

August 24, 2020

ARTICLE

Manufacturers of internet of things devices: guidance from the Canadian Federal Privacy Commissioner

There has been plenty written about the growth of the internet of things (IoT) market. Arguably, the global pandemic may have even crystallized the benefits of IoT solutions and pushed towards system-wide digitization across industries, communities, cities, and countries.

While there is currently no IoT specific legislation in Canada, on August 20, 2020, the Office of the Privacy Commissioner (OPC) [released privacy guidance for manufacturers of IoT devices](#). Notably, the OPC's guidance is informed by several investigations undertaken by the federal regulator and contains a list of "must do's" and "should do's" for device makers. Although the OPC guidance is specific to manufacturers of IoT devices, other IoT stakeholders that may use, collect, or disclose personal information as part of deploying IoT solutions should carefully review the regulator's guidance.

Key takeaways:

- **Regulatory compliance under existing laws:** Information collected by IoT devices ought to be carefully scrutinized. While there are technical and legal considerations around what is "personal information", the regulator notes that metadata may ultimately be considered personal information, and therefore such data handled by the business may be subject to the federal privacy legislation *Personal Information Protection and Electronic Documents Act* (PIPEDA), or provincial laws where the federal privacy legislation does not apply. In addition to privacy laws, the regulator directs the manufacturers of consumer products attention to the existing statutory obligations under the *Canada Consumer Product Safety Act* (CCPSA). For example, the CCPSA's statutory prohibitions extend to both manufacturers and importers in respect of manufacturing, importing, advertising, or selling a consumer product that "is" or "they know" is a **"danger to human health or safety"**.
- **Privacy accountability:** The regulator specifies the importance of establishing a privacy management program to allow monitoring of personal information to ensure minimum compliance under the law, including incorporating mandatory reporting of breaches of security safeguards. The regulator reminds manufacturers that the buck of responsibility over the data collected does pass on when the device is sold to a customer as long as the information continues to be used, collected, disclosed, or retained. In this regard, the regulator recommends as a best practice to perform a Privacy Impact Assessment as part of product development.
- **Be meaningful in handling information:** Handling information starts with identifying the purpose of collecting that information and then limiting the use, collection, and disclosure to that purpose. The purpose must be aligned with what a reasonable person would expect in the circumstance and reflected in the consent obtained from those whose information is being collected. The regulator makes it clear that individuals need to understand what they are consenting to for such consent to be meaningful. By drawing specific attention to the use of children's personal information with respect to smart toys and educational products (including e-learning platforms), the regulator confirms its position that at a minimum, consent must be obtained from the parents or guardians.
- **Access, accuracy, and safeguarding of information:** The regulator emphasizes that consumers have a statutory right to access their information and ensure that their information is accurate by correcting or revising such information. The regulator recommends that, as a best practice, manufacturers should provide consumers with a "user friendly" manner in which they can "permanently delete" their information, and inform them about such mechanism. Further, the regulator reminds IoT manufacturers of the importance of safeguarding the information they collect and store, but also the information collected and stored by its partners (including the information that is in transit). In respect of safeguarding information, the regulator reminds manufacturers of the obligation to employ technological safeguards to protect personal information (e.g. encryption). The regulator recommends that IoT manufacturers provide a means for the user of the device to "patch or update firmware" which is reflective of a product surveillance program that ensures that the IoT device is appropriately monitored throughout its lifecycle.

The OPC guidance serves as a reminder for the sector that while there are no IoT-specific laws in Canada, the existing regulatory framework with respect to privacy and product liability ought to be carefully reviewed to ensure compliance in the manner in which IoT solutions are manufactured, sold, and advertised in Canada. Beyond direct consumer applications, this guidance is a reminder to institutions that are purchasing IoT solutions to carefully ensure the protection of personal information that the institution may collect, use, and/or disclose as part of its push toward industry digitization.

By: [Éloïse Gratton](#), [Edona C. Vila](#), Max Jarvie

Services: [Cybersecurity](#), [Privacy & Data Protection](#), [Information Technology](#), [Technology](#), [Online Retail & E-commerce](#)

Key Contacts

Éloïse Gratton

Partner and National Leader, Privacy and Data Protection


📍 Toronto


✉ EGratton@blg.com

☎ [416.367.6225](tel:416.367.6225)

Edona C. Vila
Partner


 Toronto


 EVila@blg.com

 [416.367.6554](tel:416.367.6554)

George R. Wray
Partner

 Toronto

 GWray@blg.com

 [416.367.6354](tel:416.367.6354)