THE PRIVACY COMMISSIONER'S ANNUAL REPORT ON *THE PRIVACY ACT*

Posted on February 3, 2016

Categories: Insights, Publications

In December of 2015, the Office of the Privacy Commissioner of Canada released its 2014-2015 *Privacy Act* Annual Report to Parliament (the "Report"). The *Privacy Act* governs the handling of personal information by federal government institutions.

The Report identifies the key privacy issues that most significantly affected Canadians in 2015, including the recent development in government surveillance, data breaches in federal institutions and the privacy issues related to the use of portable storage devices.

1. Government Surveillance

The Report examined three specific bills which, according to the Commissioner, have given federal institutions "an unprecedented ability to disclose Canadians' personal information without individual knowledge and consent."[1] These are Bill C-51 (*Anti-Terrorism Act, 2015*), Bill C-13 (*Protecting Canadians from Online Crime Act*) and Bill C-44 (*An Act to amend the Canadian Security Intelligence Service Act*).

Bill C-51 includes the *Security of Canada Information Sharing Act* (the "Act")[2] that enables all Government of Canada institutions to share personal information with any of 17 specifically enumerated federal departments with a mandate related to national security – as long as the information is "relevant" to the recipient institution's mandate. The Commissioner recommended amending the Act to raise the threshold for sharing information from being "relevant" to being "necessary or proportional."

In addition, the Report raised concerns that the Act:

- sets no clear limits on how long information is to be kept;
- fails to require that information sharing be subject to written agreements;
- provides individuals no judicial recourse for improper collection, use or disclosure of their personal information; and
- lacks clear retention and destruction obligations and a proper mechanism for oversight.[3]

Similarly, the Commissioner expressed a number of concerns with Bill C-13, the *Protecting Canadians from*

Online Crime Act, which allows "public officers" to obtain a production order compelling an Internet Service Provider (ISP) to hand over personal information of the subscribers. According to the Commissioner, Bill C-13 defines public officers too broadly, which could include not just police, but "anyone from a township reeve to a fisheries officer to a mayor with lawful access to our personal information."[4] In addition, the Bill lacks a reporting mechanism to hold government responsible for the use of C-13's significant new powers.[5]

Finally, Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Acts*, gives the Canadian Security Intelligence Service ("**CSIS**") authority to operate outside Canada with greater power to share information with foreign partners. The Commissioner warns that information-sharing with foreign governments can lead to human rights violations and torture of innocent Canadian citizens, as in the case of Maher Arar.[6] One suggestion is to amend the Bill to include provisions preventing CSIS from sharing information that would result in a violation of Canada's international commitments, including Canada's obligations under the United Nations *Convention Against Torture*.

2. Focus on Data Breaches

The 2014 calendar year marked the first year in which federal institutions were required to report data breaches to the Privacy Commissioner. This mandatory reporting replaced the previous voluntary reporting regime.

Federal institutions reported a record-high number of data breaches in 2014 – a total of 256 breaches for the year, up from the 228 breaches reported in 2013.[7] Accidental disclosure constituted the largest category of data breaches, which the Commissioner describes as risk that "can often be mitigated by more rigorous procedures."[8] The following is the breakdown of the causes of data breaches:

- 73% involved accidental disclosures;
- 13% involved unauthorized access;
- 11% involved loss of data; and
- 3% involved theft of data.[9]

An example of accidental disclosure in the past year includes an incident where the Canada Revenue Agency accidentally delivered the personal information of more than 1,000 individuals and businesses to a CBC journalist. Another example involves Health Canada sending letters to more than 41,000 people across Canada in windowed envelopes that revealed the letters were related to the Marihuana Medical Access Program.

The Report calls upon institutions to proactively implement measures to prevent data breaches. This requires planning new initiatives to learn from past incidents and developing strong procedures to protect personal information.

3. Risks Associated with Portable Storage Devices ("PSDs")

The Report defined PSDs as small electronic devices which are designed to hold digital data. Such devices include laptops, tablets, smartphones and USB sticks. Since PSDs may be easily lost, misplaced or stolen, they can create significant privacy and security risks for institutions and individuals.

Following a series of data breaches involving PSDs, the Office of the Privacy Commissioner conducted a government-wide audit of federal practices concerning PSD management. The audit found that while policies, processes and controls surrounding the use of PSDs are in place, there are significant opportunities for improvement. The Commissioner found that among the audited entities:

- approximately 70% have not formally assessed the risks associated with the use of PSDs;
- over 90% do not take inventory and track all PSDs throughout their lifecycle;
- over 85% do not retain records verifying the secure destruction of data retained on surplus or defective PSDs; and
- approximately 55% have not assessed the risk to personal information resulting from unauthorized use of PSDs due to weak password controls, lack of encryption or the installation of unauthorized applications.[10]

Takeaways for Organizations

While the report related only to the *Privacy Act*, the Commissioner's commentary is valuable for both public and private organizations, as it highlights the importance of developing and implementing rigorous procedures and safeguards to protect personal information.

As the reported investigations revealed, the main cause of data breaches were accidental disclosure of personal information. To reduce the likelihood of an accidental breach, the Commissioner recommended that organizations develop risk analysis and inventory tracking mechanisms for all types of electronic devices, particularly with respect to management of PSDs. It is equally important to implement a strong breach response plan to mitigate against further risk in the aftermath of a breach.

by Mitch Koczerginski and Omeed Mousavi, Student-at-Law

[1] The Report, page 1.[ps2id id='1' target='/]

[2] *Security of Canada Information Sharing Act*, SC 2015, c 20, s 2.[ps2id id='2' target='/]

[3] The Report, page 14.[ps2id id='3' target='/]

[4] *Ibid*.[ps2id id='4' target='/]

[5] *Ibid*, page 15.[ps2id id='5' target='/]

[6] *Ibid*.[ps2id id='6' target='/]

[7] *Ibid*, page 17.[ps2id id='7' target='/]

[8] *Ibid*, page 2.[ps2id id='8' target='/]

[9] *Ibid*, page 19.[ps2id id='9' target='/]

[10] *Ibid*, page 25.[ps2id id='10' target='/]

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.