David Young Law
Compliance Bulletin

June 2018

OPC's new consent guidelines top out an eventful "Privacy Spring"[1]

The release of its new *Guidelines for obtaining meaningful consent* by the OPC at the end of May[2] should be viewed as the salient development in a panoply of privacy-related news items this spring. After opening with the Facebook/Cambridge Analytica disclosures in March followed by the coming into force of the European Union's new *General Data Protection Regulation* (GDPR) on May 25, the month of June is bringing this eventful period to a close - with announcement of the federal government's *Digital and Data Transformation Consultation*[3] and the tabling of a bill in Parliament[4] providing for order-making power within the OPC and significant fines for breach of the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The *Guidelines* raise the bar distinctly for user control of personal data, focusing on the collection, use and disclosure of data in the digital economy. They follow a more than two-year review and stakeholder consultation by the OPC regarding the role and viability of consent under PIPEDA. Challenges to privacy protection and PIPEDA's consent model posed by advances in technology, including digital media, big data and artificial intelligence, provided the context.

In its report on the review, the OPC concluded that consent should remain a central tenet of our privacy framework but that the challenges as to its practicability must be met with enhanced processes, supported by active guidance and oversight by the regulators.[5]

GDPR implications

Not entirely coincidentally, the release of the *Guidelines* occurred one day before the coming into force of the GDPR, providing enhanced consent rules relative to its predecessor, the 1995 *Data Protection Directive*, and which, due to the GDPR's extended extra-territoriality rule, will now apply to many

---

[1] A version of this article was published originally on June 26, 2018 as "New OPC consent guidelines mean adjustments to privacy procedures" in *The Lawyer's Daily*, an online publication of LexisNexis Canada Inc.

[2] On May 24, 2018 the Office of the Privacy Commissioner of Canada (OPC)), together with the offices of the Information and Privacy Commissioners of Alberta and British Columbia, published two important new guidance documents - *Guidelines for obtaining meaningful consent* and *Guidance on inappropriate data practices: interpretation and application of subsection 5(3)*.

[3] As stated in the government's Press Release, "Digital innovation is essential to growing our economy …. but the government recognizes that the potential of a data-driven economy must be balanced against Canadians' right to have their data and privacy protected."

[4] Bill C-413, *An Act to amend the Personal Information Protection and Electronic Documents Act (compliance with obligations),* Private Member's Bill.

[5] With respect to inappropriate data practices, the OPC concluded that specific legislative prohibitions are not required because the "gateway" prohibition contained in section 5 (3) - against collection, use or disclosure of personal information for purposes considered by a reasonable person to be inappropriate - is robust and flexible enough to address a broad range of "no-go" situations without having to prescribe them in law.

David Young Law • Hudson's Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8
T. 416-968-6286 • M. 416-318-5521
Privacy and Regulatory Law Counsel • davidyounglaw.ca

Canadian organizations. The GDPR, together with the EU's new *e-Privacy Directive* (expected to be issued next year), will require organizations to revisit and significantly upgrade their data collection practices. It will have particular impact on digital media and the now ubiquitous technologies available for tracking, targeting and otherwise collecting digital data, both actively and passively. Procedures directed at the new EU rule adopted by organizations aiming for compliance with the GDPR likely will align closely with the *Guidelines*.[6]

Seven guiding principles for meaningful consent

The *Guidelines* articulate "Seven guiding principles for meaningful consent". They also address forms of consent - express or implied - as well as guidance for consent by children. Significantly, the *Guidelines* identify which elements of the guidance are considered requirements ("Must do") versus best practices ("Should do"), the former stated as in effect having the force of law.

The seven principles that organizations are expected to comply with are as follows.

1. *Emphasize the key elements* - While organizations must make full information about their processing of individuals' personal information readily available (such as in their privacy policies), they must place additional emphasis on the following four key elements:

    (i) identification of the personal information being collected;
    (ii) identification of the parties with whom the information is being shared;
    (iii) the purposes for which personal information is being collected - in sufficient detail and appropriate language to ensure a meaningful understanding; and
    (iv) the consequences of providing consent including any meaningful risk of harm that may result not otherwise mitigated.

2. *Allow individuals to control the level of detail they get and when they get it* - Information must be provided in manageable and easily-accessible ways, including potentially in a layered format, enabling individuals to control the detail and timing of the information provided.
3. *Provide individuals with clear options to say "yes" or "no"* - Individuals must be given a separate choice as to any consent for purposes supplementary to that necessary for providing the desired product or service and the choices must be explained clearly and be easily accessible.
4. *Be innovative and creative in designing consent processes* - Organizations are encouraged to use a variety of communications strategies – including "just-in-time" notices, interactive tools and customized mobile interfaces.
5. *Consider the consumer's perspective* - Consent processes must take into account the consumer's perspective to ensure that they are user-friendly and that the information is understandable from the point of view of the target audience. Organizations also should ensure that privacy communications are easily accessible from all devices used by their target audience.

[6] A further benefit of the guidelines may be to assist a determination that PIPEDA and the provincial private sector privacy laws will meet the GDPR's "adequate level of protection" requirement for the free flow of data between the EU and Canada.

6. *Make obtaining consent a dynamic and ongoing process* - As an organization's information processing activities evolve, they should adjust their privacy practices, including adoption of smart technologies. As well, organizations should periodically audit their practices to ensure that they continue to reflect the descriptions provided in policies and other documents.
7. *Be accountable and ready to demonstrate compliance* - Organizations should be in a position to demonstrate compliance with the law, including the *Guidelines*, and in particular that their consent processes are sufficiently understandable by their target audiences, resulting in valid and meaningful consent.

Appropriate form of consent

As a key adjunct to the principles, the *Guidelines* contain guidance regarding express versus implied consent.

As a general rule, organizations must obtain express consent when:

- the personal information is sensitive,
- its collection, use or disclosure is outside of the reasonable expectations of the person providing it, or
- that creates a meaningful risk of significant harm that is not otherwise mitigated.

The *Guidelines* recognize that the ability of children and youth to provide meaningful consent depends in a significant way on their cognitive and emotional development. Generally, the threshold age below which consent by young children requires parental consent is identified as thirteen.

"Must do"/"Should do" checklists

The guidelines conclude by providing two useful checklists indicating procedures that are required for compliance (i.e. are "legal" requirements), as opposed to simply best practices. The following are key items in the "must do" checklist:

- make full privacy information available, while giving emphasis to the four key elements;
- provide information by manageable and easily-accessible means;
- provide a clear and easily accessible choice for any consent not required for the primary transaction;
- ensure consent processes are user-friendly and understandable from a consumer perspective;
- obtain consent for significant changes to privacy practices and any new data uses;
- only collect, use or disclose information for purposes that a reasonable person would consider appropriate in the circumstances;[7]
- obtain express consent for sensitive information, unexpected uses, or where there is meaningful risk of significant harm; and
- obtain consent of a parent for children under 13 and ensure older youth are able to consent.

[7] The "reasonability" requirement stipulated by s. 5(3) of PIPEDA.

Implications of the *Guidelines*

The regulators consider a significant portion of the *Guidelines* to have the force of law and have stated that they expect them to be adopted by all organizations commencing January 1, 2019.

The rules set out in the *Guidelines*, while for the most part not unfamiliar, articulate more rigorous procedures for consent than are currently followed by many mainstream data collectors. The requirements to more explicitly highlight four key information elements, to provide information in a manageable and accessible form, and to clearly provide a yes/no choice for information uses that are not central to a transaction – to call out only some of the new requirements – will require in many cases significant adjustments to information collection and (online) tracking protocols. The arguably new requirement – to disclose significant potential risks of harm, whether financial, emotional or reputational – likely will pose a new governor on many open-ended information collection practices.

Release of the *Consent Guidelines* is the most significant development in this current very active privacy environment. While other developments – such as the GDPR – have less direct impact, or represent broader policy changes that will take a longer time to institute (e.g. the *Digital Data Consultation*), the *Guidelines* will have immediate effect and are explicit in their compliance requirements.

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.