David Young Law

Review of the *Personal Information Protection and Electronics Documents Act*

Submission to the Standing Committee on Access to Information, Privacy and Ethics

David Young

Principal, David Young Law

April 2017

Hudson's Bay Centre, Suite 3500, 2 Bloor Street East, Toronto, ON M4W 1A8
T. 416-968-6286 • M. 416-318-5521
davidyounglaw.ca

Introduction

Thank you for the invitation to appear before the Committee and to present my views in connection with your study of the *Personal Information Protection and Electronic Documents Act* ("PIPEDA").

I have been advising on privacy law matters since prior to PIPEDA's enactment. I have had the opportunity to participate in the work of the Canadian Bar Association's National Privacy and Access Law Section in making submissions both to government and this Committee regarding the previous review and eventual amendment of the law, as well the current review. However the views expressed here are my own and do not represent necessarily the views of the CBA.

As a lawyer who advocates for laws that respond to changing circumstances, I am very pleased to see the focused study of PIPEDA by this Committee, as well as its study of the parallel, public-sector, statute, the *Privacy Act*. This review of PIPEDA is taking place at a particularly apt - and arguably momentous - time. Issues surrounding privacy and responses to those issues are very top of mind in today's digitally-oriented world. Non-exhaustively, we can identify:

- consent and an individual's right to control their information
- digital and online privacy
- effective enforcement
- security
- alignment with other laws internationally.

In this submission, I propose to address specifically issues of consent (particularly, in the context of digital data), enforcement, and alignment with other laws, specifically the European Union's *General Data Protection Regulation*[1] (the "GDPR").

How PIPEDA came to be and why it still responds

It is instructive to recall the background surrounding PIPEDA as it was enacted in April 2000 and why that occurred. This new legislation was very much a product of two important events. Firstly, in 1995, the European Union passed its *Data Protection Directive* – one of the first comprehensive private sector privacy laws anywhere[2]. Secondly, as we know, the latter part of the 1990s saw the original "tech boom", and that wondrous "new" communications channel – the Internet – characterized at the time as the "Information Highway". While Canada eventually might have adopted a comprehensive privacy law without the incentive of these two circumstances, it was very clear that the government wanted to ensure that the channels for economic exchange with Europe would not be closed by the EU Directive and furthermore, that Canada should be proactive in responding to the opportunities of the Information Highway. The need to respond to the looming potential of digital data very much drilled down to the

[1] Adopted April 27, 2016.
[2] Of note, Quebec's 1993 Private Sector Privacy Act (*An Act Respecting the Protection of Personal Information in the Private Sector)* preceded both the Directive and PIPEDA and ultimately was deemed to satisfy both the "adequate level of protection" requirement of the Directive as well as PIPEDA's "substantially similar" requirement.

protection of privacy, a precept that had been recognized twenty years earlier in the OECD's 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [3].

The government needed an expeditious way respond to these dictates and instead of trying to write a comprehensive law containing detailed substantive privacy rules, looked to the Canadian Standards Association's *Model Code for the Protection of Personal Information*, which had been developed and published in 1996 as a voluntary industry guidance document. It was the product of extensive consultation, overseen by the CSA, among representatives of industry, government and civil society as well as the relatively few experts who had focused on the issue of protecting personal information in the private sector. The public-sector privacy laws predated this exercise by at least a decade. The result was a statute that, in its substantive rules, was not particularly prescriptive. When you read Schedule 1 to PIPEDA (the CSA Code) you see that it consists of ten very shortly stated Principles each followed by a series of subsidiary rules intended to provide guidance for operational compliance.

As a lawyer studying the new law and its compliance requirements, I listened to many criticisms from both the privacy and technology perspectives that PIPEDA was badly written and in particular that it was not well-oriented to clear legal guidance since it relied on principles as opposed to prescriptive rules, within a code intended only 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 fast-moving digital and social media environment of today. This understanding colours very much my view as to what amendments should be considered in this current review.

Consent

It is apt for the Committee to be studying the important issue of consent. Consent is, in my view, the key precept of Canada's private sector privacy laws. What it says is that an individual has the right to control not only the collection but also any use or disclosure of their personal information, subject to specifically defined exceptions such as emergencies, law enforcement and legal procedure. For this reason, any adjustment to, or qualification of, the consent rule must be considered very carefully. Furthermore, as I point below, any lessening of the rigour of PIPEDA's consent requirements could have implications for the goal of aligning with the EU's new privacy rule.

My basic view is that the current articulation of the consent rule in PIPEDA should not be adjusted or qualified in the statute, with the understanding that its application to evolving contexts, particularly in the digital world, will be elaborated through practice in response to the ever-changing realities of information use. In this regard, I believe that 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 meaningful consent continues to operate effectively in all its potential applications. These results will I believe be reflected in published guidance from the OPC and, going forward, in its reported decisions and also should become part of the "law" as issues rise up to the level of court decisions. In this regard, an important facet of our evolving privacy law is that the courts – meaning ultimately 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

[3] *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, The Organization for Economic Co-Operation and Development, last modified 5 January 1999.

to freedom of expression and a reasonable application of the role of implied consent (see: *Alberta Information and Privacy Commissioner v. UFCW*[4]; *Royal Bank of Canada v. Trang*[5]).

The challenges that the consent rule poses in the digital world are two-fold. Firstly, individuals may provide their personal information in a variety of media – such as Facebook postings – without the thought that it may be collected by third parties and used for purposes that they did not contemplate when they posted it. Secondly, there is now a massive technology infrastructure that collects and aggregates personal information of individuals either without their knowledge or if they are aware of it, without their appreciating the full scope of potential "secondary uses" for their information (meaning primarily, marketing uses). As an example of this technology, passive cookies used on many web sites collect and feed back to third party aggregators information about visitors including their likes and dislikes as well as sensitive financial and health information. This information is used to compile detailed profiles of individuals for the purposes of targeting them with promotional marketing pitches – which can be a bit "creepy" if the pitch reveals information that the individual believed was private.

One argument in favor of adjusting the consent rule to reflect these realities suggests that the rule should be revised to be simply a requirement for notice and, if an individual objects to the proposed collection, a right to "opt out" (or more realistically, a proposed *use*, since the collection likely has already occurred). An elaboration of this rule would state that for "sensitive data" clear express or opt-in consent would be required, but otherwise not require consent.

Another proposal for adjusting the consent rule is to create "no-go zones" for which consent would be required, with the understanding that all other collection and use of personal information would not require consent. Presumably, no-go zones would include sensitive information such as personal health information and sensitive financial information.

A further proposal for adjusting the consent rule is to expand the definition of "publicly available information" for which consent would not be required.

In the consent discussions, there also has been mention of the "legitimate purposes" caveat to the GDPR's consent rule – within which consent would not be required. However, an analysis of what these purposes are indicates that they encompass simply what we know as implied consent plus uses for market research (not resulting in individual commercial targeting) and the very limited use for direct marketing to existing customers (an exception specifically enabled in CASL, our new anti-spam law[6]).

I believe strongly that PIPEDA's current consent rule, which includes, under the CSA Code, an important scope for implied consent, should be maintained in order to ensure that individuals continue to have the right to control their personal information, and that the rule is flexible enough to respond to the needs of evolving information practices and innovation. The adjustments to the 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. Furthermore, I believe that it would be very difficult to try to articulate the precise

---

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

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

[6] Canada's Anti-Spam Legislation

going-forward needs and mechanics of any adjustment in an amendment to PIPEDA to somehow anticipate the dictates of the fast-changing digital world. Additionally, as noted, any change in the direction of watering down the consent rule would put at risk our ability to comply with the adequacy requirements of the GDPR.

Enforcement model

There has been much discussion about enhancing the enforcement powers available to the Privacy Commissioner under PIPEDA. As we know, the Commissioner's role currently is that of an ombudsperson – reflected in PIPEDA's remedial provisions, which direct him to investigate and deliver a report 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. It should be understood that the Commissioner does exercise what in effect are order-making powers through his authority to make findings, to audit organizations, and to make recommendations and (as will be available under the recent amendments to PIPEDA[7]) to enter into and enforce compliance agreements. Furthermore, as we know, the Commissioner has the power to publicize privacy transgressions and name offending parties. In a world where reputation counts for everything, that power is a very strong one. As a result, very few, if any, organizations that have been the subject of an OPC investigation or audit, when all is said and done, have failed to address substantively the Commissioner's recommendations. This is essentially the model that has been used by the provincial privacy regulators, with the exception of a formal order-making authority. I believe that 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 – i.e. orders – regarding required compliance. This authority should not undermine the framework of the Commissioner's complaint resolution role – which in essence is compliance-oriented. While we have perceived that role as one of ombudsperson, it might be characterized alternatively as investigative and determinative, with significant compliance levers.

A further proposal mentioned is to provide the Commissioner with a power to impose fines or "administrative monetary penalties". You have heard that this power exists elsewhere in Canada and around the world.

Firstly, it should be understood that PIPEDA currently includes provision for fines which, once the current amendments come into force, will include failure to report a breach and to keep records of all breaches. Secondly, it should also be understood that none of the provincial private sector privacy laws, or the health information laws, contain a provision permitting the regulator to impose a fine or monetary penalty. What some of them do – and the Alberta private sector law[8] is an example – is to provide for an offence punishable by a fine for *intentionally* breaching the legislation (i.e. the substantive compliance requirements). The procedure for prosecuting such an offence is the

[7] 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.

[8] *Personal Information Protection Act*, S.A. 2003 c.P-6.5

responsibility of the law enforcement authorities in a province (e.g. the Attorney General). 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, to my knowledge, what were privacy breaches such as misuse of personal information, imposing in some instances fines in the millions of dollars.

Canada does have experience with legislation imposing such financial penalties, specifically the *Competition Act* and CASL. However 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, and the experience of our provincial privacy jurisdictions in regard to financial penalties supports this conclusion.

Providing the Privacy Commissioner with the power to impose financial penalties would be a dramatic departure from his existing authority and, I believe, would not be consistent with an ombudsperson model. However, if deemed appropriate, it would be possible to supplement the current PIPEDA offence provisions to address matters that could be subject of financial penalties. An example could be an intentional, overt breach of the law, involving complete failure to meet appropriately-framed due diligence requirements. Such provision would not be inconsistent with the pending offence for failure to comply with breach reporting requirements.

Meeting the GDPR's adequacy requirement

It is interesting to note – and not entirely coincidental – that one of the major issues being considered in the current review is the need to comply with the "adequate protection" requirement in the European Union's GDPR – the second generation of the 1995 *Data Protection Directive*. As noted above, satisfying the adequacy requirement in the Directive was one of the two main drivers for enacting PIPEDA almost 20 years ago. Clearly, Canada wants to retain its status as a country determined to satisfy this requirement under the GDPR.

While the GDPR contains a number of provisions that increase the rigour of protection, a substantial portion of the changes relative to the Directive focus on procedural and compliance process matters. Consent is still very much a core concept notwithstanding, as pointed out above, the caveat permitting use without consent for "legitimate purposes".

You will have heard reference to the GDPR's inclusion of a new "right to be forgotten" which expressed as such currently does not exist under PIPEDA. A close examination of the new right shows that it is largely a codification of the judge-made law[9] and acknowledges exceptions such as would be recognized under any articulation of the right in Canada, including the right to freedom of expression. In my view, it is not at all clear that PIPEDA does not include a right to be forgotten. Shortly, the Supreme Court of Canada will be asked to rule on this question in two cases[10]. I would argue that it is premature, and quite possibly not needed, to amend PIPEDA to include the right to be forgotten solely for the reason of meeting a perceived need to meet the EU's adequacy requirement.

More globally, it is appropriate and timely as part of this review to have reference to the need to meet the GDPR's adequacy requirement. I believe that an analysis of the GDPR will not reveal that in its substantive requirements it is dramatically different from the *Data Protection Directive* or that Canada

[9] *Google Spain v. Data Protection Agency (Spain),* European Union Court of Justice (May 13, 2014)
[10] *Equustek Solutions v. Google*, 2015 BCCA 265; *A.T. v. Globe24h.com*, 2017 FC 114

needs to consider major changes to PIPEDA in order to meet these requirements. The language of PIPEDA, while reflecting the principles of the 1995 Directive, does not include expressly all of the substantive rules of the Directive and yet the adequacy test was satisfied.

In terms of adequacy of protection, the more challenging issue to address will be satisfying the Europeans that our national security and law enforcement rules contain sufficient protection for individual privacy so as not to undermine the basic rights provided in the private sector laws. The GDPR's adequacy rule[11] differs significantly from the rule under the Directive in that it requires consideration of public and national security and criminal law and the access by public authorities to personal data. It was the law enforcement issue that led to the European Union Court of Justice decision[12] concluding that the EU-U.S. "Safe Harbor" protocol (adopted to satisfy the adequacy requirements since the U.S. has no general private sector privacy legislation) was invalid, which in turn led to a new protocol, the "Privacy Shield" to address this deficiency. The Privacy Shield has not yet been ruled as satisfying the adequacy requirement under the GDPR.

With respect to the considerations potentially on the table regarding adjusting PIPEDA's consent requirement, I believe that any lessening of the rigour of that requirement or expanding exceptions to the rule must be carefully considered to ensure that they do not undermine meeting the EU adequacy requirements. As I have stated above, I believe that PIPEDA's consent rule as currently provided and as has been and likely will continue to be interpreted by the courts is appropriate and flexible enough to respond to the changing realities of our social and economic environments, and that no qualification or amendment to that rule is necessary.

Conclusion

In conclusion, I submit that PIPEDA, as enacted and in its subsequent application through stakeholder compliance, enforcement by the Office of the Privacy Commissioner and interpretation by the courts, has and will continue to show that it is a very adaptive and flexible statute that does not require major adjustments to respond to the constantly evolving modern information idioms.

Specifically, the consent rule should be maintained without formal adjustment, recognizing that evolution of the rule will occur through practice and regulatory guidance. 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. 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 adequacy review process. Adjustments may be required in relation to the access rights of law enforcement authorities and national security agencies.

[11] GDPR, Article 45.

[12] *Maximillian Schrems v. Data Protection Commissioner*, Case 362-14

David Young – Short Biography

David Young is Principal at David Young Law, a privacy and regulatory law counsel practice. The practice focuses on regulatory law with an emphasis on privacy, security, product marketing and organizational compliance. His privacy expertise includes electronic data sharing networks, outsourcing relationships, data breach, anti-spam, access to information, organizational procedures, and related matters in both the private and public sectors.

David has been advising clients on marketing and related regulatory matters since the 1980's and on privacy issues from prior to the enactment of Canada's private sector privacy laws. He is the 2015 recipient of the Ontario Bar Association's Karen Spector Memorial Award for Excellence in Privacy Law.

David is a past Chair of the Canadian Bar Association's National Privacy and Access Law Section (2007-2008) and was a Co-chair of its 2015 6th Annual Access to Information and Privacy Law Symposium. David is a member of the Canadian Marketing Association's Ethics and Privacy Committee.

David is a co-author of *Canadian Advertising and Marketing Law*, published by Carswell.