Comments on Draft Breach of Security Safeguards Guidance

By Eloïse Gratton, Ad. E.[1], Bradley J. Freedman[2] and François Joli-Coeur[3]

We submit these comments in response to the *Notice of consultation on new mandatory breach reporting guidance and form*, issued on September 17, 2018 by the Office of the Privacy Commissioner of Canada ("**OPC**"). These comments are made in our individual capacity, not on behalf of our law firm or any of its clients.

The Notice invites comments regarding the OPC's draft *guidance*, published September 17, 2018, regarding the breach of security safeguards provisions in the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which provisions come into force on November 1, 2018.

Our comments are limited to the part of the draft guidance under the heading "Who is responsible for reporting the breach?". In particular, our comments relate to the draft guidance that a breach report must submitted by "all organizations involved in the breach", and the illustrative example that both an organization that collects personal information (Company A) and its data processing service provider (Company B) are obligated to report a breach to the OPC.

In our view, those aspects of the draft guidance are contrary to the plain language of PIPEDA's breach of security safeguards provisions and inconsistent with the approach taken in other personal information protection regimes, and could have potentially serious adverse practical consequences.

1. The Plain Language of PIPEDA

PIPEDA's breach of security safeguards provisions impose three distinct obligations – reporting to the OPC (section 10.1(1)), giving notices to affected individuals and other organizations and government institutions (sections 10.1(3) and 10.2) and keeping records of breaches (section 10.3). Those obligations apply to an organization with respect to a breach of security safeguards involving personal information "under its control" or "under the organization's control". Basic statutory interpretation principles require that the word "control" should be given the same meaning in each of those statutory provisions.[4]

The word "control" is not explicitly defined in PIPEDA, but it is generally understood to reflect the Accountability principle, which provides that an organization is responsible for personal information "under its control". Accountability principle 4.1.3 provides the paradigmatic example of control – "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing".

Parliament could have easily imposed some or all of the breach of security safeguards obligations on an organization that has "possession" or "custody" of personal information affected by a breach. However, Parliament chose not to do so. Instead, Parliament limited all of those obligations to an organization that has "control" over affected personal information. In doing so, Parliament followed the model used in the Alberta *Personal Information Protection Act* (discussed below).

The draft guidelines are inconsistent with the plain and ordinary meaning of "control", as that term is used in PIPEDA, insofar as the guidelines suggest that both an organization that collects personal information (Company A) and its data processing service provider (Company B) are obligated to report a breach to the

---

[1] Partner at Borden Ladner Gervais LLP and National Co-Leader of BLG's Privacy and Data Protection Practice Group.

[2] Partner at Borden Ladner Gervais LLP and National Co-Leader of BLG's Cybersecurity Law Group.

[3] Senior Associate at Borden Ladner Gervais LLP.

[4] *R. v. Zeolkowski*, [1989] 1 SCR 1378, 1989 CanLII 72 (SCC): "Giving the same words the same meaning throughout a statute is a basic principle of statutory interpretation". *Thomson v. Canada (Deputy Minister of Agriculture)*, [1992] 1 SCR 385, 1992 CanLII 121 (SCC): "Unless the contrary is clearly indicated by the context, a word should be given the same interpretation or meaning whenever it appears in an Act."

OPC. In the example, only Company A has "control" over the personal information. Company B has possession or custody of the personal information, but it does not have "control" over the personal information. Consequently, only Company A should be obligated to report a breach to the OPC.

2. Other Personal Information Protection regimes

The Alberta *Personal Information Protection Act*, SA 2003 ("**Alberta PIPA**") and the European *General Data Protection Regulation* ("**GDPR**") do not require data processing service providers to report personal information security breaches to the privacy regulators or affected individuals or to keep records of personal information security breaches.

(a) Alberta PIPA

Alberta PIPA provides that an organization is responsible for, and must protect, personal information that is "in its custody or under its control" (sections 5(1) and 34), but imposes breach reporting and notification obligations on an organization only with respect to personal information "under its control" (section 34.1).

The Office of the Information Privacy Commissioner of Alberta's *Practice Note – Reporting a Breach to the Commissioner* provides guidance regarding who has control over personal information and is responsible for reporting a breach to the Alberta Commissioner, The Practice Note clearly states that a data processing service provider does not have "control" over the personal information that it is processing for another organization.[5]

(b) GDPR

The GDPR has adopted a similar approach and takes it a step further by clearly defining and distinguishing between a "controller" (an organization that determines the purposes and means of the processing of personal data) and a "processor" (an organization that processes personal data on behalf of the controller). Those same concepts were used in *Directive 95/46/EC of the European Parliament*, which was the predecessor to the GDPR, and interpreted in *Opinion 1/2010 on the concepts of "controller" and "processor"* issued by the Article 29 Working Party (an advisory body comprised of representatives from the data protection authorities of each EU Member State, the European Data Protection Supervisor and the European Commission). Under the GDPR, both a data controller and a data processor are required to protect personal data (Article 32), but only a data controller is obligated to give notice of a personal data breach to the relevant supervisory authority (Article 33.1) and affected individuals (Article 34.1) and to document personal data breaches (Article 33.5). The data processor's obligations are limited to notifying the data controller of a personal data breach (Article 33.2).

3. Adverse Practical Consequences

A requirement for both a collecting organization (i.e. data controller – Company A) and its data processing service provider (i.e. data processor – Company B) to report security breaches to the OPC could have potentially serious adverse practical consequences.

(a) Notifications and Record Keeping Obligations

As noted above, the concept of "control" is the touchstone of PIPEDA's breach of security safeguards provisions. An organization that has "control" of personal information affected by a breach of security

[5] The Alberta OIPC's guidance is in line, by analogy, to analysis of the notions of custody and control under freedom to information legislation, including the Supreme Court of Canada's decision in *Canada (Information Commissioner)* v. *Canada (Minister of National Defence)* ([2011] 2 SCR 306) and case law about the notion of control under the Ontario *Freedom of Information and Protection of Privacy Act* (see for instance orders 120; P-239; MO-1251; PO-2306; PO-2683).

safeguards is required to keep records of the breach and, if the breach presents a real risk of significant harm, to report the breach to the OPC and to give notice of the breach to affected individuals and certain other organizations and government institutions.

Consequently, if both an organization that has collected personal information (Company A) and its data processing service provider (Company B) are required to report a breach of security safeguards to the OPC, then they are also both required to give notice of the breach to affected individuals and certain other organizations and government institutions and to keep records of the breach.

(b) Practical Challenges

As a practical matter, it will be difficult for service providers to comply with all application obligations. Many service providers will likely not have the information and insight required to assess whether a breach of security safeguards presents a real risk of significant harm, to identify the affected individuals and relevant organizations and government institutions to whom notice must be given, or to give direct notices to affected individuals.

(c) Confusion and Notification Fatigue to Affected Individuals

Requiring breach of security safeguard notices from both a collecting organization (Company A) and its data processing service provider (Company B) would be confusing to affected individuals, especially since in most cases the individuals will not have any knowledge about the existence or involvement of the service provider. If a breach occurs at the level of a service providers' subcontractor, then even more organizations would be required to send notices to affected individuals in connection with the breach, thus increasing their confusion.

In addition to confusion, multiple notices for each breach of security safeguards could quickly desensitize individuals or lead to "notification fatigue", so that the individuals ignore or fail to fully appreciate the consequences of having their personal information compromised.

(d) Incomplete, inaccurate and inconsistent reports and notices

Requiring both a collecting organization (Company A) and its data processing service provider (Company B) to report and give notices of security safeguard breaches could lead to disagreements between the organizations with respect to the timing and content of the reports and notices, with the result that the organizations provide incomplete, inaccurate and inconsistent information to the OPC, affected individuals and other organizations and government institutions. For instance, individuals could receive inconsistent recommendations regarding the risk of harm result from a breach and the steps they could take to reduce the risk of harm or to mitigate harm. The OPC's task of monitoring breach reports, and investigating when required, would also be made more cumbersome.

In our experience, most security safeguard breaches are complex and must be properly investigated, often with the assistance of external technical consultants, before an organization is able to properly assess whether the breach presents a real risk of significant harm or provide accurate information about the breach to regulators and affected individuals. For example, an investigation is often required to understand fully the nature of the breach and to identify the personal information involved and the affected individuals. Those kinds of investigations can be costly and time consuming. Since service providers do not have the same level of legal risk and reputational exposure as data controllers with respect to a breach (i.e. service providers have no direct relationship with affected individuals), service providers might not be willing to properly investigate a breach before reporting it to the OPC or giving notice of it to affected individuals. The result may be inaccurate and incomplete reports and notices.

(e) Conflicting Best Practices

PIPEDA expressly requires an organization to use contractual or other means to provide a comparable level of protection to personal information while it is being processed by a service provider. The OPC has issued best practices guidance for data processing arrangements, including the use of written services agreements.[6] Those kinds of agreements often set out the parties respective obligations regarding personal information security breaches, including an obligation on the service provider to promptly inform the data collecting organization of any data security breach and to allow the data collecting organization to determine whether, when and how the breach should be reported to the regulators and affected individuals. In our experience, those provisions have been efficient and effective in ensuring that personal information security breaches are properly and timely investigated and accurately reported to the OPC and affected individuals.

Requiring data processing service providers to report security breaches to the OPC and give notices of security breaches to affected individuals would conflict with those common contractual arrangements, and might require data processing service providers to breach their contractual obligations.

4. Conclusion

For the reasons set out in this comment, we strongly recommend that the draft guidance be revised to adopt the distinction between personal information controllers and personal information processors (as those concepts are used in Alberta PIPA and the GDPR), and to confirm that each of the breach of security safeguards obligations – reporting to the OPC, notices to affected individuals and other organizations and government institutions, and record-keeping – set out in PIPEDA Division 1.1 apply only to an organization that has control over affected personal information (Company A) and not to its data processing service provider (Company B).

[6] For example, see *Interpretation Bulletin: Accountability* (April 2012).