Privacy Update:

Digital Privacy Act* Amendments to the *Personal Information Protection and Electronic Documents Act

4th Annual Continuing Professional Development Event
November 12, 2015

Presented by:
Catherine Carscallen

GARDINER ROBERTS

Digital Privacy Act

- Bill S-4, the *Digital Privacy Act*, passed into law June 18, 2015
- Introduced a number of amendments to PIPEDA *most* of which came into force on June 18, 2015
- Data breach notification and reporting requirements not yet in force

2

Outline

Amendments to PIPEDA

- Enhanced consent requirement
- New exceptions to consent requirements
- Mandatory breach notification and record keeping requirements (*not yet in force*)
- Enforcement and penalties

3

Enhanced Consent Requirement

Valid consent:

- the consent of an individual is only valid 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

4

Exemption – Business Contact Information

- Definition of "**personal information**" amended: information about an identifiable individual
- New definition of "**business contact information**": any information that is used for the purpose of communicating or facilitating communicating with an individual in relation to their employment, business or profession such as the individual's name, position, name or title, work address, work telephone number, work fax number or work electronic address

5

Exemption – Business Contact Information

PIPEDA does not apply to an organization in respect of the **business contact information** of an individual that the organization collects, uses or discloses solely for the *purpose of communicating or facilitating communication with the individual in relation to their employment, business or profession*.

6

Business Transaction Exemption

- Allows organizations that are parties to a *prospective business transaction* or a *completed business transaction* to use and disclose personal information without the knowledge or consent of the individual if certain conditions are met.
- Exemptions do not apply if primary purpose, or result, of business transaction is the purchase, sale or other acquisition or disposition, or lease, of personal information.

7

Business Transaction Exemption

"**business transaction**" includes:

- purchase, sale or other acquisition or disposition of all or part of an organization or any of its assets;
- merger or amalgamation;
- making of a loan or provision of other financing;
- creating of a charge on, or taking of a security interest in or security on, assets or securities;
- lease or licensing of assets

8

Exemption – Prospective Business Transaction

Conditions:

(a) the organizations have entered into an agreement that requires the recipient: (i) to use and disclose the information solely for purposes related to the transaction, (ii) to protect the information by security safeguards appropriate to the sensitivity of the information, and (iii) if the transaction does not proceed, to return the information, or destroy it, within a reasonable time; and

9

Exemption – Prospective Business Transaction

(b) the personal information is necessary: (i) to determine whether to proceed with the transaction, and (ii) if the determination is made to proceed with the transaction, to complete it.

10

Exemption – Completed Business Transaction

Conditions:

(a) the organizations have entered into an agreement that requires each of them: (i) to use and disclose the personal information solely for the purposes for which the information was collected, permitted to be used or disclosed before the transaction was completed, (ii) to protect the information by security safeguards appropriate to the sensitivity of the information, and (iii) to give effect to any withdrawal of consent;

11

Exemption – Completed Business Transaction

(b) the personal information must be necessary for carrying on the business or activity that was the object of the transaction; and

(c) one of the parties must *notify* the individuals, within a reasonable time after the transaction is completed, that the transaction has been completed and that their personal information has been disclosed.

12

Other New Consent Exceptions

Consent is not required to collect, use or disclose personal information if it was:

- contained in a **witness statement** and collection, use or disclosure is necessary to assess, process or settle an insurance claim
- produced by the individual in course of employment, business or profession & collection, use or disclosure is consistent with purposes for which the information was produced (**work product information**)

13

Other New Consent Exceptions

Consent is not required to disclose personal information to a government institution that:

- has made a request for the information,
- identified its lawful authority to obtain the information;
- indicated that the disclosure is requested for the purpose of **communicating with next of kin** or authorized representative of an injured, ill or deceased individual

14

Other New Consent Exceptions

An organization may disclose personal information without consent to:

- a government institution if the organization has reasonable grounds to believe that the information relates to a contravention of laws of Canada, a province or foreign jurisdiction that has been, is being or is about to be committed

15

Other New Consent Exceptions

An organization may disclose personal information without consent to another organization to:

- **investigate** a breach of an agreement or a law that has been, is being or is about to be committed; or
- detect or suppress **fraud** or prevent fraud that is likely to be committed;

where reasonable to expect that obtaining consent would compromise investigation or ability to prevent, detect or suppress the fraud

16

Other New Consent Exceptions

An organization may disclose personal information without consent to the government or an individual's next of kin or authorized representative where:

- reasonable to believe that an individual has been, is or may be the victim of **financial abuse**;
- disclosure is made solely for purposes relating to preventing or investigating the abuse; and
- reasonable to expect that disclosure with consent would compromise ability to prevent or investigate the abuse

17

Other New Consent Exceptions

An organization may disclose personal information without consent if:

- necessary to **identify the individual who is injured, ill or deceased**;
- made to a government institution or individual's next of kin or authorized representative; and
- if the individual is alive, the organization informs the individual in writing without delay of the disclosure

18

Other New Consent Exceptions

Federally regulated organizations may collect, use and disclose personal information without the consent of the individual if:

- necessary to **establish, manage or terminate an employment relationship** with the individual; and
- the organization has *informed* the individual that the personal information will or may be collected, used or disclosed for those purposes

19

Mandatory Breach Notification

- Provisions will come into force at a future date once regulations are finalized
- New obligations with respect to **breaches of security safeguards**: the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards

20

Mandatory Breach Notification

- Organizations will be required to **report to the Privacy Commissioner** any breach of security safeguards involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual
- Report to be made "as soon as feasible" after organization determines that the breach has occurred

21

Mandatory Breach Notification

- Organizations will also be required to **notify individuals** (unless otherwise prohibited by law) of any breach of security safeguards involving the individual's personal information under the organization's control if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual
- Notification to be given as soon as feasible after organization determines that the breach has occurred

22

Mandatory Breach Notification

"**significant harm**" defined to include:

- bodily harm, humiliation, damage to reputation or relationships
- loss of employment, business or professional opportunities
- financial loss, identity theft, negative effects on credit record
- damage to or loss of property

23

Mandatory Breach Notification

Factors relevant to determining whether a breach of security standards creates a **real risk of significant harm** to the individual:

- sensitivity of the personal information involved
- probability that the personal information has been, is being or will be misused; and
- any other prescribed factor

24

Mandatory Breach Notification

- An organization that notifies an individual of a breach of security safeguards will also be required to **notify any other organization or government institution** of the breach if such other organization or government institution may be able to reduce the risk of harm that could result from it or mitigate that harm
- As soon as feasible after organization determines that breach occurred
- Consent not required for such disclosures

25

Mandatory Record Keeping

- Provisions will be brought into force at a future date
- Organizations will be required (in accordance with any prescribed requirements) to keep and maintain a record of **every breach** of security safeguards involving personal information under its control
- On request, must provide the Privacy Commissioner with access to, or a copy of, a record

26

Confidentiality; Public Interest

- Privacy Commissioner must keep confidential all information (including breach reports and breach records) that comes to his or her knowledge in the performance or exercise of his or her duties or powers, however, the Commissioner may, **if in the public interest to do so**, make public any such information

27

Enforcement and Penalties

Knowing violations of the breach notification or breach record keeping requirements may result in:

- offence punishable on summary conviction and a fine of up to $10,000
- indictable offence and fine up to $100,000

28

Enforcement and Penalties

Compliance agreement:

- agreement (enforceable in court) b/w Privacy Commissioner and an organization that the Commissioner reasonably believes has committed or is likely to commit a breach of PIPEDA
- aimed at ensuring compliance with PIPEDA
- once entered into, will prevent Privacy Commissioner from applying to Federal Court in respect of any matter covered in the agreement

29

Enforcement and Penalties

Compliance agreement:

- does not prevent an individual from applying to Federal Court for a hearing or the prosecution of an offence under PIPEDA

30