JUNE 2015

PRIVACY BULLETIN

Borden Ladner Gervais

NEW REQUIREMENTS OF THE *DIGITAL PRIVACY ACT* (BILL S-4)

Bill S-4, the *Digital Privacy Act*, the federal government's latest attempt to reform PIPEDA was proclaimed on June 18, 2015. This Bill is now in effect except for the breach notification regulations which have not yet been released and therefore, the breach notification section will come into effect at a later date.

The government has modernized and broadened the regulatory powers of the Executive Branch. This may result in more flexibility to pass clarifying regulations as issues arise under PIPEDA. Clause 24 of Bill S-4 modifies section 28 of PIPEDA to provide that every organization that knowingly contravenes the new sections of PIPEDA requiring organizations to record and report breaches of security safeguards or obstructs the Commissioner in the investigation of a complaint or in conducting an audit will now be liable for fines of up to $100,000 for indictable offences, or for fines of up to $10,000 for offences punishable on summary conviction.

The government is also granting the Commissioner additional powers to enter into enforceable compliance agreements with organizations. These compliance agreements may include any terms that the Commissioner considers necessary to ensure compliance with PIPEDA. If the organization does not fulfil the terms of the compliance agreement to the satisfaction of the Commissioner, the Commissioner may seek a mandatory order from the Federal Court to require compliance with the agreement. It is important to note that a compliance agreement does not provide immunity to the organization from an action by an individual for compensation or from prosecution for an offence.

The main changes of Bill S-4 can be summarized as follows:

BREACH NOTIFICATION REQUIREMENT

Bill S-4 introduces under new sections 10.1 through 10.3 an explicit obligation to notify individuals in cases of breaches, and report to the Office of the Privacy Commissioner of Canada (OPC), if it is "reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual". This allows for additional specificity via regulations (e.g. timing, form and manner, level of information, etc.) and the development of guidelines, as necessary. The definition of "significant harm" is an open-ended definition that includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property (new section 10.1(7)).

The factors for identifying whether there is a real risk of significant harm in Bill S-4 are "the sensitivity of the personal information involved in the breach" and "the probability that the personal information has been, is being or will be misused" as well as "any other prescribed factor" (new section 10.1(8)). The contents, form and timeline for issuing a notification are as follows:

- The notification must contain "sufficient information" to allow an individual to understand the significance of the breach and to take steps to mitigate or reduce any harm to him or herself that could result from it. Any other "prescribed information" that could be required under regulations in the future must also be included (new section 10.1(4)).
- The notification must be "conspicuous" and given directly to the individual, provided it is feasible to do so (new section 10.1(5)).

- The notification must be provided "as soon as feasible" after a breach has occurred. However, if a government institution requests that the organization delay notification for a criminal investigation relating to the breach, then the notification shall not be given until the organization is authorized to do so (new section 10.1(6)).

New section 10.2 also states that an organization that notifies an individual of a breach must also notify any other organization or government institution that can reduce the risk or mitigate the harm from the breach. An organization can also make limited disclosure of the personal information to such an organization or government institution without the individual's consent in order to reduce the risk or mitigate the harm resulting from the breach.

BREACH RECORD KEEPING REQUIREMENT

Bill S-4 introduces a new section (10.3) requiring organizations to keep and maintain records of every breach of security safeguards involving personal information under their control. These records must be provided to the Privacy Commissioner on request. The proposed amendments provide no details on record retention periods, the manner in which records must be designed and maintained, and the level of detail required in the report. Also, there is no threshold, so one may consider that all breaches (even trivial or inconsequential breaches) must be logged.

DISCLOSURE WITHOUT CONSENT

New PIPEDA sections 7(3)(*d.1*) and (*d.2*), proposed in clause 6(10) of Bill S-4, would permit an organization to disclose the personal information without the knowledge or consent of its customers to another organization (for example, from one business to another) in order to investigate a breach of an agreement or a contravention (or anticipated contravention) of a federal or provincial law where it is reasonable to expect that obtaining the consent from the individual for the disclosure would compromise the investigation (new section 7(3)(*d.1*)). This is connected to the removal of the concept of "investigative bodies" from PIPEDA (under the investigative body scheme, the Governor in Council could approve (by regulation) specific bodies or categories of bodies to which organizations could disclose personal information under defined circumstances).

Furthermore, a similar disclosure provision is provided for the purposes of detecting or suppressing fraud (new section 7(3)(*d.2*)). As well, new section 7(3)(*d.3*) allows disclosure without consent to a government institution or to the individual's next of kin or authorized representative if there are *reasonable* grounds to believe that the individual has been the victim of "financial abuse," and where it is reasonable to expect that obtaining the consent from the individual for the disclosure would compromise the ability to prevent or investigate the abuse.

DISCLOSURE OF INFORMATION IN A BUSINESS TRANSACTION

Clause 7 of Bill S-4 allows organizations to share personal information without an individual's consent for the purpose of engaging in a due diligence process for a "prospective business transaction" where such information is necessary to determine whether to proceed with the transaction or to complete it. The organization that receives the personal information must: (i) use and disclose it solely for purposes related to the transaction; (ii) protect it with appropriate security safeguards; and (iii) return the information or destroy it within a reasonable time if the transaction does not proceed (new section 7.2(1)). Once the business transaction is completed, new PIPEDA s. 7.2(2) would allow parties to the transaction to use and disclose personal information disclosed under s. 7.2(1) without the knowledge and consent of the individuals, if certain steps are followed.

Once a business transaction is completed, the organizations that have exchanged personal information may use and disclose it without the knowledge or consent of the individuals involved if the personal information is needed to carry on the business or activity that was the object of the transaction, under an agreement that it must be used and disclosed solely for the original reasons it was collected. That agreement must also provide appropriate security safeguards, and must stipulate that the organizations will honour any withdrawal of consent by the individuals involved. New PIPEDA section 7.2(2)(c) requires that the individual be notified of the transaction and the fact that their personal information was disclosed, similar to B.C.'s PIPA (section 20(3)(c)).

BUSINESS CONTACT INFORMATION

The government has introduced an exemption from the requirement for consent for the collection, use and disclosure of business contact information when used solely for the purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession. However, the government has tweaked the definition of business contact information as "any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment".

EMPLOYEE INFORMATION AND WORK PRODUCT INFORMATION EXCEPTIONS

Clause 7 also modifies the consent requirements for the collection, use and disclosure of the personal information of employees of federal works, undertakings and businesses. Employers will now be able to collect, use and disclose employee information without consent if it is needed to "establish, manage or terminate" employment, provided the employee in question has been notified why the information is being or may be collected, used or disclosed (new section 7.3). Exceptions for the collection, use and disclosure of work product information have also been introduced.

CHANGES TO CONSENT

Clause 5 of Bill S-4 includes a revised "valid consent" provision (PIPEDA, s. 6.1), by shifting from a subjective standard to a more objective standard. The current requirement to obtain consent in PIPEDA contained in s. 4.3.2 of Schedule 1, requires that organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.

New section 6.1 is clarifying that an individual's consent to the collection, use or disclosure of his or her personal information is valid only "if it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting."

Since this section aims to ensure that the privacy policies and notification practices of organizations covered by PIPEDA clearly and directly inform individuals about the ramifications of sharing personal information with these organizations, organizations should review their privacy notices or policies to ensure compliance with this requirement. As a matter of fact, this new section endeavours to make sure that privacy policies and practices do not try to force or mislead individuals into giving such information to the organizations.

AUTHOR

Éloïse Gratton
Montréal
514.954.3106
egratton@blg.com

PRIVACY AND DATA SECURITY GROUP

National Leaders

Éloïse Gratton	Montréal	514.954.3106	egratton@blg.com
Robert J.C. Deane	Vancouver	604.640.4250	rdeane@blg.com

Key Contacts

LuAnne Morrow	Calgary	403.232.9577	lmorrow@blg.com
Patricia Galella	Montréal	514.954.2514	pgalella@blg.com
Kirsten Crain	Ottawa	613.787.3741	kcrain@blg.com
Bonnie Freedman	Toronto	416.367.6239	bofreedman@blg.com
Bradley J. Freedman	Vancouver	604.640.4129	bfreedman@blg.com

Borden Ladner Gervais

This publication is not intended to constitute legal advice, a complete statement of the law, or an opinion on any subject. No one should act upon it or refrain from acting without a thorough examination of the law after the facts of a specific situation are considered. You are urged to consult your legal adviser if you have specific questions or concerns. BLG does not warrant, guarantee the accuracy, currency or completeness of this publication. No part of this publication may be reproduced without prior written permission of Borden Ladner Gervais LLP (BLG). If this publication was sent to you by BLG and you do not wish to receive further publications from BLG, you may ask to have your contact information removed from our mailing lists by phoning 1.877.BLG.LAW1 or by emailing unsubscribe@blg.com. BLG's privacy policy relative to publications may be found at www.blg.com/home/website-electronic-privacy.

© 2015 Borden Ladner Gervais LLP

BORDEN LADNER GERVAIS LLP
LAWYERS | PATENT & TRADEMARK AGENTS

Calgary
Centennial Place, East Tower
1900, 520 – 3rd Ave S W, Calgary, AB, Canada T2P 0R3
T 403.232.9500 | F 403.266.1395

Montréal
1000 De La Gauchetière St W, Suite 900, Montréal, QC H3B 5H4
T 514.879.1212 | F 514.954.1905

Ottawa
World Exchange Plaza, 100 Queen St, Suite 1300
Ottawa, ON, Canada K1P 1J9
T 613.237.5160 | F 613.230.8842 (Legal)
F 613.787.3558 (IP) | ipinfo@blg.com (IP)

Toronto
Scotia Plaza, 40 King St W, Toronto, ON, Canada M5H 3Y4
T 416.367.6000 | F 416.367.6749

Vancouver
1200 Waterfront Centre, 200 Burrard St, P.O. Box 48600
Vancouver, BC, Canada V7X 1T2
T 604.687.5744 | F 604.687.1415

blg.com

Borden Ladner Gervais LLP is an Ontario Limited Liability Partnership.