Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)

May 2018

On this page

Overview

Subsection 5(3) of PIPEDA is a critical gateway that either allows or prohibits organizations to collect, use and disclose personal information, depending on their purposes for doing so. It is the legal boundary that protects individuals from the inappropriate data practices of companies. It separates those legitimate information management practices that organizations may undertake in compliance with the law, from those areas in which organizations cannot venture, otherwise known as "No-go zones". In this guidance document, the Office of the Privacy Commissioner of Canada (OPC) describes the guiding principles for interpreting subsection 5(3) of PIPEDA as informed by past Court decisions, and sets out a series of no-go zones which we have determined, through past findings and extensive consultations with stakeholders and focus groups with individuals across Canada, are offside PIPEDA as viewed from the perspective of the reasonable person.

What is PIPEDA subsection 5(3)?

Subsection 5(3) of PIPEDA states:

> *An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.*

How the Courts interpret 5(3)

1. A guiding principle

Subsection 5(3) "is a guiding principle that underpins the interpretation of the various provisions of PIPEDA". [3] In turn, it must be read in light of the underlying purpose of Part 1 of PIPEDA which is to balance the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information. [4] In applying subsection 5(3), one is therefore required to engage in a "balancing of interests" between the individual and the organization concerned. [5]

2. Reasonable person lens

Subsection 5(3) requires a balancing of these interests "viewed through the eyes of a reasonable person." [6]

3. An overarching requirement

Within the scheme of PIPEDA, subsection 5(3) is "an overarching requirement" [7] that is superimposed on an organization's other obligations to ensure that their purposes for collection, use and disclosure of personal information are limited to only those which a reasonable person would consider appropriate in the circumstances.

4. Necessary but not sufficient

In order to comply with subsection 5(3), it is not enough to demonstrate compliance with the other provisions of the Act. For instance, even with consent, an organization must still show that its purposes for collecting, using or disclosing personal information in the first place are ones that a reasonable person would consider appropriate in the circumstances.

Conversely, compliance with subsection 5(3) does not automatically mean compliance with other provisions of the Act. Even if an organization's purposes are considered appropriate under subsection 5(3), it must also ensure that the Act's other requirements relating to the protection of personal information are satisfied. [8]

Evaluating an organization's purposes under 5(3)

The evaluation of subsection 5(3) requires an examination of whether the purposes are appropriate "in the circumstances." As such, the analysis must be conducted "in a contextual manner" and look at the particular facts surrounding the collection, use and disclosure, "all of which suggests flexibility and variability in accordance with the circumstances". [9] [10]

In applying subsection 5(3), the courts have generally taken into consideration whether: "1) the collection, use or disclosure of personal information is directed to a *bona fide* business interest, and 2) whether the loss of privacy is proportional to any benefit gained." [11] In *Turner v. Telus Communications Inc.* the Federal Court, in a decision affirmed by the Federal Court of Appeal, set out the following factors for evaluating whether an organization's purpose was in compliance with subsection 5(3):

- The degree of sensitivity of the personal information at issue;
- Whether the organization's purpose represents a legitimate need / *bona fide* business interest;
- Whether the collection, use and disclosure would be effective in meeting the organization's need;
- Whether there are less invasive means of achieving the same ends at comparable cost and with comparable benefits; and
- Whether the loss of privacy is proportional to the benefits. [12]

Inappropriate purposes or No-Go Zones

Based on the guiding principles and evaluative framework above, our Office's practical experience with the application of subsection 5(3) over the course of more than fifteen years of applying PIPEDA, and comments received during our consultation on consent—we have determined that the following purposes for collection, use or disclosure of personal information would generally be considered "inappropriate" by a reasonable person [13]. The following No-Go Zones are currently considered to be offside PIPEDA, and may evolve over time.

1. Collection, use or disclosure that is otherwise unlawful

Organizations should have knowledge of all regulatory and legislative requirements that may govern their activities, and individuals should be safe in the knowledge that collection, use or disclosure of their personal information will not be done for purposes that contravene the laws of Canada or its provinces. This is supported by PIPEDA Principle 4 which requires collection to be "by fair and lawful means".

For instance, the "reasonable person" would generally consider to be inappropriate any collection, use or disclosure of their personal information that would violate credit reporting legislation. In PIPEDA Report of Findings 2016-002, the OPC found that it was inappropriate for a landlord association to be operating a "bad tenant list" as by doing so, it was acting as an unlicensed credit reporting agency in violation of provincial credit reporting legislation. Similarly, in OPC's Report of Findings in respect of Bell Canada's Relevant Ads Program, we found the company's use of credit score information for the delivery of targeted ads was not permitted under Ontario's Consumer Reporting Act, and was therefore inappropriate under 5(3).

* As another example, organizations that require individuals to undergo a genetic test, or disclose the results of a genetic test, as a condition of providing good or services, or entering into a contract, will be in contravention of the *Genetic Non-Discrimination Act* of 2017. Hence, consistent with OPC's Policy statement on the use of genetic test results by life and health insurance companies, and its Guidance on Direct to Consumer Genetic Testing, requiring individuals to undergo genetic tests or provide existing genetic test results has been deemed to be a No-Go Zone.

2. Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law

In an age of big data, it is increasingly important to understand the connection between the **upstream** collections, uses and disclosures of personal information and the **downstream** discriminatory impacts thereof. [14] Data analytics—or any other type of profiling or categorization—that results in inferences being made about individuals or groups, with a view to profiling them in ways that could lead to discrimination based on prohibited grounds contrary to human rights law [15] would not be considered appropriate under subsection 5(3)'s "appropriate purpose" test.

While profiling that leads to discrimination contrary to human rights law will always be inappropriate under 5(3), determining whether a result is unfair or unethical will require a case-by-case assessment. Organizations should know, however, that unfair or unethical profiling or categorization will also generally be found inappropriate under subsection 5(3).

This is consistent with the spirit of the International Resolution on Big Data adopted by Data Protection and Privacy Commissioners around the world at their annual Conference in Mauritius in 2014, where we committed to calling on all parties to demonstrate that decisions around the use of Big Data are fair, transparent and accountable; that results from profiling be responsible, fair and ethical; and that injustice for individuals due to fully automated false positive or false negative results be avoided.

3. Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual

The digital marketplace is filled with privacy trade-offs individuals make every day in order to exercise their freedom as consumers. This includes giving up a reasonable amount of one's privacy in order to seek out convenience and choice. Individuals should be free to make their own discerning decisions of how much privacy they are willing to give up in order to obtain certain products or services.

However, the OPC believes that a reasonable person would not consider it appropriate for organizations to require an individual to undergo significant privacy harm as a known or probable cost for products or services. By "significant harm", we mean "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on (one's) credit record and damage to or loss of property". [16]

4. Publishing personal information with the intended purpose of charging individuals for its removal

OPC has written extensively about the challenges of protecting one's reputation online, and released a draft position paper on the topic. While this remains a complex issue overall, our Office has come across one practice which we clearly consider to be offside PIPEDA and that is, publishing sensitive personal information online for the primary purpose of charging individuals to have it removed. In short, we believe a reasonable person is unlikely to consider "blackmail" an appropriate purpose, and the Federal Court of Canada agreed with us when it confirmed the findings of our investigation of Globe24h.

5. Requiring passwords to social media accounts for the purpose of employee screening

PIPEDA, as amended by the *Digital Privacy Act*, protects the personal information of job applicants as well as employees of federal works, undertaking or businesses (organizations that are federally-regulated, such as banks, airlines, and telecommunications companies). Given the unequal positions of power between employer and employee (or potential employee), there is a risk that employers ask for more information than is needed to assess an individual's merit, and individuals, in turn, may feel unduly pressured to provide such information for fear of not being given the job or maintaining their employment. In some cases, employers may go overboard in requesting that employees (or potential employees) provide them with access to password-protected areas of their social media accounts. Requiring passwords in order to access private parts of social media accounts has the potential of exposing incredible amounts of highly sensitive personal information that are neither relevant nor necessary for the employers' legitimate business purposes. Many U.S. States have passed legislation prohibiting this practice. [17] The OPC agrees that requiring passwords to social media accounts for the purpose of employee screening [18] would generally not be considered appropriate by a reasonable person.

6. Surveillance by an organization through audio or video functionality of the individual's own device

Nothing can be more privacy-invasive than being tracked through the audio or video functionality of an individual's device either covertly, that is without their knowledge or consent, or even with *so-called* consent, when doing so is grossly disproportionate to the business objective sought to be achieved.

In PIPEDA Report of Findings 2013-016, the OPC found that a spyware application called "Detective Mode," used by several rent-to-own companies to covertly trace missing laptop computers resulted in surreptitious collection of keystrokes, screenshots, webcam photographs, and other information. Our Office found that the loss of privacy resulting from the use of Detective Mode in this context is vastly disproportionate to the possible benefits to be gained.

It may be permissible for the audio or video functionality of a device to regularly or constantly be turned on in order to provide a service if the individual is both fully aware and in control of this fact, and the captured information is not recorded, used, disclosed or retained except for the specific purpose of providing the service.

Conclusion

An appropriate purpose judged from the standpoint of a reasonable person is a flexible concept that requires time, careful reflection and practical experience to define. In practice, the test for appropriateness will require a contextual analysis but we find it useful—for transparency to both individual and organizations—to provide examples of our expectations, such as those listed above. It is our intention to periodically revisit and update the above list of "No-Go zones" as warranted.

Footnotes

1. *R. v. Spencer*, [2014] 2 S.C.R. 212, paragraph 63.
2. PIPEDA, s. 3; *A. T. v. Globe24h.com*, 2017 FC 114, paragraph 73 ("*Globe24h.com*").
3. *Turner v. Telus Communications Inc.*, 2005 FC 1601, ¶39, aff'd 2007 FCA 21 ("Turner"). See also *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, paragraph 129 ("Eastmond")
4. *Turner v. Telus Communications Inc.*, 2005 FC 1601, paragraph 39, aff'd 2007 FCA 21 ("*Turner*"). See also *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, paragraph 129 ("*Eastmond*").
5. *A.T. v. Globe24h.com*, 2017 FC 114, paragraph 73 ("Globe24h.com").
6. *R. v. Spencer*, [2014] 2 SCR 212, ¶63.
7. *Eastmond*, paragraph 131.
8. *Globe24h.com*, paragraph 74, citing *Turner* at para 48.
9. *Turner*, ¶48. See also *Eastmond*, ¶¶127, 177, 179-181; *Globe24h.com*, ¶74; *Penny Lane Entertainment Group v. Alberta (Information and Privacy Commissioner)*, 2009 ABQB 140, ¶¶58-61; *Leon's Furniture Limited v. Alberta (Information and Privacy Commissioner)*, 2011 ABCA 94, ¶¶58-62.
10. The OPC remains open to the possibility that in exceptional cases, information related to the described contextual factors may lead to the conclusion that a particular use would, in fact, be considered appropriate by a reasonable person, even though it falls within one of the listed no-go zone.
11. See "Privacy Upstream, Discrimination Downstream: The (Un)Intended Consequences of Data Analytics." Address by Patricia Kosseim at Reboot 18th Annual Privacy and Security Conference, February 10 2017.
12. *Canadian Human Rights Act*.
13. This is in keeping with the threshold concept of 'significant harm' as defined in subsection 10.1(7) of PIPEDA (not yet in force).
14. See e.g. Arkansas Ark. Code § 11-2-124; California Calif. Lab. Code § 980; Colorado C.R.S. 8-2-127; Connecticut Conn. Gen. Stat. § 31-40x (2015 S.B. 425, Act 16); Delaware 19 Del. Code § 709A; Illinois 820 ILCS 55/10; Louisiana La. Rev. Stat. § 51:1951 to §§ 1953 and 1955; Maine 26 M.R.S. § 616 to 619; Maryland Md. Code, Labor and Emp. Law § 3-712; Michigan MCL § 37.271-37.278; Montana Mont. Code Ann. § 39-2-307; Nebraska Neb. Rev. Stat. 48-3501 et seq.; Nevada NRS § 613.135; New Hampshire N.H. Rev. Stat. § 275:74; New Jersey N.J. Stat. § 34:6B-6; New Mexico N.M. Stat. § 50-4-34 (covers job applicants only); Oklahoma 40 Okla. Stat. § 173.2; Oregon O.R.S. § 659A.330; Rhode Island R.I. Gen. Laws § 28-56-1 to -6; Tennessee Tenn. Code §§ 50-1-1001 to -1004; Utah Code § 34-48-201 et seq.; Virginia Va. Code § 40.1-28.7:5; Washington RCW §§ 49.44.200 and 49.44.205; West Virginia W.V. Code § 21-5H-1; Wisconsin Wis. Stat. § 995.55.
15. This no-go zone has been limited to the employment screening context because this is where the practice of requiring social media passwords is known to have arisen. It should not necessarily be inferred from this that requiring passwords to social media accounts is therefore permissible in other contexts. Should this practice continue to expand inappropriately in other contexts of unequal bargaining relationship (such as landlord-lessee, for instance), we will consider making this a rule of general application.

Date modified: 2018-05-24