David Young Law
Compliance Bulletin
May 2017

Review of PIPEDA by the House of Commons Standing Committee on Access to Information, Privacy and Ethics

David Young

On April 4, 2017 I was invited to speak to the House of Commons Standing Committee on Access to Information, Privacy and Ethics ("ETHI Committee") in connection with its current study of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), the second statutory review of the legislation.

The Committee's review of PIPEDA is taking place at a particularly apt time. Issues surrounding privacy and responses to those issues are very top of mind in today's digitally-oriented world.

In my testimony before the Committee, I addressed two issues – consent and the enforcement framework. I also prepared a written Submission to the Committee in which I addressed the issues of alignment with the European Union's new privacy rule, the *General Data Protection Regulation*[1] (the "GDPR"), as well as the right to be forgotten. Following my attendance at the Committee, I provided a Supplementary Submission expanding my comments on the enforcement model.

I believe that PIPEDA has stood the test of time and does not require major revisions. However given the frequently-heard call to enhance enforcement powers, I offered some suggestions as to how this could be done, while retaining the investigative/ombudsperson model under which the Office of the Privacy Commissioner operates now.

The following is an edited version of my comments to the Committee.

The Issue of Consent

Consent is the key precept of Canada's private sector privacy laws. It says that individuals have the right to control the collection, use or disclosure of their personal information, subject to limited exceptions.

My basic view is that the current PIPEDA consent rule should not be adjusted or qualified *in the statute*, with the understanding that its application to evolving contexts will be elaborated through practice - responding to the ever-changing realities of information use. It would be very difficult in an amendment to PIPEDA to try to anticipate the precise going-forward needs and dictates of a fast-changing digital world.

[1] Adopted April 27, 2016; to come into force May 25, 2018.

The Office of the Privacy Commissioner's current consultation on consent is a timely undertaking. The results of this consultation should enable the OPC to provide guidance and develop principles to ensure that consent continues to operate effectively as the key rule in PIPEDA. These principles will be reflected also in the OPC's decisions and ultimately may be recognized as binding "law" as issues rise up to the level of court decisions. It should be noted that the courts – including the Supreme Court of Canada – have considered issues of consent and have made clear that it is inherently subject to important qualifications, including the right to freedom of expression[2] and a reasonable application of the role of implied consent.[3]

In today's digital world, individuals may provide their personal information in a variety of media without the thought that it may be collected by third parties and used for purposes that they did not contemplate. Furthermore, there is now a massive infrastructure that collects and aggregates our personal information from diverse sources, often without our knowledge. The end-result is "Big Data". The information marshalled in this manner can be used to compile detailed profiles about us for the purpose of targeted marketing. However, if it falls into the wrong hands, it also can be used for more nefarious purposes such as fraud or extortion.

Some of the adjustments to the consent rule that have been suggested would weaken its rigour and, potentially, open up the scope for much more extensive collection of personal information than exists today. This, I believe, is what the Privacy Commissioner's consultation is likely to conclude. Also, any such weakening could threaten PIPEDA's adequacy status under the European Union's GDPR.

In my view, PIPEDA's current consent rule is flexible enough to respond to the needs of evolving information practices and innovation – and should be maintained in its current form. The key objective is to ensure that individuals continue to have the right to control and protect their personal information.

The Enforcement Model

There has been much discussion about enhancing the enforcement powers available to the Privacy Commissioner. As we know, the Commissioner's role currently is that of an ombudsperson – PIPEDA's remedial provisions direct him to investigate and deliver reports on complaints made to his Office. These requirements currently do not include any authority to order an organization to take remedial actions.

I believe that his authority, as exercised through this mechanism, has been very effective. The Commissioner *does* exercise what in effect are order-making powers through his authority to make findings, audit organizations, and make recommendations, and – as will be available under the recent

[2] *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401,* 2013 SCC 62, [2013] 3 SCR 733, 2013 SCC 62

[3] *Royal Bank of Canada v. Phat Trang, Phuong Trang a.k.a. Phuong Thi Trang, et al.*, SCC 2016 50

amendments to PIPEDA[4] – to enter into and enforce compliance agreements. Furthermore, the Commissioner has the power to publicize privacy transgressions and name offending parties. This is essentially the model that has been used by the provincial privacy regulators, with the exception of a formal order-making authority. In terms of effective enforcement, the model is working well.

All this being said, if it is determined that the current model does not provide sufficient enforcement tools, I believe that it would be possible to supplement the Commissioner's existing powers with an authority to make binding recommendations – in other words, orders. This authority should not undermine the framework of the Commissioner's complaint resolution role – which in its essence is compliance-oriented.

A further proposal mentioned is to provide the Commissioner with a power to impose fines or "administrative monetary penalties". This power exists under the provincial privacy jurisdictions and around the world.

Firstly, I would note that PIPEDA currently *does* include provision for fines which, once the current amendments come into force, will include, a failure, knowingly, to report a breach or to keep records of breaches. Secondly, none of the provincial private sector privacy laws contain a provision permitting *the regulator* to impose a fine or monetary penalty. What some of them do is to provide for an offence for non-compliance with the substantive privacy requirements, punishable by a fine. Prosecution of the offence is the responsibility of the law enforcement authorities. The Alberta private sector privacy law[5] is an example of such a law. That law also provides a defence if the person acted reasonably in the circumstances. In other words, the offence requires some degree of fault, which could be characterized as "acting unreasonably". The pending PIPEDA offences require "knowledge" of a contravention – in other words, not inadvertent – which also may be characterized as a degree of fault.

The international sphere is different and we are aware that in Europe for example the regulators have the power to impose financial penalties and have done so for privacy breaches, in some instances in the millions of dollars.

Canada does have experience with legislation imposing such financial penalties, specifically the *Competition Act* and Canada's Anti-Spam Legislation. I suggest that to date, our experience in the privacy area does not equate to the type of transgressions sought to be addressed under those laws.

Providing the Privacy Commissioner with the power to impose financial penalties would be a dramatic departure from his existing authority and would not be consistent with an ombudsperson model. However, if deemed appropriate, it would be possible to supplement the current PIPEDA offence

[4] The work undertaken in the first review of PIPEDA resulted in the amendments contained in the *Digital Privacy Act*, passed in 2015, a portion of which (the breach reporting rules) are not expected to come into force until either later this year or January 2018.
[5] *Personal Information Protection Act*, S.A. 2003 c.P-6.5, section 59.

provisions to include financial penalties for matters such as an intentional, knowing, breach of the law, or a clear failure to act in a reasonable manner with regard to privacy compliance. Such provision would not be inconsistent with the pending offences for knowingly failing to comply with the breach reporting and breach record-keeping requirements.

As a final note, I agree that reference to the new EU privacy rule (GDPR) should be included in the Committee's study. However, as it stands today, significant changes to PIPEDA to respond to the GDPR would be premature. A more precise view may be revealed going forward as we have more experience with the GDPR and its trans-border adequacy review process. With the GDPR's *added focus on law enforcement and national security agencies*, adjustments may be required to enhance protective mechanisms regarding access to databases by such bodies.

Conclusion

In the early days of PIPEDA, I heard many criticisms that the law was not well-oriented to clear legal guidance since it relied on principles as opposed to prescriptive rules – based as it is on a code intended originally for voluntary compliance. However, the law has clearly stood the test of time and in my view its unusual origin provides it with the flexibility to respond to the constantly changing needs of technology and the digital environment of today. This understanding colours very much my view as to what amendments should be considered in this current review.

Specifically, the consent rule should be maintained without formal adjustment, recognizing that evolution of the rule will occur through practice, regulatory guidance and interpretation by the courts. Enforcement by the OPC has been very effective and, in my view, does not require significant new powers. However if deemed necessary, considerations for extending the Office's mandatory powers within the existing compliance-oriented model could be evaluated, including an order-making power and an appropriately-framed offence for breach of the substantive privacy provisions of the law.

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.