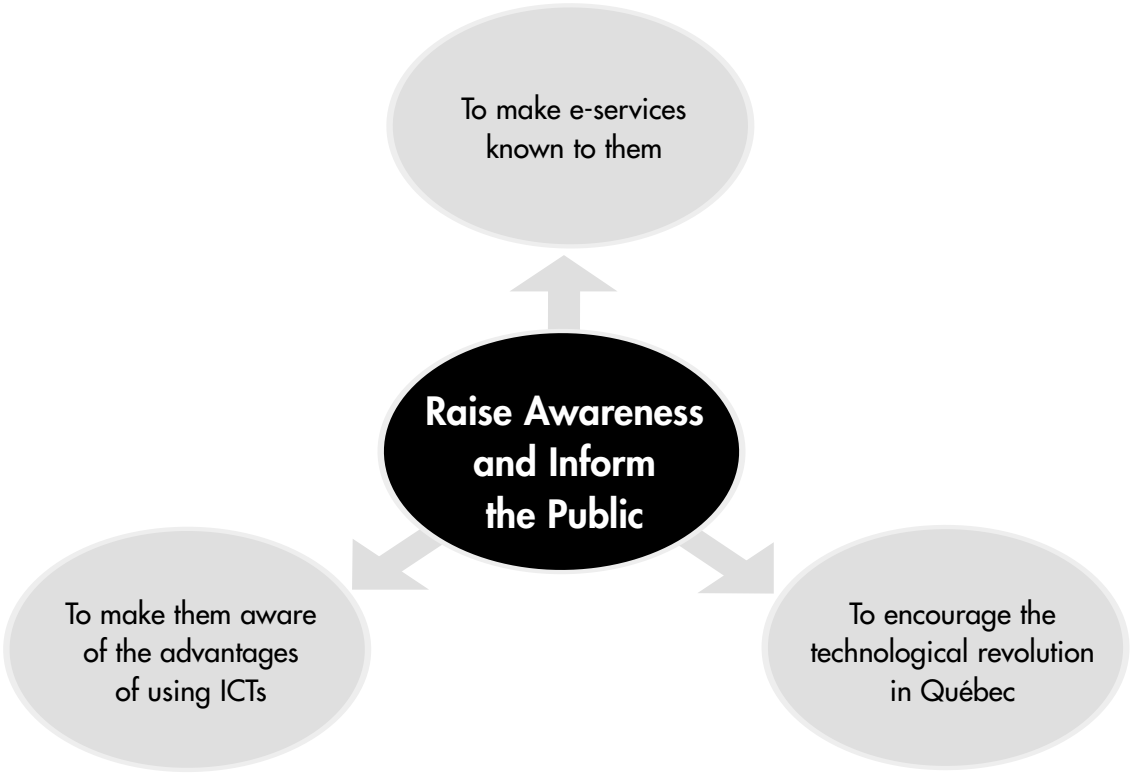
Several Québec initiatives that aim to post content on-line are worth a mention. These include *L'Encyclopédie de l'Agora* (www.agora.qc.ca), "the first virtual, dynamic and interactive encyclopedia in French." This encyclopedia, which enables users to search over 6,000 documents, is also the first to be entirely designed for the Internet. Anyone can submit a text to the encyclopedia to add to its content: "Each new component added to the original core of the work is the subject of a personal judgment that respects the principles set out in the *Charte de L'Encyclopédie*." The site offers original texts, while providing links to other Internet sites related to the subject. In this way, entire collections of books can be downloaded to your screen! "This year, 6,000,000 people, including 1,200,000 French-speaking Canadians and 4,500,000 Europeans consulted the encyclopedia and its documents, divided into 12 categories. Visits will continue to double every year. An old dream has come to fruition: The dissemination of Québec thought throughout the French-speaking world using modern technology. For example, 48,500 people have read the musings of political columnist Marc Chevrier in the past 24 months, something unthinkable using a paper medium."

The Platform for Community Networks (www.globalcn.org) is a space intended to create dialogue, debate and cooperation among members of the networks, organizations, institutions and individuals involved in the use of ICTs for community purposes and for the promotion and protection of rights and freedoms. The trilingual collaborative portal (French, English, Spanish) presents texts on subjects as varied as Internet rights, free software, the information society and the concrete application of ICT projects conducted by specialists in the private sector, while promoting cultural plurality and diversity. A list of agencies, as well as links to external resources, completes the information offered on this portal.

RECOMMENDATION

5.30 We recommend that the government equip itself with the means for promoting the emergence of Québec-content services on the Internet.

Figure 15: Why Inform the Public and Raise Awareness?



4. Commitment of the Public Service and Networks

The implementation of true e-government requires not only a change in the way services are presented to citizens (known as front-line services), but also a transformation in the actual delivery of services (known as back-office services). This transformation implies a review of the way things are done and, therefore, a reassessment of the work of public servants, both within the departments and agencies and in the institutions in the public and para-public networks. In fact, the automation of many features will render some clerical tasks obsolete. The implementation of e-government creates a unique opportunity to enhance the roles of many public servants by increasing their degree of independence and introducing new elements into their tasks that require knowledge and skill. This is fundamental to the delivery of horizontal e-services (see Figure 16, page 155).

Notes

Enhancing the Role of Public Servants

The implementation of multiservice centres (i.e., counter services and call centres) will require public servants to accept a decompartmentalization of their work, since it will include handling requests for services from several departments and agencies. For example, a public servant employed in customer service at MRCI must also, in this new situation, be able to answer citizens' requests related to employment, obtaining permits, income, etc. In this way, public servants will become resource persons capable of handling all of the needs of citizens and businesses.

Similarly, someone employed in a telephone support position could see his role change to one of a trainer, for example, to help citizens in their initial use of on-line services, whether this learning is done by telephone or in person via counter services.

In all cases, it will be essential that public servants play an active part in the transformation of their role. Individually, they must also have the opportunity to choose in which direction they wish to move.

Accordingly, public servants must view the transformation of services stemming from the implementation of e-government as an opportunity rather than an imposition. However, experience has repeatedly shown that change generally creates fear and reticence in the individuals affected. For this reason, the implementation of e-government must be done by involving the public servants in the resulting changes.

In 2001, the *Secrétariat du Conseil du Trésor* developed a *Modèle d'accompagnement des changements technologiques pour la fonction publique québécoise*. Those responsible for implementing the e-government project should follow the example set by this model and adapt it to the specific context of the current project.

Notes

The Modèle d'accompagnement des changements technologiques pour la fonction publique québécoise

The goal of the model is to "define elements in the environment specific to Québec's public service that play a role in the technological change processes; determine the strengths and weaknesses that are typical of technological change in the public service; understand the dynamics and the influence of the relationship that occurs in this process between the various stakeholders; determine efficiency indicators for this change process; determine, by standardizing with other public administrations, the best practices for managing technological change."

(*Source: Fiche synthèse de projet du centre d'expertise en gestion des ressources humaines,* www.tresor.gouv.qc.ca/resource/acrobat/projets/develop.pdf)

- ***Training***

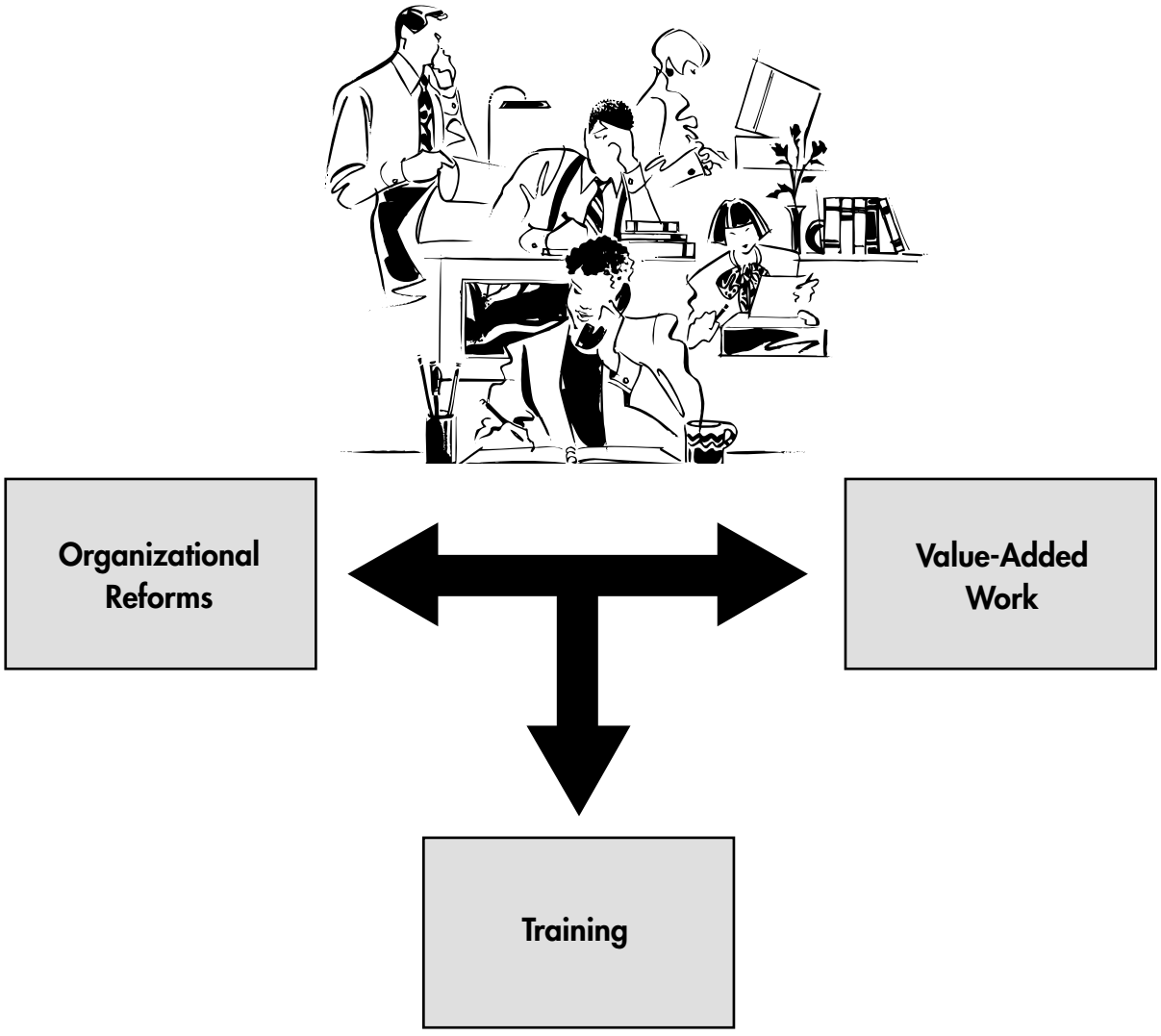
The implementation of e-government will inevitably create training needs for members of the public service. Public servants will see their tasks transformed, due, among others, to the decompartmentalization of their positions. Placing services on-line will require public servants to use new technological tools in their work. Special training sessions will be necessary to teach public servants how to use these tools.

Lastly, the new situation resulting from placing services on-line will have a major impact on the work of public servants with respect to the protection of personal information and the right to privacy, and the security of information and computer systems, among others. The delivery of e-services implies that some public servants will have access to databases containing personal information. For this reason, it is necessary to raise public servants' awareness and adapt the relevant codes of ethics accordingly to better define their rights to access information systems. This is particularly applicable for front-line public servants who deal directly with citizens. A classification of personal information determining different access rights based on hierarchical levels must also be planned. Such action will make it possible to "avoid the risks of unjustified use, deletion or loss of personal information."[73]

[73] *Centre de recherche en droit public. Les modifications à apporter aux cadres administratifs et juridiques afin de favoriser le développement de l'administration électronique dans le respect de la vie privée,* Faculty of Law, *Université de Montréal,* prepared for the *Secrétariat du Conseil du Trésor,* December 18, 2003, p. 60.

To provide this training, the government plans to use the possibilities offered by the introduction of new technologies, such as e-learning tools. Today, these innovative programs make it possible to ease the constraints generally related to traditional training, while reducing the resources necessary to implement them.

Figure 16: Support of the Public Service and Other Network Players



The Benefits of E-Learning

E-learning presents many benefits, specifically in terms of training personnel:

- Instantaneous training updates (since the content is hosted on the Internet). To this end, the Québec government intends to remain open to emerging possibilities based on ICTs. For example, the use of a hybrid CD-ROM, on which a part of the training content is recorded, the rest being downloaded from the Internet in a way that is totally transparent to the user, is one promising solution for the future in terms of updating content;
- Time, date and location of the training determined by the user (in fact, the training can be done at home provided the employee has access to the Internet. Standard browser software is sufficient for running e-learning applications);
- Integration of new learning approaches (e.g., immediate assessment of knowledge acquired, non-linear process or adaptation of the training to the user's current knowledge);
- Lower costs related to trainers. Substantial economies of scale can be generated;
- Uniformity of the message (cannot be distorted by trainers);
- Complementary Web applications enable users to discuss their training and knowledge acquired through discussion forums, for example.

RECOMMENDATIONS

5.31 We recommend involving public servants in the transformations stemming from the implementation of e-government.

5.32 We recommend that the *Conseil du trésor* adapt the *Modèle d'accompagnement des changements technologiques pour la fonction publique québécoise* to incorporate the realities specific to e-government.

5.33 We recommend that training programs which can use modern technologies be set up to enable public servants involved to adapt to changes related to placing services on-line and to the creation of multiservice centres.