Technology and Privacy, in a Time of Societal Choices
5th Quinquennial Report of the Commission d'accès à l'information du Québec
Summary

Message from the Chair

In 2002, at the time of the Commission's last quinquennial report, *Facebook, YouTube, Twitter, Google Street View* and *WikiLeaks* did not yet exist! The time elapsed since then means that our thoughts on the current legislation must take into account the reality of a new dimension that is constantly changing with information technology.

Thus, several categories of personal information may be circulated more rapidly and on a wider scale than ever before in the course of an individual's activities. At the same time, both the public sector and the private sector continue to seek such information avidly. The expanding capacity of computers allows this data to be coupled, grouped, interlinked and stored in an unlimited fashion in order to generate behavioral analyses, credit records, consumer habits, Web consultation histories, and so on.

For this reason, the Commission pays special attention to the protection of privacy in the present report. In the digital age, it is becoming increasingly urgent to establish protective measures that take into account the threats to privacy that result from information technology.

We must face this reality, because technologies will continue to develop and to be refined. The information provided to the users concerning disclosure of the personal information and the consequences that may result from it must be simple and transparent.

The Commission is concerned by what seems to be a certain heedlessness in this regard. When obtaining goods or services, the Commission is concerned by the undecipherable nature of adhesion or consent forms that are used when collecting and using personal information, if at all. In a similar vein, there is need for simplifying confidentiality policies posted by public bodies and businesses. Furthermore, if information is lost or hacked, what should we make of the fact that our existing legislation does not provide for any obligation to inform the authorities and the persons concerned? In the digital age, protection of personal information needs a major update.

In a society where information is increasingly valued, individuals are seeking easy access to information, according to their own self-determined needs. Government information, for which the State is the repository, cannot escape from this evolution. The right to know, the right to be informed and the necessary transparency of government authorities are the prerequisite foundations to modern democratic life.

Each recommendation contained in this report is consistent with the continuity of the Commission's action for nearly 30 years. While access to government information

spearheaded the adoption of the *Access Act*, it is now important to substantially increase the quantity of publicly accessible information and to facilitate access to this information, while respecting the rights of each individual.

Also, the Commission proposes to adapt the access to information scheme to the current reality by opening all government data to consultation and use, with some exceptions. Without having to govern in a glass house, the State must respond to the public's concerns by increasing transparency and by simplifying access to information.

Other recommendations contribute to strengthen the access to information scheme, particularly in bringing within the scope of the *Access Act* certain bodies presently excluded from it and requiring a public body to respect the time frame within which it may provide reasons for denial to access, thus facilitating a person's course of action in a process that must be kept simple and timely to produce its effects.

Similarly, while protection of personal information was the cornerstone of the *Private Sector Protection Act*, it is essential to ensure that rights made available to individuals can be exercised adequately and that businesses are represented by an official spokesperson.

Finally, the significant advances in information technology gives causes for concern and leads the Commission to solicit the government on the necessary means it should have at its disposal in order to adequately perform its mandate of promoting and protecting our fellow citizens' personal information. The constitution of mega databases, identity theft, heedless Internet use, and profiling of individuals, including children, must not be considered as progress gone beyond our control. Sooner or later these issues must be addressed.

To conclude on a more personal note, I must mention that my arrival as Chair of the Commission allowed me to take the measure of the unwavering commitment of my predecessor, M^{e} Jacques Saint-Laurent, who initiated the preparation of this report. We are following the trails he blazed and his contribution deserves our recognition.

Since my appointment to the Commission in 2006, I had the opportunity to develop privileged relationships with the institution's staff. Over the past few months, I also had the opportunity to appreciate their competence and their remarkable dedication. All of them combined their efforts and expertise to produce this report. On behalf of all my fellow commissioners, I wish to thank them and express my appreciation.

JEAN CHARTIER

Technology and Privacy, at a Time of Societal Choices is the fifth Quinquennial Report of the Commission d'accès à l'information du Québec ("the Commission"). This report meets the requirements of the *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*[1] and the *Act Respecting the Protection of Personal Information in the Private Sector*[2], since it contains findings regarding the application of these two Acts and proposes recommendations.

The first part of this report concerns **protection of personal information.**

The Commission considers that it is necessary, in the digital age, to simplify information that precedes the expression of consent by persons concerned and by the same token simplifies the expression of their consent. The action of checking a box stating "I have read and I accept" or "I certify that I have read" means that the persons concerned have read and understood the conditions of use or the confidentiality policy associated with a website or a social network. Many users check such a box without consulting the information and thus do not always know what they are consenting to. The Commission considers that actions must be taken so that public bodies and businesses adopt different mechanisms likely to meet these objectives. For this purpose, it recommends the adoption of simplified confidentiality policies. Thus, instead of publishing such a policy in linear form, public bodies and businesses must offer a condensed policy presenting, in a few paragraphs, their undertakings regarding the protection of personal information and from which it is possible to access a detailed policy containing more information on these undertakings. This approach allows presentation of the confidentiality policies in a format adapted to the medium. In effect, a document is not read in the same way if it exists on paper or in an electronic format. Moreover, because the reader's attention span is not the same when reading electronic documents, it is important to present texts that require little or no scrolling. It also recommends using protection pictograms and better information for individuals using technology likely to locate and to identify them (video surveillance, biometry, geolocation and radiofrequency identification, for example).

This oversight of the information provided to the individuals concerned, in order to ensure that consent is expressed freely and in an informed manner, must benefit everyone, both adults and youths.

Youths – digital natives – resort to blogs, *Twitter*, *MySpace* or *Facebook* to communicate with their friends here and abroad, publish photos and videos, and to find out where their friends are. They surf the Internet for their homework, for entertainment by playing games online, to download music or to purchase goods and services. They thus disclose a certain amount of information that allows them to be identified and tracked. Certainly, they communicate this information voluntarily. But do they know how their personal information will be used by the people in charge of commercial websites or social networks? Have they consented to the use of their data for sales or profiling? Do they know in what country their information is stored and who will have access to it? In short, are they aware of the possible incidents and harm caused by the disclosure of their personal information, not only today but in the future? As soon as information is published online, it becomes permanent.

This finding does not only concern digital natives. However, several stakeholders, including the Commission, are concerned about their increasingly numerous presence and their IT and Web 2.0 behaviour regarding their personal information. The Commission

1 R.S.Q., c. A.2-1, hereinafter "Access Act"
2 R.S.Q., c. P.39-1, hereinafter "Private Sector Protection Act"

recommends several avenues to address this issue. One concerns awareness and education for digital natives. A second pertains to the involvement of businesses to address this problem. Nonetheless, to ensure that these recommendations do not fall on deaf ears, they must be accompanied by collective consciousness raising. Protecting the personal information of youths is everyone's business.

Our vigilance must not only concentrate on what is disclosed regarding the electronic environments, but must also apply to the security of personal information. Public bodies and businesses must adopt organizational, human and technical security measures adapted to the context. However, as news reports frequently remind us, "zero risk" does not exist in security matters. Public bodies and businesses are not protected from incidents that may lead, for example, to forgetting documents containing personal information in a public place, sending business correspondence to the wrong destination, insecure storage of material containing personal information by a repository mandated to destroy it, or loss and theft of these documents.

Such a security breach represents a failure in the implementation and application of security measures. It can lead to a loss of personal information or to unauthorized access, use or disclosure. It is not always associated with information technology and may result from a simple error or human negligence.

A security breach thus is a phenomenon with multiple causes calling for various means of prevention. One of the means is to analyze the risks, accounting for the media and the sensitivity of the data. Another means is to inform the personnel of a public body or a business about the protective measures adopted and the risks resulting from non-compliance. Regularly testing the security measures in place and, if applicable, proceeding with the necessary adjustments also allows public bodies and businesses to maintain effective and efficient security measures.

In order to consolidate the obligation to adopt and maintain effective and efficient security measures throughout the life cycle of personal information, the Commission recommends that this be accompanied by mandatory security breach reporting to it and, in some cases, to inform the persons concerned.

With respect to public bodies or companies, the Commission's duties include overseeing the application of the law and ensuring compliance with protection of personal information. Mandatory security breach reporting is congruent with the Commission's overall duties. Mandatory reporting would allow the Commission to promptly counsel and guide public bodies and businesses in choosing the measures to be taken when there is a security breach and provide for follow-up. This would also allow the Commission to respond adequately to media requests and eventual complaints that may be brought by the public and to develop documents describing ways to deal with situations where there has been a security breach. Mandatory security breach reporting would serve to strengthen public confidence in the public bodies and businesses that hold their personal information and would allow the Commission to better play its oversight role.

The Commission, in its oversight role, must be able to communicate with a person designated as being responsible for the protection of personal information. In the public sector, the notion of person in charge of access to documents and protection of personal information was introduced in the legislation 29 years ago and has proved its usefulness ever since. However, no such provision exists in the private sector. While a business is currently responsible for the personal information held in its possession or custody, nothing obliges it to designate a person to assume this responsibility.

We cannot overestimate the advantages related to designating such a person, not only to

answer to the public and to the Commission, but also to promote protection of personal information within business operating in the private sector. The Commission therefore recommends that for each business operating in the private sector a person in charge of personal information access and protection be designated. While the means to ensure compliance with the Act may vary depending on the size of the organization, its structure, and the quantity and sensitivity of the personal information processed by a business, the legislator may take this into account and subject only certain businesses having more than a determinate number of employees.

Nonetheless, the proposed alignment of the private sector with the public sector is required in order to ensure respect for individual rights and strengthen the application of the *Private Sector Protection Act*. Equally, personal information being especially coveted in the digital age, the proposed alignment is considered essential in order to promote awareness and accountability with regards to its protection.

After emphasizing the importance of protection of personal information, the Commission, in the second part of this report, addresses certain problems encountered in **access to documents held by public bodies**. This is the case for the delay to provide justification for refusal of a request for access, representation by counsel before the Commission, subjecting certain entities whose joint stock is in the public domain to the *Access Act*, and the inquiry powers and immunity of members of the Commission's Adjudicative Division. This is also the case with the necessary transition from transparency to open government.

For this purpose, the Commission recommends that the *Regulation respecting the distribution of information and the protection of personal information*[3] be extended to include public bodies that are presently exempted from it. The Commission acknowledges that this measure is not an end in itself and that it is only a first step towards a concept of open government. Nonetheless, the coming into force of this regulation allowed the transition from reactive disclosure on request to proactive distribution of certain documents and information. Yet, citizens are demanding new ways to participate more actively in democratic life and influence public policies. The different communication platforms allow this expectation to be met and are resulting in a gradual paradigm shift. The Commission thus encourages the government to be part of this open approach, inspired by an Internet culture that promotes transparency through the release of public data and citizen participation.

3 R.S.Q., c. A-2.1, r. 0.2.

Recommendations

Protection of personal information in the digital age

Recommendation 1: The Commission recommends that the legislator oblige public bodies and businesses to adopt simplified confidentiality policies presenting, in clear and comprehensible terms, an overview of their undertakings for the protection of personal information.

Recommendation 2: The Commission recommends that the legislator impose on public bodies and businesses the use of protection pictograms informing individuals of their undertakings for protection of personal information.

Recommendation 3: The Commission recommends that the legislator oblige public bodies and businesses to report the presence of mechanisms likely to identify or locate a natural person during use of their products.

Recommendation 4: The Commission reminds public bodies and businesses to integrate the principles of protection of personal information when they design their goods and services and to apply them throughout the life cycle of this information.

Digital natives

Recommendation 5: The Commission recommends that the school system develop curricula at the elementary and secondary level to educate youth about IT and Web 2.0 issues.

Recommendation 6: The Commission invites the legislator to consider the appropriateness of amending consumer protection or personal information legislation, particularly to prohibit profiling of minors in electronic environments.

Reporting of security breaches

Recommendation 7: The Commission recommends that the *Access Act* and the *Private Sector Protection Act* be amended by the addition of an obligation to report to the Commission on security breaches that occur in public bodies and businesses and that involve personal information.

Recommendation 8: The Commission recommends that the terms and conditions be determined, leading to reporting of security breaches involving personal information.

Recommendation 9: The Commission recommends that it be entrusted with the power to order public bodies and businesses, on the conditions it determines, to notify the persons concerned by a security breach involving their personal information and to take the measures the Commission will deem necessary to ensure adequate protection of their

personal information.

The provision for a person in charge in the private sector

Recommendation 10: The Commission recommends that the *Private Sector Protection Act* provide for the creation of the function of person in charge of protection of personal information.

Recommendation 11: The Commission recommends that the function of person in charge in the private sector can be delegated by the business to a person working within the business.

The transition from transparency to open government

Recommendation 12: The Commission recommends that the application of the *Distribution Regulation* be extended to the public bodies currently exempted.

Recommendation 13: The Commission recommends that public bodies be subject to an enhanced regime of openness to government data, which allows free access to all government information useful to the public.

Recommendation 14: The Commission recommends that a public debate involving all partners (parliamentarians, individuals, associations, experts) be held to establish a model for an open Québec government, based on participation and collaboration.

The time limit to justify a refusal of access to information

Recommendation 15: The Commission recommends that the *Access Act* be amended to specify that the time limit provided for in section 47 to respond to a request for access and justify a refusal to access on the basis of an optional restriction become mandatory and results in forfeiture.

Recommendation 16: The Commission recommends that a public body cannot be relieved from the consequences of the failure to invoke a reason for optional refusal within the mandatory time limit provided to respond to request of access except in exceptional circumstances, which it would have the burden of proving to the Commission.

Recommendation 17: The Commission recommends that the *Private Sector Protection Act* be amended to specify that the time limit stipulated in section 32 to respond to a request for access and justify a refusal on the basis of an optional restriction of access is mandatory and involves forfeiture.

Recommendation 18: The Commission recommends that a business cannot be relieved from the consequences of the failure to invoke a reason for optional refusal within the mandatory time limit provided to respond to request of access except in exceptional

circumstances, which it would have the burden of proving to the Commission.

Representation by counsel before the Commission

Recommendations 19: In such a situation and subject to the decisions that may be rendered by the Court of Québec, the Commission suggests a reflection be initiated together with the partners involved in order to analyze the relevance and necessity of making the requirements of the *Act Respecting the Barreau du Québec* more flexible regarding applications for review and examination of a disagreement that are presented to it by legal persons.

Bodies with joint stock that is part of the public domain

Recommendations 20: The Commission recommends that the *Access Act* be amended to bring within the scope of the *Access Act*, all bodies having more than 50% of their joint stock held by the State.

Inquiry powers and immunity of members of the Commission's Adjudication Division

Recommendation 21: The Commission recommends that the *Access Act* and, by concordance, the *Private Sector Protection Act* be amended to grant all its members explicitly the powers and immunities of commissioners appointed under the *Act respecting public inquiry commissions.*