Privacy & What is Reasonable? OPC Inappropriate Data Practices Guidelines Are Now Being Applied.

October 18, 2018

By Catherine Lovrics and Amanda Branch

In the digital age, personal information and data is a new quasi-currency. Privacy is often the trade-off to use a digital service that is 'free' in the traditional sense. As early as 2009, the OPC recognized this trade-off, and found, for example:

> Facebook has a different business model from organizations we have looked at to date. The site is free to users but not to Facebook, which needs the revenues from advertising in order to provide the service. From that perspective, advertising is essential to the provision of the service, and persons who wish to use the service must be willing to receive a certain amount of advertising.

This view was echoed again in 2017 by the Supreme Court of Canada in Douez v. Facebook, Inc. where the court noted that "Facebook is free to join and use, but all potential users… must agree to its terms of use as part of the registration process." The business models may have evolved over the past decade, but as the Court in *Douez* pointed out, "the reality is that transactions between businesses and consumers are generally covered by non-negotiable standard form contracts presented to consumers on a "take-it-or-leave-it" basis."

In May, the Office of the Privacy Commissioner of Canada (the "**OPC**") introduced Guidance on inappropriate data practices: Interpretation and application of subsection 5(3) (the "**Inappropriate Data Practices Guidelines**"). The Guidelines interpret Subsection 5(3) of PIPEDA:

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

Applying this subsection requires a balancing of interests between the individual and the organization, and this analysis should be viewed through the eyes of a reasonable person. The OPC is of the opinion that the following purposes for collection, use or disclosure of personal information would generally be considered "inappropriate" by a reasonable person and therefore are currently considered to be offside PIPEDA.

1. **Profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law** Data analytics or other profiling/categorization that could lead to discrimination contrary to human rights law would not be considered "appropriate". Unfair or unethical results will require a case-by-case assessment; however, the OPC is of the view that these types of results will also generally be found to be inappropriate.
2. **Collection, use or disclosure for purposes that are known or likely to cause significant harm to the individual** Individuals typically understand that the digital marketplace is filled with privacy trade-offs; however, it is not appropriate for organizations to require an individual to undergo significant privacy harm as a known or probable cost for products or services. Significant harm means "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".
3. **Publishing personal information with the intended purposes of charging individuals for its removal**. "Blackmail" is not an appropriate purpose and this has previously been declared as offside to PIPEDA (see OPC investigation of Globe24h).
4. **Requiring passwords to social media accounts for the purpose of employee screening**. Requiring passwords in order to access private social media accounts may expose highly sensitive personal information that

are neither relevant nor necessary for the employers' legitimate business purposes. As a result, requiring passwords to social media accounts for the purposes of employee screening is generally not appropriate.

5. **Surveillance by an organization through audio or video functionality of the individual's own device**. Generally speaking, organizations cannot track an individual through audio or video functionality of an individual's device, either covertly or with consent in instances where doing so is grossly disproportionate to the business objectives. It may be permissible for the audio or video functionality to be turned on in order to provide a service if the individual is fully aware and in control and the captured information is not recorded, used, disclosed or retained except for the purpose of providing the service.
6. **Collection, use or disclosure that is otherwise unlawful**. Organizations should know all regulatory and legislative requirements that may govern their activities. Individuals should feel safe knowing the 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".

It is important that businesses be familiar with the Guidelines, as the OPC began applying them in July. The OPC noted that these "No-Go Zones" may evolve over time and plans to periodically revisit and update this list.

For more information, please contact our Regulatory, Advertising and Marketing Group.