Important Recommendations from the Québec Privacy Commissioner on the Protection of Personal Information

November 04, 2016

On October 3, 2016, the Commission d'accès à l'information (CAI) released its 2016 quinquennial report, entitled "Rétablir l'équilibre" (Restoring the Balance), concerning the application of the *Act respecting documents held by public bodies and the protection* of personal information and the *Act respecting the protection of personal information in the private sector*(the "Private Sector Act"). Among the 67 recommendations made to the Government of Québec in the report, our attention has been drawn in particular to 10 proposals which could have a significant impact on private sector organizations carrying on activities in Québec.

The Obligation of Accountability of Enterprises and the Establishment of the Position of Person in Charge of Access and the Protection of Personal Information

Repeating a recommendation contained in its 2011 quinquennial report, the CAI is once again recommending that the Private Sector Act be amended, in order to impose an obligation of accountability on business enterprises. This obligation would be combined with the establishment, in the private sector, of the position of person in charge of access to, and the protection of, personal information, and the public disclosure of the names of such persons. It is noteworthy that certain Canadian statutes governing the protection of personal information, notably the *Personal Information Protection and* Electronic Documents Act ("PIPEDA"), already include the principle of organizational accountability and the designation of individuals responsible for access to, and the protection of, personal information.

From the Concept of a "File" to the Purpose of the Collection

Given the collection and ever-increasing use of images captured by surveillance cameras and megadata which are kept and used by businesses, present-day obligations of business organizations with respect to the creation and holding of files no longer appear well adapted to these new realities. In fact, although they are required to do so, many businesses do not necessarily keep the personal information about individuals that they retain in files identified by the names of the persons concerned. That being the case, the CAI is proposing that the concept of "file" be removed from the

Private Sector Act and that the obligations of business organizations be framed instead in relation to the purposes for which the personal information in question is collected. Such a change would, in particular, be intended to limit the use of personal information to the uses that prompted its collection, as well as to prevent the "generalized reuse" of such information for purposes unrelated to the initial reason for which it was collected from the individuals in question. Concretely, section 8 of the Private Sector Act would be amended to specify the time at which the information must be provided to the person concerned (depending upon whether the information is collected from the person, with or without his or her knowledge, or from a third party). The amendment would also require the person in question to be informed as to what personal information is to be collected, and by what means, and to ensure that all such information is clear, understandable and accessible, regardless of the support used for its collection.

Excluding Employee Information from the Definition of "Personal Information"

At present, the Private Sector Act does not provide any exception for employee-related information, contrary to PIPEDA and the corresponding private sector enactments (hereinafter the "PIPA statutes") in Alberta and British Columbia. The CAI recommends amending the Private Sector Act, so as to provide that information relating to the performance of an employee's duties in a business organization does not constitute "personal information". Since such information is not excluded from the definition of "personal information", certain decisions have concluded that it is of a confidential nature, without regard to the context of its use and the reasonable expectations of privacy of the employees concerned. Hence the CAI proposes to exclude certain information relating to employees and the performance of their duties in a business operation, for example, their names, titles, duties, (mailing and email) addresses, or their telephone or fax numbers in the workplace.

In our opinion, these recommendations could have gone further, so as to provide that employers need not obtain the consent of their employees with respect to information that is reasonably necessary to their management, as is the case under the PIPA statutes of British Columbia and Alberta, as well as under the recent amendments to the federal PIPEDA,1as long as these employees are properly informed of such practices.

The concept of "Manifest Consent"

Under section 14 of the Private Sector Act, "Consent to the collection, communication or use of personal information must be manifest, free, and enlightened, and must be given for specific purposes (…)". There was always a kind of uncertainty as to whether the concept of "manifest" consent was to be construed as being an explicit ("opt-in" type) of consent. That would imply that, unlike PIPEDA or the PIPAs of Alberta and British Columbia, which include a concept of implied consent, more particularly in certain situations involving non-sensitive information, the Private Sector Act would afford no flexibility as to the form of consent. The CAI, in its report, explains that "manifest consent" means that there must remain no doubt as to the intention underlying what it expresses, regardless of the means used to express it. Interestingly, the CAI explains that consent may therefore be either explicit or implicit. Although a number of business organizations were necessarily employing a concept of implicit consent in Québec, this clarification by the CAI is helpful, since it removes any uncertainty in this regard and confirms the legality of the current practice, adopted by many business organizations, of using implicit consent in certain situations involving non-sensitive information.

Consent and Sensitive Information

For the CAI, harmful consequences are likely to result from the disclosure or the use of some sensitive information, such as racial or ethnic origin, information about health or sexuality and financial information provided for income tax purposes. Likewise, information of another nature could also become sensitive, to the extent to which it is used to target one group of vulnerable individuals, for example, children or young people, or if it is likely to foster discrimination or to stigmatize one particular group of persons. Accordingly, the CAI recommends amending the Private Sector Act so as to provide that the communication of sensitive information or its use for purposes other than those for which it was collected is only possible with the express consent of the person concerned or as authorized by law. That requirement is already found in other enactments. Finally, the CAI further recommends closer supervision of the collection and use of personal information relating to children or young people.

Withdrawal of Consent, At Any Time

Along the same lines, the CAI recommends that the Private Sector Act be amended so as to permit consent to be withdrawn at any time, subject to any restrictions provided for by law. The present wording of the Private Sector Act provides that: "Such consent is valid only for the length of time needed to achieve the purposes for which it was requested". Contrary to a number of Canadian and foreign statutes governing the protection of personal information in the private sector, the Private Sector Act contains no provision expressly stating that the person concerned may withdraw his or her consent before the expiry of the time for which it was granted.

Genetic, Insurance and Employment Information

Given certain concerns relating to the possibility that individuals may be requested to communicate results of their genetic tests for non-medical purposes, for example, to apply for insurance or to make a job application, CAI is also proposing to prohibit the collection, use and communication of personal information for any purposes other than medical, scientific or legal ones. For the CAI, given the present state of knowledge, the health-related issues raised by the use of genetic tests for insurance purposes militate in favour of their prohibition. Similarly, the CAI is of the opinion that the prospect that genetic information will be used raises societal issues that are too important for employers to be allowed to obtain such information, even if they observe the legal parameters laid down by the Québec Charter of Human Rights and Freedoms. For that reason, the CAI is inviting the legislator to also prohibit the collection and use of genetic information in an employment-related context.

Biometric Information

In view of the ever more frequent recourse to biometric information, such as fingerprints, hand morphology, eye scans, and facial or voice recognition, the CAI raises various issues and advances several recommendations to protect such information. More particularly, the CAI is recommending referring, in the Private Sector Act, to the provisions addressing biometrics in the *Act to establish a legal framework for information technology*. That statute requires that organizations obtain the consent of the person concerned, minimizing the biometric characteristics or measurements recorded, refraining from recording such information unknown to the person concerned,

and respecting the purposes for which biometric characteristics or measurements were recorded, and their destruction where the reasons for which they were collected no longer exist. Furthermore, the CAI recommends adding an obligation requiring a declaration of the establishment of any databank of biometric characteristics or measurements to be made to the CAI 60 days before it is put into service.

In one recommendation which could have a significant impact on businesses, the CAI is also proposing to oblige businesses that contemplate implementing a procedure for recording biometric characteristics or measurements to carry out a prior assessment of the risks and impacts of doing so as regards privacy and the protection of personal information, before activating any such system, and to monitor it for as long as it is in use. Lastly, the CAI suggests establishing appropriate measures to govern the storage and conservation of biometric characteristics or measurements, in order to safeguard their confidentiality. More particularly, such measures (technology permitting) could take the form of compulsory and irreversible deletion of the names of those whose biometric characteristics or measurements are recorded immediately after they have been collected (the conversion of the image of the gross biometric data to a coded formula may be used for this purpose). Also recommended are: the mandatory destruction of the original gross characteristics or measurements once the anonymization process has been completed; the obligation to use an external, individual or portable support for the keeping of anonymized biometric characteristics or measurements, under the control of the person concerned; and the imposition of measures requiring the database to be local rather than centralized, whenever its creation is absolutely necessary.

Mandatory Reporting of Security-Related Incidents Affecting Personal Information

The CAI is also emphasizing the importance of including, in the Private Sector Act, a provision that would require organizations to manage security-related incidents affecting personal information in a transparent manner. More specifically, the CAI recommends modifying the Private Sector Act so as to add a requirement to report security-related incidents affecting personal information to the CAI, and specifying the terms and conditions of such declarations. As the CAI notes, such an obligation would permit the Private Sector Act to remain essentially similar to PIPEDA when the provisions of Bill S-4 concerning breaches of security safeguards, adopted by the Parliament of Canada, come into force in June 2015 (although the section mandatory breach notification is not yet in force). In addition, the CAI recommends amending the Private Sector Act so as to oblige businesses to notify the individuals concerned whenever a security-related incident affecting personal information occurs.

Finally, the CAI proposes that the Private Sector Act be amended so as to reinforce its powers to take action in cases of personal information security breaches and that it be granted the power to issue orders to protect the rights of the individuals concerned, applying criteria similar to those found in safeguarding orders, as well as a power to order anyone in possession of such information unlawfully to return or destroy it.

Transfers out of Québec

At the present time, the Private Sector Act obliges organizations to make sure that, when they transfer personal information outside Québec, the information receives the same protection as if it had remained in Québec. But absent any clearly defined monitoring criteria, it is difficult for organizations that are called upon to send personal

information to third parties outside Québec to assess the equivalency of protective legislation in the jurisdictions to which the third parties receiving the personal information are subject. In view of that observation, the CAI is recommending that the Private Sector Act be amended so as to require businesses to analyze the impacts and risks associated with the protection of personal information before any personal information is sent out of Québec. It would be desirable for the CAI to confirm that it is possible for an enterprise to transfer personal information at least within Canada (especially if the information is managed by the same organization, operating across the country), without having to take any additional protective measures.

The CAI further suggests amending the statute so as to require business organizations to enter into contracts with the public or private entities to which the personal information will be sent and entrusted and to prescribe in such agreements any measures required to mitigate the impacts and risks identified in the analysis. In practice, it would appear that the business organizations that transferred personal information outside of Canada were already interpreting section 17 of the Private Sector Act as requiring that business organizations enter into a contract stipulating that the business organization that receives personal information shall use adequate security measures.

Conclusion

Although these are merely recommendations, it is foreseeable that several of these proposals will be introduced and potentially adopted by the Québec Government. In fact, the CAI mentions a number of times in its report the importance of harmonizing the provisions applying to the public and private sectors. In the CAI's opinion, it is unjustifiable that a number of the provisions of the public sector legislation confer more protection on personal information than those governing the private sector. In addition, the matter of coordinating with Europe should take on greater and greater importance, especially in the wake of Advisory Opinion 7/2014 concerning the coordination of the Private Sector Act with the European Directive, issued by the Article 29 Data Protection Working Party, and with the upcoming entry into force of the new European Directive in May 2018. It is therefore likely that the Private Sector Act will be amended in the foreseeable future to respond to those concerns.

1 PIPEDA was amended to that end in recent amendments made by Bill S-4, which came into force in June 2015.

By

Raphaël Girard

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749