For Discussion

Data Breach Notification and Reporting Regulations

Innovation, Science and Economic Development Canada

March 2016

This page is intentionally blank

Table of Contents

Preface

On June 18, 2015, the *Digital Privacy Act* (also known as Bill S-4) received Royal Assent in Canada's Parliament. The *Digital Privacy Act* amended Canada's private sector privacy law, the *Personal Information Protection and Electronic Documents Act* (PIPEDA). In general, PIPEDA sets the rules for the collection, use and disclosure of personal information by organizations in the course of commercial activities. It establishes basic legal requirements that private-sector organizations must respect to ensure that Canadians trust that their privacy will be protected when their personal information is in the hands of businesses.

Among other important changes, the *Digital Privacy Act* amended PIPEDA to require private-sector organizations to notify Canadians in circumstances where their personal information has been lost or stolen, and they have been put at risk of harm as a result. In addition, organizations are required to report these potentially harmful data breaches to the Privacy Commissioner of Canada.

The new data breach requirements in PIPEDA will come into force once the Government passes regulations, which will provide greater clarity and specificity of the requirements of the Act. The purpose of this discussion paper is to solicit stakeholder input and views on these regulations. Comments received will be taken into consideration in the preparation of the draft regulations.

Interested stakeholders are encouraged to review the issues identified in this consultation paper and to provide written comments and responses to questions by no later than May 31, 2016. Submissions (Microsoft Word or Adobe PDF) may be sent electronically to: ic.ised.breach-atteinte.isde.ic@canada.ca; or in hard-copy format by mail to: Data Breach Consultations, Privacy and Data Protection Directorate, Innovation, Science and Economic Development Canada, 235 Queen Street, Ottawa, Ontario K1A 0H5.

Please note that, throughout this document, references are made to legislation and regulations in other jurisdictions that are current to December 17, 2015. As a result, any developments in these jurisdictions beyond this date are not reflected.

Innovation, Science and Economic Development Canada thanks all stakeholders for the valuable contribution they may have already provided to the development of PIPEDA's data breach requirements and for their continued input into this proposal.

Introduction

In general, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) sets the rules for the collection, use and disclosure of personal information by organizations covered by the Act in the course of commercial activities. It establishes basic legal requirements that private-sector organizations must respect so that Canadians trust that their privacy is protected when their personal information is in the hands of businesses.

PIPEDA is based on 10 internationally recognized principles set out in the Canadian Standards Association's *Model Code for the Protection of Personal Information*, a national standard that was developed in 1996 by consumer and business groups, privacy advocates and government representatives. As set out in Section 3, the purpose of the Act is to balance individual privacy rights with the legitimate needs of businesses to collect, use and disclose personal information for reasonable purposes. PIPEDA sets out a flexible, non-prescriptive approach to achieve this objective.

The Act provides for independent oversight and redress through the Office of the Privacy Commissioner of Canada and the Federal Court. The Privacy Commissioner may resolve privacy conflicts through the use of various dispute resolution mechanisms, while the court is empowered to order organizations to change their practices to comply with the law, and can also award damages to individuals who have suffered harm when their privacy has been violated in contravention of PIPEDA.

PIPEDA applies to federal works, undertakings and businesses across Canada, and to all organizations engaged in commercial activities, except those subject to substantially similar provincial legislation[1].

The *Digital Privacy Act*

On June 18, 2015, the *Digital Privacy Act* (also known as Bill S-4) received Royal Assent. The *Digital Privacy Act* made a number of important changes to PIPEDA to strengthen privacy protection, streamline rules for businesses and increase compliance. The Bill implemented the government's response to the first statutory review of PIPEDA, completed in 2007[2].

[1] Provincial Acts designated as substantially similar to PIPEDA: British Columbia's Personal Information Protection Act, Alberta's Personal Information Protection Act, Québec's An Act Respecting the Protection of Personal Information in the Private Sector, Ontario's Personal Health Information Protection Act, with respect to health information custodians, New Brunswick's Personal Health Information Privacy and Access Act, with respect to personal health information custodians, Newfoundland and Labrador's Personal Health Information Act, with respect to health information custodians

[2] Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics: Statutory Review of PIPEDA.

Among the changes made by the *Digital Privacy Act* is the establishment of mandatory data breach reporting requirements. These obligations are set out in Division 1.1 of the *Digital Privacy Act*. In summary, organizations that experience a data breach – referred to in the Act as "a breach of security safeguards" – must:

- determine if the breach poses a "real risk of significant harm" to any individual whose personal information was involved in the breach;
- notify individuals as soon as feasible of any breach that poses a "real risk of significant harm";
- report any data breach that poses a "real risk of significant harm" to the Privacy Commissioner, as soon as feasible;
- where appropriate, notify any third party that the organization experiencing the breach believes is in a position to mitigate the risk of harm; and
- maintain a record of the data breach and make these records available to the Privacy Commissioner upon request.

Data Breach Notification and Reporting Regulations

The Government has the authority to make regulations to provide greater clarity and specificity with respect to the Act's data breach reporting requirements. This includes the authority to set out the form and content of notifications and reports, additional factors to be considered in the determination of risk and details on record keeping requirements, as well as other elements.

What is a "Breach of Security Safeguards"?

The new data breach reporting requirements in PIPEDA apply to any "breach of security safeguards". As a result, a clear understanding of this term is required.

Subsection 2(1) of PIPEDA defines a "breach of security safeguards" as:

> *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*

The definition is intended to include two elements – the first being that personal information is lost, or accessed by an unauthorized individual (either through theft or wrongful disclosure), and second, that the loss or unauthorized access is the result of someone violating the organization's security safeguards (or is the result of the organization failing to establish such safeguards).

For example, the failure of an employee to password-protect a database containing customer personal information as required by an organization's security policy, which resulted in the database being accessed by contract employees not authorized to view it, would meet the definition of a data breach under PIPEDA. However, a failure to password-protect the database alone, without the data being accessed by an unauthorized individual, would not meet the definition of a "breach of security safeguards" in the Act.

The new data breach requirements will come into force once the Government passes final regulations. The purpose of this consultation is to solicit stakeholder input and views, which will be taken into consideration in the preparation of the draft regulations.

Following this consultation process, the Government will publish draft regulations in Part I of the *Canada Gazette* for public comment and consultation. Based on all the input received, final regulations will be published in Part 2 of the *Canada Gazette*, and PIPEDA's new data breach provisions will be brought into force.

Experience in Other Jurisdictions

A number of data protection authorities have established or proposed data breach reporting frameworks (both mandatory and voluntary). It is instructive for the Government of Canada to consider the specific requirements set out under these frameworks to both increase regulatory harmonization and decrease administrative burden on organizations, and to adopt what has proven to be best practice.

Office of the Privacy Commissioner: Voluntary Data Breach Reporting

Of particular relevance to organizations subject to PIPEDA is the existing voluntary data breach reporting program established by the Office of the Privacy Commissioner of Canada (OPC)[3]. This voluntary program has been in place since 2007, and many organizations subject to PIPEDA participate as a matter of best practice. The program will be updated once the mandatory provisions established by the *Digital Privacy Act* are brought into force.

Under the voluntary program, organizations are encouraged to report "material" data breaches to the OPC and to notify affected customers or employees where the breach poses a "risk of harm". Accompanying guidance material, such as *Key Steps for Organizations in Responding to Privacy Breaches*[4] provide suggestions and recommendations for best practices, such as evaluating the risk posed by a data breach, why and how to notify and what information should be included in a notification. As a result, the OPC's voluntary program provides a good foundation for the development of the data breach notification and reporting regulations.

Treasury Board Policy on Data Breach Reporting

In 2014 the Government implemented a new policy on mandatory breach reporting within the federal public sector. The amended Treasury Board of Canada *Directive on Privacy Practices* imposes a requirement for all federal government institutions to report certain breaches of personal information to both the Treasury Board Secretariat and the Office of the Privacy Commissioner, and to notify affected individuals.

The policy aligns with the obligations in the *Digital Privacy Act* in that they both employ a risk-based threshold for reporting, have a broad definition of harm and utilize a flexible timeframe for reporting.

[3] https://www.priv.gc.ca/resource/pb-avp/index_e.asp
[4] https://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.asp

Canadian Provinces

Alberta is currently the only province in Canada to have mandatory data breach reporting requirements for all private sector organizations. These requirements are set out under Alberta's *Personal Information Protection Act* (PIPA) [5]. Provincial health privacy laws in Ontario; New Brunswick; and Newfoundland and Labrador also contain reporting requirements for the healthcare sector[6].

United States

The majority of U.S. states have had legislative data breach reporting requirements for several years, and some are now beginning to update these requirements based on experience with the existing rules.

The U.S. has specific laws for the financial and health sectors that also contain breach reporting obligations specific to those sectors. These laws are the *Gramm-Leach-Bliley Act*,[7] which applies to the financial sector, the *Health Insurance Portability and Accountability Act*[8] and the *American Recovery and Reinvestment Act,*[9] which both apply to the handling of electronic health information.

At the Federal level, several bills have been put forward to set nationwide rules, though none have passed to date. The most recent, a proposal by the White House, is entitled the *U.S. Personal Data Notification and Protection Act*[10].

---

[5] Alberta's *Personal Information Protection Act* is available at http://www.qp.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779762507

[6] Ontario's *Personal Health Information Protection Act* is available at *http://www.ontario.ca/laws/statute/04p03* , New Brunswick's *Personal Health Information Privacy and Access Act* is available at http://laws.gnb.ca/en/showfulldoc/cs/P-7.05/20121030 , Newfoundland and Labrador's *Personal Health Information Act is available at http://assembly.nl.ca/Legislation/sr/statutes/p07-01.htm*

[7] See the Safeguards Rule of the *Gramm-Leach-Bliley Act at http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16*

[8] See the Breach Notification Rule of the *Health Insurance Portability and Accountability Act,* available at http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6

[9] See the Breach Notification Rule for Electronic Health Information of the *American Recovery and Reinvestment Act* at http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=6ae79a215bd299fd401a63594e98ce70&ty=HTML&h=L&n=16y1.0.1.3.42&r=PART

[10] The *U.S. Personal Data Notification and Protection Act* is available at *https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf*

European Union

In Europe, the European Commission's *ePrivacy Directive*[11] currently establishes breach reporting obligations on telecommunications service providers. Specific requirements under the Directive are set out in Commission Regulation (EU) No 611/2013[12]. The European Union has published a draft *General Data Protection Regulation* which proposes to extend these requirements to all organizations.

[11] Directive 2002/58/EC (Directive on Privacy and Electronic Communications) is available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002L0058, as amended and supplemented by Directive 2009/136/EC http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF

[12] Regulation (EU) No 611/2013 is available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

Elements of the Regulations

Determining Real Risk of Significant Harm

Under the new data breach provisions, organizations that become aware that they have experienced a breach of security safeguards must conduct a situational analysis to determine whether or not the breach poses a "real risk of significant harm" to an individual whose personal information was involved in the breach. The conclusion of this analysis is what triggers organizations to take additional actions.

Section 10.1(8) requires that, at a minimum, this analysis consider the sensitivity of the personal information involved in the breach and the probability that the information has or will be misused to inflict harm.

Section 10.1(8) provides the Government with the authority to specify additional factors that are relevant in determining whether a breach poses a real risk of significant harm.

> ***10.1 (8)*** *The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include:*
>
> *a) the sensitivity of the personal information involved in the breach;*
>
> b) *the probability that the personal information has been, is being or will be misused; and*
>
> c) *any other prescribed factor.*

Considerations

The overall objective of PIPEDA's data breach requirements is to ensure that individuals are informed when their personal information has been compromised and that they have been put at risk of harm as a result so that they can take steps to protect themselves and mitigate the harm. This is why a risk-based framework has been established in the Act.

One of the fundamental principles in privacy protection is that context matters. In certain circumstances, the unauthorized access of personal information could be innocuous, while in another, the loss or theft of the same personal information could have seriously harmful consequences. As a result, it is not practical to list specific types of personal information or to identify a defined list of circumstances that trigger the reporting and notification requirements. Instead, PIPEDA requires organizations to conduct a situational analysis that considers both the sensitivity of the personal information involved, given the context; and the probability that the information has or will be used to inflict harm.

Determining whether or not a particular piece of personal information is sensitive, given the context, is something that organizations are already required to do under PIPEDA. For example,

organizations must consider the sensitivity of personal information when obtaining consent, consistent with clauses 4.3.4 and 4.3.6 of Schedule 1 of the Act; or in establishing appropriate security safeguards pursuant to Clause 4.7.2 of Schedule 1 of the Act.

The requirement to consider the probability that the personal information involved in the breach has been, is being, or will be misused will also involve examining a number of sub-factors, depending on the circumstances. Was the data encrypted? How much time has passed between the time the breach occurred and when it was detected? Who obtained access to the data?

Under the OPC's voluntary guidelines, *Key Steps for Organizations in Responding to Privacy Breaches*, organizations are encouraged to consider the following factors in assessing risk:

- The personal information involved, including its sensitivity, whether it was anonymized or encrypted and whether it can be used to inflict harm;
- The cause and extent of the breach;
- The individuals affected by the breach, including how many and whether they were customers, employees or clients of the organization; and
- Foreseeable harm from the breach.

Under Alberta's *Personal Information Protection Act*, there are no criteria set out in the Act or in regulations for determining real risk of significant harm.

In the U.S., regulations pursuant to the *Health Insurance Portability and Accountability Act* specify that the following factors must be considered in an assessment of risk as to the probability that personal information has been compromised:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated[13].

Under the proposed U.S. *Personal Data Notification and Protection Act*, an organization would be able to presume that no risk exists when the information involved in the breach has been "rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted by experts in the field of information security". However the

[13] See Part 164.402 of HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 at http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6

bill states that this presumption would not apply if there is evidence that the encryption was compromised. [14]

In the European Union, the *ePrivacy Directive* requires notification when "the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual". Regulations under the directive require that the following factors be considered in assessing the likelihood of an adverse effect:

- The nature and content of the personal information concerned, including, in particular, enumerated information such as financial information, location data, Internet log files and web browsing history;
- The likely consequences of the breach, particularly if the breach could result in identity theft or fraud, physical harm, humiliation, etc.; and
- The circumstances of the breach, in particular where the data was stolen or is known to be in the possession of an unauthorized third party[15].

In addition, the Directive provides that notification is not required "if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it."[16]

Questions for Discussion

Question 1: Is it necessary to identify additional risk-assessment factors in the regulations? Or are the factors listed in the legislation sufficiently clear?

Question 2: If additional factors should be prescribed, what are they?

Question 3: Should the regulations specify that the risk to individuals can be presumed to be low in circumstances where appropriate encryption has been used? If so, please comment on how an appropriate level of protection should be defined.

[14] See Section 102(b) of the U.S. Personal Notification and Protection Act at https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf

[15] See Article 3.2 of Regulation 611/2013/EC

[16] See Article 4.1 of Regulation 611/2013/EC

Report to Commissioner – Form and Content

If an organization concludes that a breach of security safeguards poses a real risk of significant harm, Section 10.1(1) requires that the organization report the breach to the Privacy Commissioner of Canada.

Section 10.1(2) provides the Government with the authority to list the types of information that must be included in such a report and to specify a particular form and manner for such reports.

> ***10.1(2)*** *The report shall contain the prescribed information and shall be made in the prescribed form and manner as soon as feasible after the organization determines that the breach has occurred.*

Considerations

Reporting breaches to the OPC enables it to fulfil its oversight role to ensure that organizations are complying with their requirement to notify individuals. It will also allow for standardized tracking of serious data breaches in Canada. As a result, reports must contain sufficient information to achieve these objectives, while minimizing at the same time the reporting burden on organizations.

Report Content

The OPC voluntary reporting program has a standard *Privacy Breach Incident Form*,[17] which requests that organizations provide the following information when making a report to the Commissioner:

- Date and location of the breach and date of its discovery;
- Description of the incident;
- Cause of the breach;
- Estimated # of individuals affected;
- Relation of those individuals to the organization (employee, customer);
- Type of information involved;
- Measures taken by the organization to contain the breach; and
- Whether anyone else has been notified of the incident (affected individuals, law enforcement) and when.

In Alberta, the *Personal Information Protection Regulation*[18] specifies the form and manner of a breach report to the Privacy Commissioner of Alberta pursuant to the notification requirement

[17] https://www.priv.gc.ca/resource/pb-avp/pb_form_e.asp

in the *Personal Information Protection Act*[19]. The regulation specifies that the report must be submitted in writing and must contain, at a minimum:

- a description of the circumstances of the breach;
- the date (or time period) of the breach;
- a description of the information involved in the breach;
- an assessment of the risk of harm to individuals that may result from the breach; and
- estimated # of individuals involved
- measures taken by the organisation to reduce the risk of harm to individuals
- contact information for a representative of the organization that can respond to the Commissioner's questions about the breach

It is worth noting that, under this regime, the decision whether to notify individuals rests with the Commissioner. Despite this, the organization is required to provide an assessment of the risk of harm to individuals that may result from the breach. These elements align closely with what is required under breach reporting regimes in other jurisdictions, with some exceptions.

In the U.S., organizations reporting breaches under the *Health Insurance Portability and Accountability Act* are also required to provide the names of law enforcement agencies that have been contacted about the incident and to indicate whether or not individuals have been notified.

Under the European Union's *ePrivacy Directive*, organizations are required to provide authorities with 17 different data points covering the identification of the organization; initial information on the data breach (such as date and time of breach and the nature and content of the personal information concerned); further information on the data breach (such as the number of individuals affected, a summary of the incident that caused the breach); possible additional notification to individuals (such as the content of the notification and means of communication); and possible cross-border issues (such as notification to other competent national authorities)[20].

Questions for Discussion

Question 4: (a) Is there any information required under the existing OPC voluntary report form that should not be included in a mandatory report? If so, what?; (b) Is there additional information that should be required? If so, what?

---

[18] See Alberta Regulation 366/2003 (with amendments up to and including Alberta Regulation 51/21010) at http://www.qp.alberta.ca/documents/Regs/2003_366.pdf

[19] http://www.qp.alberta.ca/documents/Acts/P06P5.pdf

[20] See Annex I of Regulation (EU) No 611/2013 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

Question 5: Should reports to the Commissioner contain an assessment by organizations of the type of harm that may result from a breach and the likelihood of that harm occurring?

The data breach reporting requirements in PIPEDA place an emphasis on the rapid reporting of incidents to the Commissioner – organizations are required to make a report "as soon as feasible after the organization determines that the breach has occurred". This gives organizations some flexibility, permitting them to address more urgent concerns – such as containing the breach – before making the report. However, some data elements required in the report may be more easily known by organizations than others. In addition, following further investigation of a breach, information may change. As a result, the requirement to file the report will need to be quickly balanced with the need to provide complete and accurate information.

In the European Union, regulations under the *ePrivacy Directive* require organizations to report data breaches to the competent national authority no later than 24 hours following detection of the breach. The regulation provides that, where all required information is not available and further investigation is required, the organization shall make an initial report within 24 hours, and then a second report as soon as possible, providing the missing information and any update to information already provided.[21]

Questions for Discussion

Question 6: To what extent should the completion and validation of all elements of the report to OPC be required for an organization to be considered in compliance with the reporting requirement?

Question 7: Should the regulations require organizations to update the Commissioner in circumstances where the information provided in the original report is discovered to be inaccurate, incomplete or has changed?

Report Form

Under its voluntary reporting program, the OPC currently allows breach reports to be submitted by email, standard mail or telephone. In Alberta, reporting to the Commissioner can only take place by email or standard mail. This is also the case under most U.S. state laws. The U.S. *Health Insurance Portability and Accountability* is an exception; electronic reporting of breaches is only permitted via a Web portal designed for this purpose.

[21] See Article 2.3 of Regulation (EU) No 611/2013 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

Similarly, pursuant to regulations made under the European Union's *ePrivacy Directive,* the relevant data protection authority is required to establish "a secure electronic means for notification of personal data breaches" to authorities in each member state[22]. An example can be found on the website of Ireland's Data Protection Commissioner (https://www.dataprotection.ie/secur-breach/form.asp)

Questions for Discussion

Question 8: Should organizations be required to report to the Privacy Commissioner in written format only (electronic or hardcopy) for greater efficiency? If not, why?

Question 9: Should a secure, electronic means of reporting data breaches to the Privacy Commissioner be established?

Notification to Individuals – Content

Section 10.1(3) of the Act requires organizations to notify individuals of any breach involving their personal information that poses a real risk of significant harm. Section 10.1(4) provides that the notification must contain "sufficient information" to ensure the individual understands the risks posed by the breach, and what steps, if any, he or she can personally take to reduce or mitigate the harm.

Section 10.1(4) also provides the Government with the authority to specify additional information in the regulations that must be included in a notification to individuals.

10.1 *(4) The notification shall contain sufficient information to allow the individual to understand the significance to them of the breach and to take steps, if any are possible, to reduce the risk of the harm that could result from it or to mitigate that harm. It shall also contain any other prescribed information*

Considerations

A 2012 consumer study[23] on the impact of data breach notifications in the U.S. found that the type of information provided in a notification to individuals has a direct impact on the effectiveness of the notification. According to the study, most individuals who received notifications were disappointed in how organizations handled the incident, largely due to the perception that the notifications did not help them understand the significance of the breach. In

[22] See Article 2.4 of Regulation (EU) No 611/2013 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

[23] Ponemon Institute Research Report, *2012 Consumer Study on Data Breach Notification*, June 2012.

particular, recipients found that the notifications contained too much "legalese" and were too long.

To improve the effectiveness of notifications, the study recommended that notifications contain specific details about the cause of the breach and the types of data that were lost or stolen. In addition, the study recommended that the organization provide individuals with an explanation of the risks or harm they may experience as a result of the breach.

The OPC's voluntary data breach reporting program suggests that the following information be included in a notification sent to individuals:

- Information about the incident and its timing "in general terms";
- A description of the personal information involved and efforts to control or reduce the harm resulting from the breach;
- What the organization will do to assist individuals, what steps individuals should take to avoid or reduce their harm;
- Sources of information that are designed to assist individuals;
- A contact point within the organization for answering questions or providing further explanation; and
- Contact information for the appropriate (federal or provincial) Privacy Commissioner.

Requirements under provincial data breach frameworks vary. For example, regulations under New Brunswick's *Personal Health Information Privacy and Access Act* stipulate that notifications must include the name of the organization and the contact information of an individual within the organization who can respond to inquiries; a description of the nature of the data breach, the date and location of the breach, and the date the organization became aware of the breach[24].

In Alberta, the *Personal Information Protection Act* leaves the determination for notification to individuals and the timing of that notification in the hands of the Commissioner. However, the associated *Personal Information Protection Regulation*[25] specifies what information should be contained in a notification, should it be required:

- A description of the circumstances of the breach;
- The date (or time period) of the breach;
- A description of the information involved in the breach;
- Measures taken by the organization to reduce the risk of harm; and
- Contact information for a representative of the organization who can answer questions about the breach.

[24] See Section 19(2) of the *General Regulations* made under the *Personal Health Information Privacy and Access Act* at https://www.canlii.org/en/nb/laws/regu/nb-reg-2010-112/latest/nb-reg-2010-112.html
[25] http://www.qp.alberta.ca/documents/Regs/2003_366.pdf

Additional information required under some U.S. laws include the date on which the breach was discovered (in addition to the date the breach is believed to have occurred), as required by the *Health Insurance Portability and Accountability*[26], and a toll-free telephone number and email address through which individuals could obtain more information, as required by the proposed *U.S. Personal Data Notification and Protection Act*[27].

Under the European Union's *ePrivacy Directive*, telecommunication service providers are required to include 9 specific types of information in a notification to individuals. In addition to information about the organizations and details surrounding the breach itself (date, summary of the incident, nature of personal information involved), organizations are required to describe the measures it has taken to address the breach, the "likely consequences" of the breach for the individual concerned; and "measures taken by the organization to mitigate possible adverse effects".[28]

Questions for Discussion

Question 10: Is it necessary for the regulations to identify specific information to be included in notifications to individuals or is the legislation sufficiently clear?

Question 11: If specific information should be prescribed, what information should it be?

Notification to Individuals – Form and Manner

Ensuring that an individual receives a data breach notification and that he or she clearly understands that their personal information has been compromised such that they are at risk of potential harm is the single most important aspect of the framework. As a result, Section 10.1(5) of the Act requires that the notice be communicated directly to an affected individual in a manner that ensures it is not confused with "junk mail" or hidden in other communications material.

In some circumstances however, direct notification to affected individuals may not be feasible. For example, an organization may not have direct contact information for the affected

[26] See Section 164.404 of the *Health Insurance Portability and Accountability Act*'s Breach Notification Rule at http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6

[27] See Section 104 of the proposed *U.S. Personal Data Notification and Protection Act* at *https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf*

[28] See Annex II of Regulation (EU) No 611/2013 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

individual. In these circumstances, notification may need to be made indirectly through alternate means.

Section 10.1(5) provides the Government with the authority to specify in the regulations: (i) the form and manner that direct notifications must take; (ii) the circumstances in which indirect notification may be made instead of direct notification; and (iii) the form and manner in which indirect notification may be made.

> ***10.1*** *(5) The notification shall be conspicuous and shall be given directly to the individual in the prescribed form and manner, except in prescribed circumstances, in which case it shall be given indirectly in the prescribed form and manner.*

Considerations

Direct Notification

Given the wide range of organizations subject to PIPEDA and the different circumstances in which data breaches can occur, some degree of flexibility concerning how data breach notifications can be made is desirable. For example, email is an efficient and cost-effective means of communicating with a large number of individuals but may not be appropriate for notifications that discuss the loss of highly sensitive information, such as health or financial information. Similarly, in-person meetings with individuals may be suited to organizations dealing with highly valued customers or employees but would not be practical for communicating with a large number of people.

In all cases, it is important that the notification be conspicuous and clear and that individuals understand and appreciate it. Regardless of the method of direct notification (email, regular mail, telephone, in person, etc.), it is important that the notification be distinct from other communications between the organization and affected individuals. For example, it would not be appropriate for a data breach notification to be provided as part of a regular customer bill or invoice.

Under its voluntary privacy breach reporting program, the OPC recommends that notification be made to individuals by telephone, letter, email or in-person.

Rules under provincial data breach frameworks vary slightly. Regulations under New Brunswick's *Personal Health Information Privacy and Access Act* stipulate that notification must be made "by telephone or in writing". Alberta's *Personal Information Protection Act*, is silent on the specific

means of notification permitted; regulations simply state that the notification must be "given directly"[29].

In contrast, the proposed *U.S. Personal Data Notification and Protection Act* would not allow for in-person notification and places certain conditions around the use of other methods. For example, notification by standard mail must be sent to the last known home mailing address of an affected individual. Telephone notification must be provided to the affected individual personally (i.e. the information cannot be provided in a voice message). E-mail notification is only permitted where the individual has provided the required consent beforehand, and the email must meet the technical standards identified in the Act[30].

The U.S. *Health Insurance Portability and Accountability Act* requires written notification by two means only: first class mail to the affected individual's last known address; or by e-mail, where the individual has chosen *not* to receive notifications by mail.[31]

Most U.S. state laws require notifications to be sent by first class mail. Those that allow telephone notification require the organization to keep a log of calls made. Where email is permitted, a common condition placed on its use is that the individual has "expressly consented to receiving this type of notice in electronic form" and that a log of each notification be kept by the organization.

In the European Union, the *ePrivacy Directive* does not outline specific methods by which notifications are to be made, beyond requiring that it be "by means of communication that ensure prompt receipt of information and that are appropriately secured according to the state of the art. Information about the breach shall be dedicated to the breach and not associated with information about another topic."[32]

[29] See Subsection 19.1(1) of the *Personal Information Protection Act Regulation* at http://www.qp.alberta.ca/documents/Acts/P06P5.pdf

[30] See Section 103 of the *Personal Data Notification and Protection Act* at https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-data-breach-notification.pdf

[31] See Part 164.404 of the *Health Insurance Portability and Accountability Act*'s Breach Notification Rule at http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6

[32] See Article 3.6 of Regulation (EU) No 611/2013 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

Questions for Discussion

Question 12: What methods of communication should be permitted for direct notification to individuals?

Question 13: Should the regulations set any conditions and/or limitations on the use of any method of direct communication? If yes, what conditions and/or limitations?

Question 14: Should the regulations set-out specific requirements for notifications to be conspicuous and distinct from other communications?

Indirect Notification – Permitted Circumstances

As discussed previously, PIPEDA recognizes that there are circumstances where direct notification to individuals affected by a data breach is not practical or possible. In these circumstances, notifications are to be made indirectly.

Under the OPC's voluntary data breach reporting program, organizations are encouraged to indirectly notify individuals of a data breach in the following circumstances:

- Where direct notification would cause further harm to the individual;
- Where direct notification is prohibitive in cost; or
- Where the contact information of affected individuals is not known.

It should be noted that the word "prohibitive" is not defined in the OPC guidance. As the term is subjective, consideration may need to be given to the meaning of this term if used in regulations. For example, the cost of notification to all affected individuals in the case of a large breach may be prohibitive to one organization, but entirely manageable to another.

Alberta's *Personal Information Protection Act* also allows for indirect notification where the Commissioner determines that direct notification would be "unreasonable under the circumstances".

Pursuant to regulations made under the European Union's *ePrivacy Directive*, there is less flexibility. Organizations are only permitted to use indirect means of communication when the organization cannot identify all the individuals affected by a breach within a specific timeframe. In this case, the organization may provide indirect notification through advertisements in major national or regional media outlets.[33]

[33] See Article 3.7 of Regulation (EU) No 611/2013 at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

Similarly, legislation pertaining to the US health care sector only permits the use of indirect notification to individuals where the contact information of affected individuals is not available. The *Health Insurance Portability and Accountability Act* allows for "substitute notification" if the contact information is "insufficient or out-of-date"[34]. The *American Recovery and Reinvestment Act* is similar but stipulates that the organization must first make a reasonable effort to contact affected individuals before substitute notification can be employed.[35]

Questions for Discussion

Question 15: In what circumstances should organizations be permitted to indirectly notify individuals of a data breach?

Question 16: If cost is a consideration in determining whether indirect notification is permitted, how should the regulations establish the appropriate threshold?

Indirect Notification

Under the OPC's voluntary data breach reporting program, where notification to individuals is made indirectly, organizations are encouraged to use websites and/or the media to inform the public.

Although Alberta's *Personal Information Protection Act* allows indirect notification to replace direct notification in certain circumstances, neither the Act nor associated regulations specify permitted means.

Within the U.S. healthcare sector, both the *Health Insurance Portability and Accountability Act* and the *American Recovery Reinvestment Act* permit indirect notification (referred to as "substitute notification") in the event that the notifying organization is unable to find contact information for affected individuals. In circumstances where fewer than 10 individuals are affected by the breach, the organization can choose an alternate means of notification that would be "reasonably calculated to reach the individual". In the case of 10 or more individuals, notification may be provided by:

[34] See Part 164.404 of the Health Insurance Portability and Accountability Breach Notification Rule at http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6

[35] See Part 318.5 of the ARRA *Health Breach Notification Rule* at http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=6ae79a215bd299fd401a63594e98ce70&ty=HTML&h=L&n=16y1.0.1.3.42&r=PART

- a conspicuous posting on the home page of the organization's website for 90 days; or
- major print or broadcast media in geographic areas where the individuals are likely to reside. This notice must include a toll-free telephone number where members of the public can learn whether or not their information may be affected.[36]

In the European Union, organizations indirectly notifying individuals through major national or regional media outlets must include the same information that is required in a direct notification to individuals, where necessary, in a condensed form. As well, organizations are required to continue to make all reasonable efforts to identify individuals not provided with direct notification and to contact them directly as soon as possible.

Questions for Discussion

Question 17: For indirect notifications to individuals, what methods of communication should be permitted?

Question 18: Should the regulations place any conditions and/or limitations on the use of any method of indirect communication? If yes, what conditions and/or limitations?

Notification to Other Organizations

The primary objective of the new data breach reporting and notification framework in PIPEDA is to prevent or mitigate the potential harm to individuals resulting from a breach. In certain circumstances, this objective may be achieved by requiring organizations to notify other organizations that are in a position to reduce or mitigate the risk of harm. As a result, Section 10.2(1) requires organizations to notify third parties of a potentially harmful data breach if the organization making the notification believes that the third party may reduce or mitigate the potential harm.

In addition, Section 10.2(1) gives the government the authority to prescribe specific circumstances where notification to a third party is required.

10.2 (1) *An organization that notifies an individual of a breach of security safeguards under Subsection 10.1(3) shall notify any other organization, a government institution*

[36] See Part 164.404 of the Health Insurance Portability and Accountability Act Breach Notification Rule at http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6 and Section 318.5 of the *American Recovery and Reinvestment Act*'s Health Breach Notification Rule at http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=6ae79a215bd299fd401a63594e98ce70&ty=HTML&h=L&n=16y1.0.1.3.42&r=PART

or a part of a government institution of the breach if the notifying organization believes that the other organization or the government institution or part concerned may be able to reduce the risk of harm that could result from it or mitigate that harm, or if any of the prescribed conditions are satisfied.

Considerations

The OPC's voluntary data breach reporting program recommends that organizations experiencing a breach consider whether the following organizations be notified of the data breach in certain circumstances:

- Law enforcement agencies, if theft or another crime is suspected;
- Insurance companies, if required by contractual obligations;
- Professional or other regulatory bodies, if professional or regulatory standards require notification of these bodies;
- Credit card companies, financial institutions or credit reporting agencies, if their assistance is necessary for contacting individuals or assisting with mitigating harm; and
- Union or other employee bargaining units, if the breach involves their members.

In Alberta, it is the provincial Privacy Commissioner who determines whether notification to other organizations is required and which organizations to notify. The legislation and associated guidance do not indicate how this determination is made.

In the U.S., most state laws require notifying organizations to inform law enforcement agencies when financial information is compromised. In addition, many state laws require notification to credit reporting agencies of any breach affecting a large number of individuals, anywhere from 1,000 to 10,000 individuals.

Interpretation guidance pursuant to the U.S. *Gramm-Leah- Bliley Act*[37] requires that, in the event of any breach where criminal activity is believed to be involved, or there is evidence of identity theft resulting from the breach, relevant law enforcement agencies must be notified.

The proposed *U.S. Personal Data Notification and Protection Act* would require organizations to inform national consumer credit reporting agencies in cases where more than 5,000 individuals are affected by a breach. Law enforcement would also need to be notified where the breach affects:

- more than 500,000 individuals;
- any database owned by the Federal Government; or

[37] See *Supplement A to Appendix B to Part 570 —Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice at* https://www.law.cornell.edu/cfr/text/12/part-570/appendix-B

- the information of Federal Government employees working in national security or law enforcement.

Questions for Discussion

Question 19: Should the regulations set out specific circumstances where organizations would always be required to notify third parties of a data breach? If yes, in what circumstances?

Record Keeping

Under Section 10.3(1) of PIPEDA, organizations that become aware of a breach of security safeguards must keep and maintain a record of the breach, regardless of the conclusion of their situational analysis into whether the breach poses a "real risk of significant harm".

Section 10.3(1) provides the government with the authority to specify requirements for these records.

10.3 (1) *An organization shall, in accordance with any prescribed requirements, keep and maintain a record of every breach of security safeguards involving personal information under its control.*

Considerations

The requirement to maintain records of any data breach experienced by an organization is intended to achieve two main objectives. First, the record will provide a mechanism for the Privacy Commissioner to provide oversight of the data breach reporting and notification requirements set out in Section 10.1 of the Act. Section 10.3(2) of the Act requires organizations to provide the Commissioner with access to or a copy of a data breach record, upon request of the Commissioner.

Second, the need to maintain records will force organizations to systematically document data breaches, regardless of their risk or severity, across their business. This will provide a mechanism for organizations to identify any pattern of breaches that indicates a systemic problem or failure in their security safeguards. On this basis, organizations can take action to correct any systemic problem to avoid any future breaches that may pose a risk of harm to individuals.

With these two objectives in mind, specific requirements for records set out in the regulations should contain sufficient information for the Commissioner to provide effective oversight and for organizations to recognize systemic patterns. At the same time, the requirements should be flexible and reasonable so as to minimize the burden on organizations.

Contents of Records

Several data breach reporting and notification frameworks contain record keeping requirements. In many cases, these records are required so that an organization can demonstrate why it determined it was not required to notify individuals of the data breach.

In Canada, for example, under the New Brunswick *Personal Health Information Privacy and Access Act,* organizations are required to "keep a record of all security breaches by recording the security breaches and corrective procedures taken to diminish the likelihood of future breaches"[38].

Under the U.S. *American Reinvestment and Recovery Act*, organizations must be able to demonstrate compliance with the notification requirements of the Act or that a use or disclosure of unsecured information did not constitute a breach. For this purpose, they are required to maintain supporting documentation[39]. Where an organization has chosen not to notify individuals, for example, it must maintain a record of a risk assessment demonstrating a low probability of risk arising from that breach.

The European Union's *ePrivacy Directive*[40] requires organizations to maintain an inventory of personal data breaches that they have experienced, which must include "the facts surrounding the breach, its effects and the remedial action taken". The directive further stipulates that "the inventory shall only include the information necessary" for the purpose of enabling national data protection authorities (counterparts to Canada's Privacy Commissioner) to verify compliance with the directive's data breach reporting requirements. Explanatory notes pertaining to this requirement[41] state that the inventory allows authorities to verify an organization's obligations under the Directive.

[38] See Section 20(2) of the *General Regulations* made under the *Personal Health Information Privacy and Access Act* at https://www.canlii.org/en/nb/laws/regu/nb-reg-2010-112/latest/nb-reg-2010-112.html
[39] See Part 164.414 of the Health Insurance Portability and Accountability Breach Notification Rule at http://www.ecfr.gov/cgi-bin/text-idx?SID=ec9b2abf79543bc3ee8b52174c97648c&mc=true&node=sp45.1.164.d&rgn=div6 and the U.S. Department of Health and Human Services website on the Breach Notification Rule at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html
[40] See Article 2 of Directive 2009/136/EC
[41] Recital 58 of Directive 2009/136/EC

Questions for Discussion

Question 20: Should the regulations list specific data fields for records or should it set-out a more flexible approach requiring "sufficient information to indicate the breach does not pose a real risk of significant harm" or similar?

Question 21: What information should the regulations require be included in a data breach record?

Maintenance of Records

During Parliamentary review of the *Digital Privacy Act*, some stakeholders expressed concern over specific requirements related to the maintenance of data breach records. Issues that were identified included:

- the retention period of records;
- whether specific individuals in the organization are required to maintain the records and provide them to the Privacy Commissioner upon request (those individuals designated by the organization to oversee the organization's compliance with PIPEDA as required under Schedule 1 of the Act);
- whether records are required for data breaches that have been reported to the Privacy Commissioner;
- whether the obligation to maintain records applies only to data breaches where the organization has actual knowledge of the breach, or if the obligation also applies to assumed breaches (for example, established estimates of misdirected mail containing personal information); and
- whether records could take the form of a consolidated monthly, quarterly or annual roll-up of data breaches experienced by the organization (containing the required information for each breach).

Questions for Discussion

Question 22: Should the regulations specify a retention period for data breach records? If yes, how long would be considered a reasonable retention period?

Question 23: Should the regulations clarify that the individual(s) designated by the organization as those responsible for overseeing compliance with PIPEDA are those accountable for maintaining data breach records and providing them to the Privacy Commissioner upon request?

Question 24: Should the regulations clarify that a report made to the Privacy Commissioner satisfies the record-keeping requirement under Section 10.3(1)?

Question 25: Should the regulations clarify that the obligation to maintain a data breach record applies only to data breaches for which the organization has actual knowledge?

Question 26: Should the regulations permit data breach records to take the form of periodic roll-ups that consolidate information concerning data breaches experienced by the organization over the applicable period? Or should the regulations specify that a separate record is required for each data breach experienced by the organization?

Other Issues

Innovation, Science and Economic Development Canada would appreciate hearing about any other issues that should be considered in the drafting of the regulations.

Of particular interest to the Department are issues and questions which relate to:

- specific industry sectors;
- multi-national organizations;
- organizations working in multiple jurisdictions; or
- small- to medium-sized organizations.

Responding to This Consultation

Innovation, Science and Economic Development Canada invites written views and comments on the issue raised in this document to be submitted by May 31, 2016. Submissions may be sent in electronic format (Microsoft Word or Adobe PDF) to the address below; or in hard-copy format by mail. In your reply, please indicate whether you are responding in a private capacity or on behalf of an organization, and provide the name, telephone number and email address of a contact person in your organization for any questions on your submission.

Please note that submissions and/or a summary of submissions may be published on the Innovation, Science and Economic Development Canada website.

Mailing address:

Data Breach Consultations
Privacy and Data Protection Policy Directorate
Innovation, Science and Economic Development Canada
235 Queen Street
Ottawa ON K1A 0H5

Email: **ic.ised.breach-atteinte.isde.ic@canada.ca**