Canada's Digital Privacy Act introduces breach notification et al

Robin M. Bayley and Colin J. Bennett

August 2015

Canada's Digital Privacy Act introduces breach notification et al

Robin M. Bayley and **Colin J. Bennett** report from Canada on the new provisions including those on enforcement.

The recently passed Digital Privacy Act (Bill S-4) includes the most significant amendments to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), since it became law in 2000. Despite two mandatory parliamentary reviews, and a string of calls for reform from successive Privacy Commissioners, past attempts to amend PIPEDA have died on the order paper, even though a number of the provisions in S-4 have been carried over in similar form from previous iterations.[1] The Digital Privacy Act received Royal Assent on June 18, 2015, but some provisions, most notably breach notification, will be brought into force at an unspecified future date.

PIPEDA is Canada's main law that governs the private sector's processing of personal data. It is overseen by the Office of the Privacy Commissioner of Canada (OPC). And three provinces (Alberta, British Columbia and Quebec) have enacted "substantially similar" laws, which govern provincially regulated organisations. Other laws govern the practices of Federal and provincial governments. The legislative landscape in Canada is a complex patchwork, governed by its unique federal structure. The Digital Privacy Act adds to the patchwork. PIPEDA, not only applies to Canadian companies, but also to any organisation that collects, uses, discloses, or stores personal data in Canada for commercial purposes. The legislation, therefore, has global reach.

Overview

Provisions of the Digital Privacy Act include:

- Mandatory reporting and notification requirements for organisations that experience data security breaches, and new penalties for failure to comply
- New grounds for organisations to disclose individuals' personal information without their knowledge or consent
- New powers for the Privacy Commissioner to enter into enforceable compliance agreements with organisations, in some circumstances.

Mandatory Security Breach Notification

Under Section 10 of the Digital Privacy Act, organisations will be required to report significant breaches to the Commissioner and notify affected individuals. Further, they must record every security breach of personal information for which they are responsible, and make those records available to the Privacy Commissioner when requested. Organisations face penalties of up to $100,000 per violation.

The test for whether an organisation must report a breach to the Commissioner is if it is "reasonable in the circumstances to believe that the breach creates a real risk of significant harm to an individual." "Significant harm" is defined by a non-exhaustive list including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

In assessing the "real risk of significant harm" organisations need to assess the sensitivity of the personal information involved" and "the probability that the personal information has been, is being or will be misused". Further factors may be prescribed in regulations.

In addition, the amendments require organisations to notify affected individuals of a security breach "as soon as feasible." Notifications must be "conspicuous", provided directly to the affected individuals, if feasible, and contain "sufficient information" to allow an individual to understand the significance of the breach and to take steps to mitigate or reduce the risk of any harm to him or herself.

Less frequently reported are provisions requiring organisations to report breaches to other organisations and government institutions if the other entity can reduce the risk or mitigate harm from the breach. Further, organisation experiencing the breach may disclose personal information to the other entity to reduce risk or harm, without the individuals' consent. The amendments also give individuals the right to complain to the Commissioner about organisations' non-compliance with the new breach provisions.

Businesses and their representatives have criticised the new rules as onerous and costly, and for increasing the risk of class and other civil actions. Certainly, organisations may have to change their internal procedures to record security incidents and inform the regulator and customers of breaches. However, ethical organisations with a proper privacy governance framework should be conducting those activities in some form already, and constantly reassessing and adjusting their processes. The transparency of the notifications and record keeping, and the oversight and sanctions were deemed necessary to encourage good corporate privacy practices.

The Act introduces liability for knowingly violating the notification requirements. An organisation may be liable for fines up to $100,000 per violation. It is unclear at this time whether a "violation" will include a single incident, such as a single failure to notify all individuals, or each incident (e.g. each failure to notify each individual). Faced with the risk of this kind of liability, organisations will likely be inclined to over-report, once again leading to "breach fatigue" in consumers.

Disclosure without Consent Provisions

There are a number of amendments to PIPEDA's consent provisions. Clause 5 clarifies what it means to provide valid consent. An individual's consent to the

collection, use or disclosure of his or her personal information is valid only "if it is reasonable to expect that an individual to whom the organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." Many organisations will have to review their privacy policies and notification practices in order to meet this standard. The Privacy Commissioner has produced guidance, which although predating the amendments, should be useful.

Clauses 6 and 7 add to the exceptions in which personal information may be collected, used or disclosed without consent. Most of these provisions were found in prior bills, for example, the exception for disclosure of certain "business contact information," now defined as "any information that is used for the purpose of communicating or facilitating communication with an individual in relation to their employment". Narrowly defined non-consensual disclosures are also allowed when communicating with next of kin about an injured, ill or deceased individual, when necessary to assess, process or settle an insurance claim, in prospective merger and acquisitions type transactions, with specified notifications and safeguards, and when the information relates to the work products of employment.

By far the most controversial amendment, however, relates to the permissions to disclose individuals' personal information without their knowledge or consent, for the purpose of investigation a breach of an agreement or an actual or anticipated contravention of a federal or provincial law where it is reasonable to expect that obtaining the consent from the individual for the disclosure would compromise the investigation. These provisions need to be understood in the context of the wider debate in Canada about what is generally referred to as "warrantless disclosure" and the controversial plans to allow internet and other digital service providers to disclose personal information of subscribers to law enforcement and security agencies seeking to prevent or investigate terrorism and other crimes. As some commentators have noted, service providers can no longer use privacy legislation to protect the privacy of clients in such circumstances.

Enhanced enforcement by way of compliance agreements

While the amendments are touted as providing more tools and teeth for the Privacy Commissioner, the ombudsman model continues, and the national regulator still lacks the order making powers that its provincial counterparts enjoy.

However, the Privacy Commissioner may now, in certain circumstances, enter into compliance agreements with organisations, which can be enforced at the Federal Court. Compliance agreements may be formed when the Commissioner has reasonable grounds to believe that an organisation has or is likely to contravene the provisions of Division 1 (Protection of Personal Information) or 1.1 (Breaches of Security Safeguards), or has contravened a principle enshrined in Schedule 1 of the Act. Such agreements may contain any terms that the Commissioner considers necessary to ensure compliance with PIPEDA.

When the Commissioner believes that an organisation is not complying with the agreement, after notifying the organisation, the Commissioner can apply to the Federal Court to order the organisation to comply, and the Court may add other remedies.

Why would an organisation enter such an agreement, when it can be enforced in court? When an agreement is in place and being followed, an organisation's reputation may better withstand a contravention of PIPEDA. The Commissioner has the ability, to "name and shame" organisations it has found in contravention of PIPEDA and has exercised this in some well-publicised cases. However, the Commissioner is unlikely to do so if the organisation agrees to change its ways. Published case summaries can find a complaint "well founded and conditionally resolved", meaning that "an organisation contravened a provision of PIPEDA" but has also "committed to implementing the recommendations made by the Commissioner and demonstrating their implementation within the timeframe specified." This reflects much better on an organisation than a simple "well founded" finding, which indicates that the organisation has not undertaken to change and may be actively fighting the finding. If an organisation has been able to make changes before the finding is issued, the case is "resolved" and no compliance agreement is necessary. Previously, when an organisation did not implement the changes it had agreed to, the Commissioner was largely without recourse.

When a compliance agreement is in place, and an organisation is complying, it can avoid Federal Court. In such circumstances, the Commissioner cannot apply to the Court for a hearing (the Commissioner's sole means of enforcement) and must apply for the suspension of pending applications. However, qualifying individuals can still apply for a hearing at the Court.

Conclusions

Thus, the Digital Privacy Act is a mixed bag with many provisions that have been discussed for a number of years. Some of the provisions have been welcomed by privacy experts; others criticised. Some seem fairly minor and procedural; others potentially consequential. But none should come as a surprise for Canadian or international business. Although the provisions for mandatory data breach notification will come into effect in future, businesses would do well to examine their privacy and security governance arrangements to prepare now.

AUTHORS

Robin M. Bayley, President, Linden Consulting: RB@LindenConsult.ca and Professor Colin J. Bennett, Department of Political Science, University of Victoria. BC. Canada: cjb@uvic.ca

REFERENCE

1 A detailed analysis comparing 2014 Bill S-4 and previous versions, may be found in the Legislative Summary by Dara Lithwick, Legal and Social Affairs Division, Parliamentary Information and Research Service titled Bill S-4: An Act to amend the Personal Information Protection and Electronic Documents Act and to make a consequential amendment to another Act, Publication No. 41-2-S4-E 11 June 2014, ©Library of Parliament, Ottawa, Canada, 2014, found at: http://www.parl.gc.ca/Content/LOP/LegislativeSummaries/41/2/s4-e.pdf

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

The role and current priorities of Ireland's DP Commissioner

Helen Dixon, Ireland's new Data Protection Commissioner, on 6 July, gave *PL&B*'s 28th Annual International Conference insights into her role and priorities.

I took up office in the autumn of 2014 following the retirement of the highly respected Billy Hawkes who had served as Commissioner for Ireland for almost 10 years. As you might expect, I set about assessing the organisational structure over which I now have management responsibility, the legislation from which I derive my powers and the European and international context in which the

Continued on p.3

ECJ to decide on territorial scope of EU DP Directive

Hungary's Weltimmo case has great importance in the context of the EU DP Regulation, and fears of forum shopping under the One-Stop-Shop. By **Andrea Klára Soós**.

Advocate General, Pedro Cruz Villalón, recently published his opinion[1] on the so-called Weltimmo case. This European Court of Justice (now renamed the Court of Justice of the European Union) case is expected to be a very important decision regarding the interpretation of the territorial scope of the Directive[2]. The Advocate General recommended the ECJ to adopt a decision

Continued on p.5

Issue 136 **August 2015**

INTERNATIONAL report

ISSUE NO 136 AUGUST 2015

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

REPORT SUBSCRIPTIONS
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS
Robin Bayley
Linden Consulting, British Colombia, Canada
Marcus Belke
2B Advice, Germany
Colin Bennett
University of Victoria, British Colombia, Canada
Oliver Butler
PL&B Correspondent
Helen Dixon
Data Protection Commissioner, Ireland
Scott Livingston
American Lawyer specialising in Chinese technology and data privacy law
Lisa Peets & Ezra Steinhardt
Covington & Burling LLP UK
Lyndsey Shaw
PL&B Correspondent
Andrea Klára Soós
Soos law firm, Hungary

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Email: info@privacylaws.com
Website: www.privacylaws.com
Subscriptions: The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X

comment

DPAs' roles being redefined

It is clear that national Data Protection Authorities' (DPA) roles and functions will be formulated not just by the future EU Regulation, but also as a result of EU case law. The Court of Justice of the European Union (formerly the European Court of Justice) is now considering: the Hungarian case of Weltimmo on the jurisdiction of the national DPA (p.1); the Netherlands case on the discretion of national DPAs to choose their priorities (p.18); and the case brought by Max Schrems on whether Ireland's decision not to investigate an international transfer is legitimate.

The EU bodies have started Trilogue negotiations on the draft DP Regulation (p.10). International transfers were being negotiated in the Trilogue in July, but the process lacks transparency.

In the meantime, the EU and US are still busy over talks on trade agreements (p.22); the EU view is that EU DP rules cannot be overlooked. The US-EU Safe Harbor revision, which started back in 2013 (p.14), has still not been finished – but maybe we are into the final stretch?

Ireland's new DP Commissioner, Helen Dixon, writes about her role and the increased resources she has been allocated by the government (p.1). But all DPAs will need better resources to cope with the increased workload that looms under the new EU regime, as the UK Information Commissioner has been strongly advocating.

Germany is still keen to see mandatory Data Protection Officers in the EU DP Regulation, and this view is supported by a recent survey among current German DPOs (p.20). Also in this issue we look at how DP compliance works in France and the Netherlands (p.18). While different methods are used, most DPAs in the EU are getting stricter and enforcing their DP laws more effectively than before.

PL&B's Asia Pacific Editor, Graham Greenleaf, evaluates the type of contribution the newly appointed UN Special Rapporteur on Privacy could make towards harmonising global data protection laws (p.7), and analyses, together with Scott Livingston, tort liability for online privacy violations in China (p.24). Also, the question of balancing between DP and other EU Treaty objectives is discussed on p.28.

Elsewhere, new legislation has been prepared. Our correspondents review Canada's Digital Privacy Act (p.12). Bermuda has drafted a data protection law that follows the European model, a move motivated by commercial factors, and now open for consultation until 17 August (p.23).

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 100+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access
You will be sent the PDF version of the new issue on the day of publication. You will also be able to access the issue via the website. You may choose to receive one printed copy of each Report.

3. E-Mail Updates
E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues
Access all the *PL&B International Report* back issues since 1987.

5. Special Reports
Access *PL&B* special reports on Data Privacy Laws in 100+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation
Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service
Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

"*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Chief Privacy Officer, BT Retail, UK**"

Subscription Fees

Single User Access

International Edition **£500 + VAT***

UK Edition **£400 + VAT***

UK & International Combined Edition **£800 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-4 or 5-25 users – see website for details.

Subscription Discounts

Special charity and academic rate:
50% discount on all prices. Use HPSUB when subscribing.

Number of years:
2 (10% discount) or 3 (15% discount) year subscriptions.

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.
www.privacylaws.com/UK