Cassels

Personal Information – You're So Sensitive!

Bernice Karn, Courtney Wong

May 25, 2022

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) defines "personal information" simply as "information about an identifiable individual." PIPEDA also requires organizations that handle personal information to protect it with safeguards appropriate to its sensitivity. What does that mean? How does one judge the sensitivity of personal information in order to determine the appropriate measures to protect it, especially given the rapidly changing technology landscape? Unfortunately, for those seeking specific guidance on how to comply with this requirement, PIPEDA is not terribly prescriptive.

Recognizing this need for up-to-date guidance, on May 16, 2022 the Office of the Privacy Commissioner of Canada (OPC) issued an Interpretation Bulletin on the topic of sensitive personal information and its treatment under PIPEDA. This Interpretation Bulletin is not meant to act as a binding legal interpretation, but rather a summary and guide for compliance with PIPEDA.

PIPEDA discusses the concept of sensitive personal information in several provisions, summarized as follows:

- **Principle 4.3.4 – Form of Consent Required:** The form of consent required by the organization varies depending on the circumstances and type and sensitivity of information. While some information is inherently sensitive, the sensitivity of other information can depend on the context in which it is used.
- **Principle 4.7 – Security Safeguards:** All safeguards to protect personal information should be appropriate to the level of sensitivity of the information.
- **Principle 4.7.2 – Nature of Security Safeguards:** The types of safeguards used to protect personal information will vary depending on factors such as its sensitivity, amount, distribution, format, and method of storage.
- **Subsection 7.2(1)(a) – Prospective Business Transactions:** In prospective business transactions, organizations that are parties to the transaction may use and disclose personal information without knowledge or consent of the individual if, among other things, there is an agreement that requires the organization to utilize security safeguards appropriate to the sensitivity of the information.
- **Subsection 7.2(2)(a) – Completed Business Transactions:** In completed business transactions, organizations that are parties to the transaction can use and disclose personal information that was disclosed as part of the transaction without knowledge or consent of the individual if, among other things, there is an agreement that requires the parties to protect the information utilizing security safeguards appropriate to the sensitivity of the information.
- **Subsection 10.1(8) – Factors to Assess Real Risk of Significant Harm:** When assessing "real

risk of significant harm" in a breach of security safeguards, one of the factors to consider is the sensitivity of the information involved in the breach.

Application of PIPEDA by Courts and the OPC

Consistent with the European Union's concept of "special categories" of personal data under the General Data Protection Regulation,[1] according to the Interpretation Bulletin, information that is considered sensitive generally includes health and financial data, genetic and biometric data, and information about an individual's ethnic and racial origins, political opinions, sex life, sexual orientation, and religious or philosophical beliefs. However, whether something will be considered "sensitive" under PIPEDA depends on the facts of any given situation. The OPC has laid out the following principles in its guidance, based on PIPEDA case law and the OPC's own findings to date:

- **Context is important in assessment:** The purpose of PIPEDA is to strike a balance between protection of privacy and facilitating the collection, use, and disclosure of personal information by the private sector for appropriate commercial purposes.[2] However, information that is otherwise not sensitive can be deemed sensitive when connected to services that reveal preferences of its users.[3]
- **Information can become sensitive when combined with other information:** When sensitive information is used to generate non-sensitive interest categories, the underlying information must still be assessed for sensitivity.[4] The sensitivity of the combination of several forms of information can be heightened by known risk environments and data breaches, and safeguards must, therefore, by proportionately high.[5]
- **Health information as sensitive information:** Medical information is of the utmost sensitivity and requires the highest degree of protection; meaningful and express consent is required for its disclosure.[6] Biometric information, particularly facial biometric information, is sensitive in almost all circumstances.[7]
- **Financial information as sensitive information:** Financial information is generally extremely sensitive, but must be assessed in the "context of related financial information already in the public domain, the purpose served by making the related information public, and the nature of the relationship" between the parties and directly affected third parties.[8] Financial information requires heightened safeguards to protect against data breaches, and disclosure requires consent.
- **Personal information affecting an individual's reputation:** Organizations that hold personal information electronically must adopt appropriate procedures and policies to manage security risk, especially if compromised data can cause significant reputational harm.[9]
- **Security safeguards for sensitive information:** The degree and nature of security safeguards depend on the type of information that is collected. Organizations that manage large amounts of personal information must have adequate and coherent governance frameworks. The level of controls to ensure protection when processed by third parties must be proportionately high.[10]
- **Other information generally considered sensitive:** Social networking sites should not set default

user settings to “visible to all” when dealing with user profiles containing sensitive personal information.[11] Similarly, operating systems must provide for meaningful consent during installation, particularly where highly sensitive information might be collected.[12] Information revealing sexual practices, preferences and fantasies is sensitive personal information[13] as is personal information involving the collection, use and disclosure of information relating to ethnicity.[14] Sharing an email address to deliver political communications to the individual could reveal their political views, which is sensitive personal information.[15]

Conclusion and Take-Aways

PIPEDA aims to balance the protection of individuals’ privacy with the needs of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances. Will this new guidance mean that organizations now have a quick and easy way to categorize personal information as “sensitive” and strike the appropriate balance? Probably not; organizations are still going to have to go through the often difficult exercise of taking a hard look at the personal information that they are collecting and make a judgement call on whether or not it is sensitive. The challenge is that the form of consent for disclosure and required level of security safeguards will depend on the sensitivity of the information that has been collected, and that sensitivity must be addressed contextually – not an easy task. Fortunately, certain types of information such as health, financial, and biometric information can be assumed to be generally intrinsically sensitive and subject to informed consent for collection, use and disclosure as well as a higher standard for protection; however, for other types of information with a lower threshold of sensitivity, the sensitivity will be dependent on factors such as how the personal information is used and how much it reveals about an individual’s personal characteristics and lifestyle. Judging this latter category of information is more difficult and will be one of the ongoing challenges of PIPEDA compliance.

---

[1] *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[2] *Englander v Telus Communications Inc*, 2004 FCA 384 at paras 45–46. See also Office of the Privacy Commissioner, *PIPEDA Report of Findings #2012-002 – Facebook didn’t get non-members’ consent to use email addresses to suggest friends, investigation finds* (April 2012), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2012/pipeda-2012-002/>.

[3] Office of the Privacy Commissioner, *PIPEDA Report of Findings #2016-005 – Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner* (August 2016), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/>.

[4] Office of the Privacy Commissioner, *PIPEDA Report of Findings #2015-001 – Results of the Commissioner Initiated Investigation into Bell’s Relevant Ads Program* (April 2015), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2015/pipeda-2015-001/>.

[5] Office of the Privacy Commissioner, *PIPEDA Report of Findings #2020-003 – Dell improves security and complaint handling practices following breaches and OPC Investigation* (July 2020), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-003/>.

[6] *Townsend v Sun Life Financial*, 2012 FC 550 at para 38.

[7] Office of the Privacy Commissioner, *PIPEDA Report of Findings #2020-004 – Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner of British Columbia* (October 2020), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/>. See also Office of the Privacy Commissioner, *PIPEDA Report of Findings #2021-001 – Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Quebec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (February 2021), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.

[8] *RBC v Trang*, 2016 SCC 50 at para 36.

[9] *Joint investigation of Ashley Madison*, *supra* note 3.

[10] Office of the Privacy Commissioner, *PIPEDA Report of Findings #2019-001 – Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information* (April 2019), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/>.

[11] Office of the Privacy Commissioner, *PIPEDA Report of Findings #2012-001 – Social networking site for youth, Nexopia, breached Canadian privacy law* (February 2013), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2012/pipeda-2012-001/#section1>.

[12] Office of the Privacy Commissioner, *PIPEDA Report of Findings #2018-004 – Microsoft to obtain opt-in consent, enhance transparency for Windows 10 privacy settings* (June 2018), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-004/>.

[13] *Joint investigation of Ashley Madison*, *supra* note 3.

[14] Office of the Privacy Commissioner, *PIPEDA Report of Findings #2019-004 – Joint investigation of AggregateIQ Data Services Ltd. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia* (November 2019), online: OPC <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-004/>.

[15] *Ibid.*
