

## 4. What Is the Threshold for Reporting and Individual Notification?

The Privacy Officer's Guide to Personal Information Protection and Electronic Documents Act, 2024 Ed.

Timothy M. Banks

**The Privacy Officer's Guide to Personal Information Protection and Electronic Documents Act, 2024 Ed. (Banks) > Chapter 5 OBLIGATIONS IN CONNECTION WITH MANAGING PERSONAL INFORMATION > G. Breach Reports, Individual Notification and Recordkeeping**

### **Chapter 5 OBLIGATIONS IN CONNECTION WITH MANAGING PERSONAL INFORMATION**

#### **G. Breach Reports, Individual Notification and Recordkeeping**

##### ***4. What Is the Threshold for Reporting and Individual Notification?***

An organization 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” (PIPEDA, s. 10.1(1)). The CPPA contains the same provision (CPPA, s. 58(1)). The OPC refers to this as the “RROSH” test. This is the same threshold for the mandatory breach notification obligations to affected individuals. PIPEDA requires notification to individuals unless prohibited by law “if it is reasonable in the circumstances to believe that the breach creates a real risk of significant harm to the individual” (PIPEDA, s. 10.1(3)). The CPPA contains the same requirement (CPPA, s. 58(3)). Therefore, any breach that must be reported to the OPC must also be reported to the individual.

The wording of the threshold for reporting and notification under PIPEDA (and the CPPA) is very similar to that in Alberta’s breach reporting provisions.<sup>1</sup> However, to date the OPC has not provided any guidance on whether it agrees or disagrees with the way in which the Alberta Commissioner has applied the test. However, it is worthwhile to consider how the Alberta Commissioner has interpreted the test in Alberta, given the potential influence of those decisions on the OPC.

PIPEDA states that significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property (PIPEDA s. 10.1(7)). This list is open-ended. This same open-ended list is found in the CPPA (CPPA, s. 58(7)). This is a very broad sense of what might constitute significant harm. Although it would seem absurd if trivial damage was considered to be significant harm simply because it is mentioned in the list of what is included in the definition of that concept, this seems to be the effect of the definition. Any harm listed would be deemed to be significant harm. The Alberta statute does not contain a definition of significant harm. Instead, the Alberta Privacy Commissioner has concluded that significant harm requires that the damage or detriment be important, meaningful and non-trivial in terms of consequences or effects.<sup>2</sup> This is a sensible approach and may be used to assess whether harms not listed in the definition of significant harm meet the threshold. However, it is unlikely that an organization can use this more flexible approach to whether a harm is “significant” if it is already listed in the definition.

Unlike the Alberta legislation, PIPEDA also expressly provides for an open-ended list of factors that are relevant to determining whether there is a “real risk” of significant harm. These include the sensitivity of the affected personal information, the probability that the personal information has been, is being or will be misused and any other factor prescribed by regulation (PIPEDA, s. 10.1(8)). No additional factors have been prescribed. The CPPA contains the same provision (CPPA, s. 58(8)). When interpreting the Alberta statute, the Alberta Commissioner has concluded that this concept requires something more than mere speculation or conjecture and that there must be a causal

#### 4. What Is the Threshold for Reporting and Individual Notification?

relationship between the breach and the possible harm.<sup>3</sup> This is also sensible. In order for there to be a “real risk”, the analysis should be evidence-based.

The OPC has issued some guidance on assessing the real risk of significant harm test.<sup>4</sup> Interpreting the probability of misuse, the OPC suggests that organizations consider the following factors among others:

- the length of time the personal information had been exposed;
- whether there is evidence of malicious intent (e.g., theft, hacking);
- the number of pieces of personal information about the individual that were the subject of the breach;
- whether there could be a reputation risk to the individual as a result of the information being in the hands of someone like an ex-spouse or employer;
- if the information was misdirected, whether the recipient has committed to destroy and not disclose the data;
- whether the information was inadvertently disclosed and the likelihood of misuse is low;
- whether any harm has actually materialized;
- whether the information has been recovered; and
- whether the information was adequately encrypted, anonymized or otherwise not easily accessible.

In *PIPEDA Report of Findings #2022-004*,<sup>5</sup> the OPC investigated MGM Resorts International (“MGM”) for failing to report a breach of security safeguards relating to its U.S. hotels and casinos. In February 2020, the OPC became aware of media reports relating to the posting of personal information of 10.6 million guests on a hacking forum following a hacking incident involving a service provider to MGM. In some cases, information included driver’s licenses and passport numbers. The OPC concluded that “government-issued identifiers” were sensitive information because “these can be very useful in the context of fraud and identity theft.”<sup>6</sup> The OPC agreed that other information (names, dates of birth, phone numbers, email address, and residential address) may not be sensitive in isolation; however, they were sensitive when attached to a government identifier. Further, these data elements were more sensitive in the contest of being posted for sale to malicious actors because they could be misused for “harm activities such as identity fraud, financial harm, and phishing.”<sup>7</sup> In assessing the risk of misuse, the OPC found that the fact that the information was exfiltrated by a malicious third party and posted for sale for the likely purpose of further malicious activity.<sup>8</sup> MGM’s view was that the data was not well-structured and so the risk of being able to make meaningful use of the data set was unlikely.<sup>9</sup> The OPC tested this theory by reviewing a sample of the dataset and the OPC was able to organize the data into a format that allowed for identification of individuals without significant effort or time.<sup>10</sup> MGM further argued that there was no evidence of actual misuse. However, the OPC stated that “the data could have been misused in a way that MGM has not yet detected or could be misused in the future.”<sup>11</sup> Accordingly, the OPC found that the test for reporting and notification was met.

Organizations should consider establishing a written methodology for assessing risk. In addition to the OPC guidance, organizations may wish to take into account the following factors when creating a risk matrix. Factors that increase the real risk of significant harm could include:

- malicious intrusion or other evidence of criminal activity;
- inability to recover the data from unknown recipient;
- long period of exposure;
- reports of misuse by one or more affected individuals;
- credit card, banking or other similar information that could be used for fraud;
- social insurance numbers, driver’s licence numbers or other government identifiers that are often used to verify identity;
- biometric or other identifiers that are not easy to change;

#### 4. What Is the Threshold for Reporting and Individual Notification?

- passwords;
- contact information plus additional transaction or profile information that could be used to facilitate phishing; and
- health information, relationship information or other information that is intrinsically private and could be humiliating to the person.

Factors that might be indicative of a lower risk of harm might include:

- accidental disclosure to an individual who is not known to the affected individual and the information is recovered without any misuse;
- encrypted data where the encrypted key was protected and it can be proven that the encryption key was not accessible to the intruder; and
- the disclosure was purely internal, the data was recovered and the organization can use internal policies and monitoring to prevent misuse.

During the consultations on the *Breach of Security Safeguards Regulations*, many of the respondents supported a presumption in the Regulations that the risk of harm should be presumed to be low if appropriate encryption has been used. The OPC disagreed and this presumption was not included in the final Regulations. This does not mean that encryption is irrelevant to the inquiry. However, encryption is not automatically a safe harbour.

One of the many questions that the OPC has yet to address is whether unauthorized access to contact information, including email addresses, is sufficient to establish a real risk of significant harm without sensitive information also having been implicated in the breach. The answer in Alberta is that the current and former Alberta Commissioners believe that the mere loss of an email address could give rise to a real risk of significant harm at least in circumstances of a malicious attack.<sup>12</sup> In *P2011-ND-011*, the former Alberta Commissioner, Frank Work, considered this issue in the context of a malicious intrusion into Best Buy. Commissioner Work stated:

In my opinion, the foreseeability of fraud or identity theft as harms that may arise from the Epsilon breach is not mere speculation or conjecture. There is a clear cause and effect relationship between the potential harm that may arise from the Epsilon breach. Affected individuals are likely to be targeted with “spear phishing” emails which directly target them as known customers of Best Buy. It is to be hoped that most individuals will ignore these emails, particularly so in cases where they have received notification of the breach and potential risks. However, a small (it is hoped) portion of affected individuals are likely to either open attachments with malware or be tricked into providing additional information. This is the known pattern that is used by criminals when attempting to obtain personal information. Phishing attempts have been successful in the past and there is no evidence to indicate that the information obtained through the Epsilon breach will be treated any differently.<sup>13</sup>

Commissioner Work stated that his view, in this case, was informed by the magnitude of the breach and its sophistication. Although he acknowledged that there was no evidence of harm or, he believed, a way to predict whether there was harm, he concluded that “even if there is only a one in a million chance that a Best Buy customer will be misled by a spear phishing email ... at least two affected individuals in Canada would actually be affected as a result of the breach”.<sup>14</sup> This is an odd approach to assessing whether harm is speculative. However, it appears that the moment there is evidence of a malicious intrusion, the test for a real risk of significant harm will be met in Alberta.

The current Alberta Commissioner continues to double-down on this approach.<sup>15</sup> Moreover, the Alberta Commissioner has extended this reasoning to business email addresses, without any recognition that these business email addresses may already be published.<sup>16</sup> Business email addresses are generally exempted from the requirements of the Alberta statute when they are used for the purposes of enabling the individual to be contacted in relation to the individual’s business responsibilities and for no other purpose. However, the Alberta Commissioner believes that the unauthorized disclosure of the business email address brings the email address back under the provisions of the Alberta legislation.<sup>17</sup>

The decisions of the Alberta Commissioner depart from decisions of courts in class proceedings when those courts

#### 4. What Is the Threshold for Reporting and Individual Notification?




are called upon to assess the risks of a data breach to class members. For example, in *Lozanski v. Home Depot Inc.*,<sup>18</sup> the court accepted that there was “little risk that the data breach, including the disclosure of email addresses, increased the risk of identity theft, because the stolen data would have been inadequate to allow a criminal to fake another’s identity”.<sup>19</sup> The data stolen from the Home Depot did not include any government identifiers. In addition, the court noted that there was “little risk of fraudulent charges” using the credit card numbers taken from Home Depot “because of sophisticated safeguards developed by credit card companies”. In addition, the court noted that “when there are frauds, the losses are almost always absorbed by the credit card company or the retailer”.<sup>20</sup>

There is reason to believe the OPC will not take the same position. This author has been involved in cases and has heard from other advisors that the OPC has not questioned decisions not to notify even when the Alberta Commissioner came to different conclusions. However, there is no guidance on this point and so organizations should seek legal counsel. It is to be hoped that the OPC will soon provide guidance. Until then, there is a very real danger that the OPC will adopt the same short trigger for notifications (including with respect to business contact information, given the similar wording of PIPEDA), which would place Canada out of step with Europe, Australia, the United States and other countries that have adopted a harms-based threshold.


The tide may be turning. In *Setoguchi v. Uber B.V.*,<sup>21</sup> the Alberta Court considered whether to certify a class action against Uber in respect of a data breach that involved the personal information of Uber drivers. In 2016, Uber was contacted by two individuals who illegally accessed Uber data and demanded a ransom. Uber paid the hackers and secured a commitment that the data had been destroyed. However, Uber did not have any concrete evidence proving that the information had, in fact, been destroyed. It was on this basis, that the Alberta Commissioner ordered Uber to make a breach report.<sup>22</sup> However, in a subsequent class action, the Alberta Court of Queen’s Bench considered whether there was some basis in fact for claims of harm, loss or damage to sustain the class action. At the time the case was heard, there was no evidence of any driver having suffered any actual harm. However, the plaintiff argued that the affected individuals’ loss of control over their data was itself a harm. However, there was no evidence that the data was not actually destroyed. The court concluded that any harm was speculative. The Associate Chief Justice specifically held that: “I not only find no evidence of any actual harm or loss, but do find evidence of no actual harm or loss, in relation to the common law or statutory breaches, including what is called ‘significant harm’ in PIPEDA, s. 10.1(7) and (8).”<sup>23</sup> This case suggests that the burden will be on the Commissioners to establish that there is at least some evidence on which to support a finding of significant harm if an organization’s decision not to notify were to go to court.

---

#### Footnote(s)

- 1 *Personal Information Protection Act*, S.A. 2003, c. P-6.5, s. 34.1.
- 2 Office of the Information and Privacy Commissioner of Alberta, “Practice Note: Reporting a Breach to the Commissioner” (August 2018); online: [https://www.oipc.ab.ca/media/952732/Practice\\_Note\\_Reporting\\_a\\_Breach\\_Aug2018.pdf](https://www.oipc.ab.ca/media/952732/Practice_Note_Reporting_a_Breach_Aug2018.pdf) .
- 3 See Mandatory Breach Reporting Tool, Office of the Information and Privacy Commissioner of Alberta, “Practice Note: Reporting a Breach to the Commissioner” (August 2018), online: [https://www.oipc.ab.ca/media/952732/Practice\\_Note\\_Reporting\\_a\\_Breach\\_Aug2018.pdf](https://www.oipc.ab.ca/media/952732/Practice_Note_Reporting_a_Breach_Aug2018.pdf) .
- 4 Office of the Privacy Commissioner of Canada, “What you need to know about mandatory reporting of breaches of security safeguards” (October 2018), online: [https://priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd\\_pb\\_201810/](https://priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/) .
- 5 *Investigation into MGM breach highlights how to assess risk, and need for timely assessment*, [2022] C.P.C.S.F. No. 6 (Can. Priv. Comm.).
- 6 *PIPEDA Report of Findings #2022-004, Investigation into MGM breach highlights how to assess risk, and need for timely assessment*, [2022] C.P.C.S.F. No. 6 at para. 17 (Can. Priv. Comm.).

#### 4. What Is the Threshold for Reporting and Individual Notification?

- 7 *PIPEDA Report of Findings #2022-004, Investigation into MGM breach highlights how to assess risk, and need for timely assessment*, [2022] C.P.C.S.F. No. 6 at para. 18 (Can. Priv. Comm.).
- 8 *PIPEDA Report of Findings #2022-004, Investigation into MGM breach highlights how to assess risk, and need for timely assessment*, [2022] C.P.C.S.F. No. 6 at para. 22 (Can. Priv. Comm.).
- 9 *PIPEDA Report of Findings #2022-004, Investigation into MGM breach highlights how to assess risk, and need for timely assessment*, [2022] C.P.C.S.F. No. 6 at para. 24 (Can. Priv. Comm.).
- 10 *PIPEDA Report of Findings #2022-004, Investigation into MGM breach highlights how to assess risk, and need for timely assessment*, [2022] C.P.C.S.F. No. 6 at para. 25 (Can. Priv. Comm.).
- 11 *PIPEDA Report of Findings #2022-004, Investigation into MGM breach highlights how to assess risk, and need for timely assessment*, [2022] C.P.C.S.F. No. 6 at para. 26 (Can. Priv. Comm.).
- 12 *Re Best Buy Canada Ltd.* (May 11, 2011), online: <https://www.oipc.ab.ca/media/386598/P2011-ND-011-.pdf> .
- 13 *Re Best Buy Canada Ltd.* (May 11, 2011), online: <https://www.oipc.ab.ca/media/386598/P2011-ND-011-.pdf>  at para. 20.
- 14 *Re Best Buy Canada Ltd.* (May 11, 2011), online: <https://www.oipc.ab.ca/media/386598/P2011-ND-011-.pdf>  at para. 22.
- 15 See, for example, *Re Uber B.V.*, P2018-ND-030 (February 28, 2018), online: [https://www.oipc.ab.ca/media/979177/p2018\\_nd\\_030\\_007458.pdf](https://www.oipc.ab.ca/media/979177/p2018_nd_030_007458.pdf) .
- 16 For example: *Re Trisotech Computer Consulting Services Inc.*, P2018-ND-150 (November 16, 2018), online: [https://www.oipc.ab.ca/media/973364/P2018\\_ND\\_150\\_008175.pdf](https://www.oipc.ab.ca/media/973364/P2018_ND_150_008175.pdf) .
- 17 For example: *Re Trisotech Computer Consulting Services Inc.*, P2018-ND-150 (November 16, 2018), online: [https://www.oipc.ab.ca/media/973364/P2018\\_ND\\_150\\_008175.pdf](https://www.oipc.ab.ca/media/973364/P2018_ND_150_008175.pdf) .
- 18 [2016] O.J. No. 4503, 2016 ONSC 5447 (Ont. S.C.J.).
- 19 *Lozanski v. Home Depot Inc.*, [2016] O.J. No. 4503 at paras. 49-50, 2016 ONSC 5447 (Ont. S.C.J.).
- 20 *Lozanski v. Home Depot Inc.*, [2016] O.J. No. 4503 at para. 47, 2016 ONSC 5447 (Ont. S.C.J.).
- 21 [2021] A.J. No. 22, 2021 ABQB 18 (Alta. Q.B.) (“Uber”).
- 22 *Re Uber B.V.*, P2018-ND-030 (February 28, 2018), online: [https://www.oipc.ab.ca/media/979177/p2018\\_nd\\_030\\_007458.pdf](https://www.oipc.ab.ca/media/979177/p2018_nd_030_007458.pdf) .
- 23 *Setoguchi v. Uber B.V.*, [2021] A.J. No. 22 at para. 28, 2021 ABQB 18 (Alta. Q.B.).