# Privacy Commissioner weighs in on Breach of Security Safeguards Regulations

Posted by Derek A. Lackey, Editor / October 11, 2017

The following is the text of the Office of the Privacy Commissioner of Canada's **Submission to Innovation, Science and Economic Development Canada October 2, 2017**


Jill Paterson
Senior Policy Analyst
Digital Policy Branch
Spectrum Information Technologies and Telecommunications (SITT) Sector
Innovation, Science and Economic Development Canada
CD Howe Building, 235 Queen Street, Room 162D
Ottawa, Ontario K1A 0H5

Dear Ms. Paterson,
Re: Breach of Security Safeguards Regulations

The Office of the Privacy Commissioner of Canada (OPC) appreciates the opportunity to provide comments on the data breach regulations published in Part 1 of theCanada Gazette, dated September 2nd2017.Footnote1
The draft regulations posted in theCanada Gazetteaddress some of the recommendations our Office made to the Department of Innovation, Science and Economic Development (ISED)Footnote2in response to their March 2016 breach discussion document.Footnote3

That said, a number of key issues recommended in our submission are absent in the regulations. We believe this may challenge the regulations ability to fully achieve the sought-after benefits to organizations, individuals and the Digital Economy.

In our view, the data breach reporting and notification regulations are a key instrument to improve security practices and consumer trust.
As a result, theOPCurges the Government to consider the following:

**Content of Breach Reports to the Privacy Commissioner**

Our Office believes that breach reports to theOPCprovide the Privacy Commissioner with information necessary to assess the quality of organizations safeguards. Without this, our Offices ability to improve security practices will be substantially hampered.

Omitting the requirement to report on the state of relevant safeguards sends a signal that prevention of breaches is less important than mitigation of breach impact after the fact.

As well, such information would give our Office the opportunity to supplement information obtained through breach records, allowing us to develop a broad understanding of the overall challenges with respect to security safeguards and breaches in the marketplace. In turn, this would support our ability to more effectively advise and guide organizations on how to improve their security practices and better protect Canadians personal information.

As recommended in our Officessubmission to the 2016ISEDdiscussion paper, we would once again urge the Government to consider that reports to the Privacy Commissioner contain an organizations assessment of the risk of harm caused by the breach.

We believe that this crucial assessment requirement should be reflected in the data breach regulations. As theRIASnotes that the proposed requirements align with those of Alberta and theEU, we would note that this type of requirement, in some fashion, can be found in both those jurisdictions.Footnote4

If the intent of the data breach regulations is indeed to align the laws in Canada with those in other jurisdictions to standardize an organizations reporting requirements and promote economic interests, as theRIASstates, our Office recommends that reports to the Privacy Commissioner should include similar assessments.

In addition to the data elements required to be reported to the Privacy Commissioner in the regulations, we refer to our 2016 submission toISEDand are of the position that these reports should include:

An assessment of the risk of harm to individuals resulting from the breach;

A list or description of third party organizations that were notified of the breach, pursuant to s. 10.2(1) ofPIPEDA, as well as Privacy Enforcement Authorities from other jurisdictions;

A description of mitigation measures that have beenor will be undertakento contain the breach and reduce or control the risk of harm to affected individuals. Knowing what measures are being taken to prevent a further breach will be helpful from our perspective; and

A description of the organizations relevant security safeguards, taking into consideration any improvements made or committed to, to protect against the risk of a similar breach reoccurring in the future.

As well, we note that theRIASsuggests that the data breach reports have broader public security benefits and will play a role in terms of a much needed repository of information on data security incidents in Canada. While we indeed support this objective, the utility of such a repository may be impacted if reports to the

Commissioner do not contain key data elements, such as the assessment of harm.

Furthermore, while theRIASsuggests that organizations can provide additional information in a report to the Privacy Commissioner if they choose to, it is unclear to what extent organizations will voluntarily report on their assessments of real risk of significant harm (RROSH) or their assessment of the types of harms.

**Record Keeping Requirements Require Clarity**

TheRIASnotes:The proposed regulations will affirm that the purpose of data breach record-keeping is to facilitate oversight by the Commissioner to ensure compliance with the requirements to report to the Commissioner and notify affected individuals of significant breaches. This in turn will encourage better data security practices by the organizations.

In order for recordkeeping to fulfill the intent identified in theRIAS, it would be important to have a set of prescribed data elements to facilitate oversight by the Privacy Commissionerandhelp organizations to approach record keeping in a consistent manner. We would like to reference our 2016 submission toISEDand are of the position that the following data elements should be recorded foranybreach:

Date or estimated date of the breach;
General description of the circumstances of the breach;
Nature of the information involved in the breach; and
Summary and conclusion of the organizations risk assessment leading to its decision whether to notify/report or not.

We also note that recordkeeping requirements have only been set for a minimum of twenty four (24) months, as opposed to five (5) years, as our Office had recommended. Part of the rationale for this retention period, as per theRIAS, is that twenty four (24) months aligns with limitations on initiating civil litigation. Our Office, though, believes that if the purpose of the regulations is to support economic interests, organizational health, and consumer trust, then reliance on a retention standard based on civil liability may overlook the benefits a slightly longer retention period will provide for companies, individuals, and the digital marketplace.

Our Office also believes that two (2) years is not a sufficient time frame to develop a wholesome assessment, as five (5) years will provide a clearer picture of how the various aspects of the breach are and have been addressed by an organization. In addition, five (5) years will allow theOPCand organizations to have a better understanding of risks this would help improve the intelligence and analytical capabilities required for theOPCto identify any systemic issues and more effectively guide organizations develop better security practices.

**Coming into Force**

While we understand that the coming into force of the regulations has not yet been determined, our Office notes thatISEDhas heard from stakeholders that this should range from six (6) to eighteen (18) months.

TheOPCunderstands that while there may indeed be an implementation window that is required, we would also note that organizations have been aware of the overall, upcoming mandatory data breach reporting and notification requirements since the updates to thePersonal Information Protection and Electronic Documents Act(PIPEDA) came into force in June 2015.

As other jurisdictions in Canada have long had data breach reporting and notification for the private sector, and the 2018 coming into force of theGDPRhas macro-level economic and political considerations, theOPCis of the view that eighteen (18) months is too long, and recommends that a shorter time period be given in order to improve the landscape for organizations and individuals and bring Canada into line globally.

**Concluding Remarks**

As mentioned in theRIAS,ISEDhas offered to work with theOPCto identify areas where guidance material is required to assist organizations in interpreting and complying with their new obligations. TheOPCappreciates this offer and looks forward to our on-going positive working relationship withISED. We believe this collaboration will be particularly helpful as guidance is developed on reports to the Privacy Commissioner, risk assessment, and record keeping.

We await the finalization of the regulations, and their imminent coming into force, and the Governments effort and commitment to improving the privacy landscape for all stakeholders in Canada.

Sincerely,
(Original signed by)
Barbara Bucknell
Director, Policy and Research

Link to OPC document