Cassels

Mandatory Data Breach Reporting Under PIPEDA: The Final Countdown to November 1

October 11, 2018

On November 1, 2018, important legislative compliance requirements pursuant to the *Personal Information Protection and Electronic Documents Act* (PIPEDA)[1] and the Breaches of Security Safeguards Regulation (Regulations) will come into force.[2] Of particular note, organizations subject to PIPEDA will have to comply with the mandatory reporting requirements regarding breaches of security safeguards involving personal information that pose a "real risk of significant harm" to individuals. The Office of the Privacy Commissioner of Canada (OPC) has recently published guidance clarifying these breach notification obligations.[3]

What is a Breach?

As a starting point, an organization subject to PIPEDA must report to the OPC *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. A breach of security safeguard is defined under PIPEDA as "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards."[4]

"Real Risk of Significant Harm"

Applying and implementing this definition of "real risk of significant harm" can be difficult in practice. To provide some guidance, the OPC highlights two factors that are relevant in assessing whether a breach creates a real risk of significant harm: one, the sensitivity of the personal information involved in the breach; and two, the probability that the personal information has been, is being, or will be misused.[5] The assessment of sensitivity of the information is contextual and the circumstances of the breach will inform the extent to which the information is sensitive. Although certain information may be obviously sensitive, other information may not be. Organizations should consider the potential harms that could accrue to an individual. The assessment of the probability of misuse requires an organization to inquire into several aspects of the breach. For example, factors such as who actually accessed or could have accessed the personal information, the length of time the information has been exposed, and the presence of any evidence of malicious intent are all to be taken into account.

The province of Alberta has had breach notification using the "real risk of significant harm" test as part of its *Personal Information Protection Act* since 2010.[6] Therefore, it is helpful to canvass existing interpretive guidance that the Alberta's Office of the Information and Privacy Commissioner (AOIPC) has provided as well as the applicable cases on the definition of "real risk of significant harm" under the Alberta statute.

Based on the Alberta experience, to meet the "significant" harm test the harm must be important, meaningful, and have non-trivial consequences or effects.[7] A common theme across many of the Alberta cases is that identity theft, fraud, and financial loss militate in favour of a finding of significant harm.[8]

In terms of meeting the threshold of “real risk”, the likelihood that the significant harm will result must be more than mere speculation or conjecture.[9] A broad exposure of the compromised information (e.g. on the dark web with unknown source)[10] can increase the probability of risk. As well, in *Feld Entertainment, Inc.*[11], it is explicitly stated that the lack of reported misuse over a period of as long as three months does not mean such activities will not occur in the future. Importantly, other forms of harm beyond the most directly causal consequence will be considered in assessing risk. For example, speculation on the part of an organization that the breach would not cause credit card fraud does not necessarily mitigate the potential harm from identity theft or other forms of fraud as it was determined that many individuals use the same credentials across various accounts.[12]

As another example, in *McAfee Ireland Ltd.*[13], the AOIPC decided that there was a real risk of significant harm from an incident where customers of the organization’s India-based support service vendor received fraudulent phone calls from callers misrepresenting themselves as the support vendor. In *McAfee*, the presence of malicious intent (social engineering for financial gain) was deemed a real risk, and the combination of compromised contact information and subscriber information could be used for unsolicited targeted telephone calls and phishing attacks, constituting significant harm.[14]

It is important to note that under PIPEDA, notification to individuals must be given as soon as feasible after an organization has determined a breach involving a real risk of significant harm has occurred. The policy rationale behind this requirement is that by providing notification to the individual, it allows the individual to understand the significance of the breach and to take steps to reduce the risk of or mitigate the harm.[15]

Contract Negotiation with Service Providers

As the PIPEDA breach notification requirement applies to all organizations with control of personal information involved in a breach, each organization must consider its own obligations under PIPEDA. The OPC expects that each organization will submit its own report to the OPC in the event that the breach notification obligation is triggered. Companies engaging in contractor and subcontractor work should provide a process for dealing with these respective obligations upfront in their contractual arrangements to avoid any confusion.[16]

Record Keeping

Organizations must keep a record of every data breach for at least two years, however, the OPC actually recommends that the records be kept for five years.[17] Also of note is that although there is no enumerated definition of a “record” in the Regulations, the definition of a “record” is construed broadly by the OPC.[18] The

Access to Information Act[19] (AIA) has been amended to provide an exception from disclosure for data breach reports, so this broad interpretation of a "record" would shelter a wider array of information from disclosure under the AIA.

Conclusion

As of November 1, 2018, organizations are required to report to the OPC and the affected individuals 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 the individuals. A common theme that militates in favour of a finding of "real risk" from Alberta's experience with a similar requirement is evidence of malicious intent (e.g. financial gain, vehicle break-in, theft, or impersonation of a person in authority, etc.). In drafting and negotiating contracts with service providers who handle personal information, organizations need to address the parties' respective breach notification obligations as well as the record-keeping obligations. As these changes to PIPEDA and the Regulations will shortly come into force, organizations handling personal information must quickly adapt to the new landscape of privacy protection.

The author of this article gratefully acknowledges the contributions of articling student Tiffany Chiu in the preparation of this article.

---

[1] *Personal Information Protection and Electronic Documents Act* SC 2000, c5.
[2] Breach of Security Safeguards Regulations: SOR/2018-64, C Gaz Vol. 152, No. 8, available at <http://gazette.gc.ca/rp-pr/p2/2018/2018-04-18/html/sor-dors64-eng.html > "Regulations".
[3] The OPC has released some guidance for businesses to understand the mandatory breach notification requirements, available online: PRIV.gc.ca <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-pb/gd_pb_201809/> "OPC Guidance".
[4] *Personal Information Protection and Electronic Documents Act* SC 2000, c 5 Part 1 at 2(1).
[5] OPC Guidance, *supra* note 3.
[6] The Privacy Commissioner of Alberta has published decisions on breach notification, available online: OIPC.ab.ca <https://www.oipc.ab.ca/decisions/breach-notification-decisions.aspx> "Alberta Decisions".
[7] Alberta Decisions: P2018-ND-124, *supra* note 6.
[8] Alberta Decisions: P2018-ND-123; P2018-ND-122; P2018-ND-121, *supra* note 6.
[9] Alberta Decisions: P2018-ND-124, *supra* note 6.
[10] Alberta Decisions: P2018-ND-124, *supra* note 6.
[11] Alberta Decisions: P2018-ND-120, *supra* note 6.
[12] Alberta Decisions: P2018-ND-116, *supra* note 6.
[13] Alberta Decisions: P2018-ND-124, *supra* note 6.
[14] *Ibid*.
[15] OPC Guidance, *supra* note 3.
[16] *Ibid*.
[17] Regulations, *supra* note 2.
[18] *Ibid*.
[19] *Access to Information Act*, RSC 1985, c A-1.