CCCA
ACCJE
Canadian Corporate Counsel Association
Association canadienne des conseillers (ères) juridiques d'entreprises

THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN
INFLUENCE. LEADERSHIP. PROTECTION.

Personal Information Protection and Electronic Documents Act (PIPEDA)

CANADIAN BAR ASSOCIATION
PRIVACY AND ACCESS LAW SECTION AND
CANADIAN CORPORATE COUNSEL ASSOCIATION
March 2017

500-865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
tel/tél : 613.237.2925 | **toll free/sans frais** : 1.800.267.8860 | **fax/téléc :** 613.237.0185 | info@cba.org | **www.cba.org**

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the Canadian Corporate Counsel Association and the Privacy and Access Law Section, both of the CBA, with assistance from the Legislation and Law Reform Directorate at the CBA office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the CBA Privacy and Access Law Section and Canadian Corporate Counsel Association.

TABLE OF CONTENTS

Personal Information Protection and Electronic Documents Act (PIPEDA)

Personal Information Protection and Electronic Documents Act (PIPEDA)

I. INTRODUCTION

The Canadian Corporate Counsel Association and the Canadian Bar Association Privacy and Access Law Section (the CBA Sections) appreciate the opportunity to comment on the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The Canadian Bar Association is a national association representing approximately 36,000 jurists across Canada, including lawyers, notaries, law teachers and students, and its primary objectives include improvements in the law and the administration of justice. The CBA Sections comprise lawyers with in-depth knowledge in privacy law and access to information. The CBA Section members include lawyers in private practice, and in-house counsel working for public and private companies, not-for-profit associations, government and regulatory boards, Crown corporations, municipalities, hospitals, post-secondary institutions and school boards.

We have made numerous submissions on PIPEDA since its enactment, including our most recent submissions, Consent Model for Collection of Personal Information under PIPEDA (July 2016), PIPEDA Data Breach Notification and Reporting Regulations (May 2016), Bill S-4 – *Digital Privacy Act* (February 2015) and Review of PIPEDA (August 2009).[1]

The CBA Sections generally support maintaining the existing consent and ombudsperson models in PIPEDA in the absence of a compelling need for legislative change, while carefully monitoring Canada's European Union (EU) adequacy status. Within these existing models, PIPEDA and its regulations should be amended to update the concept of publicly available information, to ensure they are technology neutral, and to allow the Office of the Privacy Commissioner of Canada (OPC) to issue non-binding advance opinions. Our comments focus

---

1 *See* Canadian Bar Association, *Consent Model for Collection of Personal Information under PIPEDA* (July, 2016), available online (http://ow.ly/IhZt30a9kPV). *See also* Canadian Bar Association, *PIPEDA Data Breach Notification and Reporting Regulations* (May, 2016), available online (http://ow.ly/pTZR30a9l07). *See also* Canadian Bar Association, *Bill S-4 — Digital Privacy Act* (February, 2015), available online (http://ow.ly/xMvF30a9l4D). *See also* Canadian Bar Association, Review of the Personal Information Protection and Electronic Documents Act (PIPEDA) (August, 2009), available online (http://ow.ly/vW9Z30a9lp1).

on consent, the right to be forgotten, order making powers, non-binding advance opinions, public availability and public information, as well as adequacy.

II. CONSENT

PIPEDA is consent-based, requiring an individual's knowledge and consent for an organization to collect, use and disclose their personal information.[2] This model continues to work well for Canadians and organizations operating in Canada. It has proven to be flexible in adapting to rapidly evolving technologies (including the internet and "big data"), business practices and individual privacy expectations.

Privacy is not an inviolable right – it is a right read into section 7 of the *Canadian Charter of Rights and Freedoms* – and must be balanced against competing concerns, including law enforcement, national security, third party individual rights and legitimate business purposes.[3] Reflecting this balance, Canadian privacy rights, obligations and remedies exist in an extensive legal framework, which gives breadth to the meaning of consent, and yet recognizes that consent is not required in certain circumstances.

This framework encompasses federal and provincial private and public sector privacy laws, criminal and human rights legislation, emerging common law torts and, in Québec, developments in the civil liability regime. For example, the *Protecting Canadians from Online Crime Act* created new criminal offences that are designed primarily to require consent for the distribution of intimate private images, and protect vulnerable persons from public humiliation and cyberbullying.[4]

Schedule 1 of PIPEDA speaks directly to the underlying principles of consent in the private sector, laying the foundation that businesses must seek meaningful consent and cannot force individuals to consent to the use of personal information beyond legitimately identified purposes (s. 4.3.3). PIPEDA's consent model comes with ten fair information principles – or "bells and whistles" – that include accountability, identifying purposes, consent, limiting

---

2 *Personal Information Protection and Electronic Documents Act,* SC 2000, c 5, available online (http://ow.ly/oaJJ30a9lvb).

3 Part I of the *Constitution Act, 1982, Schedule B to the Canada Act 1982* (UK), 1982, c 11, available online (http://canlii.ca/t/ldsx).

4 *Protecting Canadians from Online Crime Act*, SC 2014, c 31, at s. 162.1 and s. 163, available online (http://canlii.ca/t/52m4g).

collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access, and challenging compliance.

These principles balance protecting individual privacy rights by holding organizations accountable for their privacy practices, with enabling innovation by allowing organizations to use personal information in the pursuit of legitimate business opportunities. Importantly, all treatment of personal information is subject to the "reasonable person test," which limits the collection, use and disclosure of personal information to what is reasonable in the circumstances, particularly where consent is required. In addition, industry best practices in Canada have long incorporated Privacy by Design principles and the use of privacy impact assessments, which support PIPEDA's overarching accountability principle.

The PIPEDA consent model, supported by the broader legal framework, continues to be robust in its protection of the privacy of Canadians – including vulnerable groups – in the face of emerging technologies and business models that increasingly rely on the collection of personal information. While there is not a compelling case for legislative change at this time, we support the continued use of a multifaceted "tool kit" approach to privacy protection in Canada.

RECOMMENDATION

1. **The CBA Sections recommend maintaining the existing consent model in PIPEDA in the absence of a compelling need for legislative change, and the continuing use of a multifaceted "tool kit" approach to privacy protection in Canada.**

III. RIGHT TO BE FORGOTTEN

While the CBA Sections do not make any recommendations on whether a specific right to be forgotten should be included in PIPEDA, this is as an issue that merits attention. The OPC is currently consulting on reputational privacy, including whether the right to be forgotten has application in PIPEDA, and if there is a need to enhance available recourses in the face of reputational harm.

The right to be forgotten, as it has evolved in the EU, is not addressed directly in PIPEDA. However, PIPEDA allows an individual to withdraw consent, which partially addresses the concerns that this right seeks to address (subject to certain limitations, such as those related to publicly available information). PIPEDA also requires organizations to use published personal

information for consistent purposes. This was found not to be the case in the recent Federal Court decision *A.T. v. Globe24HR.com,* where a Romanian website copied and made Canadian court decisions available through Google searches.[5] The Court required the website to delete all of the decisions and seek to have them removed from search engine caches. This is similar in some respects to the right to be forgotten, but for different reasons.

As discussion continues about the right to be forgotten, and the extent to which it has a place in the Canadian legal landscape, we need to be mindful that PIPEDA and other private sector privacy legislation is not the catch-all for issues that arise from the ongoing evolution of technology. Beyond PIPEDA, there are numerous other considerations – such as the right to freedom of expression, which is a critical piece of our democratic fabric found in the *Charter*.

IV. ORDER MAKING POWERS

In PIPEDA, the OPC generally has the role of ombudsperson, and does not have the powers to make orders, to order statutory damages, or to impose administrative monetary penalties. The CBA Sections recommend maintaining the ombudsperson model, unless there is compelling evidence that a change to the OPC's enforcement powers is actually needed.

Those in favour of giving the OPC more enforcement powers argue that companies are not deterred by the consequences of being found non-compliant with PIPEDA, and that the two-step procedure to obtain a remedy in Federal Court is time-consuming and costly. However, cybersecurity concerns are often front page news, and privacy breach clauses in commercial agreements often reflect uncapped liability, making them top-of mind for most organizations.

Proponents of order-making powers also point to the OPC's counterparts in Europe, the US and some Canadian provinces, which have the authority to make binding orders – and in the case of the EU's new General Data Protection Regulation (GDPR), the authority to impose fines. However, in many ways the GDPR is catching up with principles in PIPEDA – in particular the accountability principle, which has been the cornerstone of PIPEDA for over 15 years.

Existing Enforcement Powers

The OPC enforces privacy rights by leveraging its existing powers to investigate, audit and take organizations that fail to uphold their obligations in PIPEDA to court.

---

5 *A.T. v. Globe24HR.com,* 2017 FC 114, available online (http://ow.ly/HeJY30a9mLM).

The main remedy exercised by the OPC has been to make formal findings based on investigations of section 11 complaints. The findings conclude that a complaint is "well founded", "not well-founded" or "resolved," and give the complainant the right to apply to the Federal Court for specified relief. In cases where the OPC deems it appropriate to publicize findings, a summary is posted on its website, usually without naming the parties. The names of parties are included only when deemed to be in the public interest; however this has proven to be a powerful tool, forcing domestic and foreign organizations of all sizes to revise their privacy practices. The OPC has taken a proactive approach in following up with organizations to determine if they have made the necessary changes. The OPC can also settle a complaint during the course of an investigation or implement early resolutions before investigating. These are also posted on the OPC website.

Recent amendments to PIPEDA give the OPC the ability to enter into binding compliance agreements with organizations, and to enforce non-compliance through the courts. These amendments will also make a common industry practice a mandatory obligation when they come into force: organizations must notify individuals when a breach of their privacy safeguards may lead to a real risk of significant harm to the individual, and report breaches to the OPC. This new breach reporting framework includes potential fines for failing to report a breach.

Canadian courts are uniquely qualified and well-placed to assess damages uncovered by OPC investigations, and have done so in numerous cases – including to order any necessary changes to an organization's practices. They can also recognize new civil actions in the privacy protection realm, and reinforce the principle that consent must be robust and freely given only for the purposes for which they were initially contemplated.

Courts in common law jurisdictions, for example, have recently created two new torts giving rise to a cause of action: intrusion upon seclusion (*Jones v. Tsige*); and non-consensual distribution and publication of intimate facts and images (*Jane Doe 464533 v. N.D.*).[6] In *Jane Doe*, the aggrieved party was awarded $141,708.03 in general, aggravated and punitive damages, and costs. Québec courts also have a long history of providing meaningful remedies for victims of non-consensual use of personal information.[7]

---

6 *Jones v. Tsige,* 2012 ONCA 32, available online (http://canlii.ca/t/fpnld). *Jane Doe 464533 v. N.D.,* 2016 ONSC 541, available online (http://canlii.ca/t/gn23z).

7 *L.D. c J.V.*, 2015 QCCS 1224, available online (http://canlii.ca/t/ggzlq). *Pia Grillo v. Google inc.*, 2014 QCCQ 9394, available online (http://canlii.ca/t/gf2c4).

Privacy protections in other parts of Canada's privacy framework also provide remedies for non-consensual uses and disclosures of personal information. For example, British Columbia, Saskatchewan, Manitoba and Newfoundland and Labrador have a statutory tort for invasion of privacy. Regulators like the Canadian Radio-television and Telecommunications Commission (CRTC) also have enforcement powers in Canada's Anti-Spam Legislation (CASL) and the CRTC Unsolicited Telecommunications Rules. The *Criminal Code* contains offences related to the interception of private communications, unauthorized use of a computer, and mischief in relation to computer data.

The CBA Sections recommend maintaining the OPC's ombudsperson role for a number of reasons. First, it holds organizations accountable to protect privacy in a way that enhances their service delivery and encourages technological innovation in Canada. Second, it would be prudent to see how the OPC's new power to issue and enforce binding compliance agreements through the courts is interpreted and used, as well as how the new breach reporting obligations unfold. Third, as the Commissioner's role is currently structured, conferring order-making powers on the Commissioner could result in a violation of the principles of fundamental justice. Combining advocacy, investigative and decision-making roles may place the Commissioner in a conflict of interest and undermine the credibility of the Office. Fourth, order powers would fundamentally alter the OPC's relationship with organizations, and have a chilling effect on the openness and cooperative dialogue that many organizations currently enjoy with the OPC. Finally, order making powers in the context of a flexible principles-based law like PIPEDA – which requires organizations to constantly make judgments about what is appropriate in their circumstances – can be difficult to apply in practice.

RECOMMENDATION

2. **The CBA Sections recommend maintaining the ombudsperson model, unless there is compelling evidence that a change to the OPC's enforcement powers is actually needed.**

V. NON-BINDING ADVANCE OPINIONS

The CBA Sections recommend that PIPEDA be amended to authorize the OPC to issue non-binding advance opinions to organizations proposing new programs, technologies, methodologies or specific transactions, on request.

While the OPC currently offers general guidance in the form of case summaries, interpretation bulletins, issue-specific guidance documents and more general best practices guidance documents, it does not provide organization-specific guidance in the absence of an investigation or audit.[8] Advance non-binding opinions could be issued pursuant to the OPC's general power to promote the purposes of PIPEDA. However, stipulating this express authority would make it clear that the OPC is expected to perform this function when approached by an organization, and support the allocation of additional resources to it.

Similar models in other statutes form a precedent for advance guidance to organizations in situations broadly analogous to PIPEDA compliance. For example, the *Competition Act* gives the Commissioner of Competition authority to issue binding advance opinions, and the Canada Revenue Agency exercises a similar role with its advance rulings on compliance with the *Income Tax Act*. While the CBA Sections do not currently recommend that the OPC issue binding opinions, if experience with non-binding advance opinions indicates a value in providing binding opinions, the OPC's authority could be amended in the future to allow it.

Advance non-binding opinions would allow organizations to voluntarily submit a description of relevant facts about a proposal to the OPC, including the organization's existing privacy compliance framework, and proposed approach to address privacy compliance for the new program or transaction. The OPC could then respond with a non-binding opinion providing comments and recommendations on the proposal's compliance with PIPEDA.

The benefits of this approach for organizations include clear guidance and confidence on the privacy compliance of their new initiative. Where possible, advance opinions with general application could be anonymized and published by the OPC to assist other organizations contemplating similar initiatives.

RECOMMENDATION

3. **The CBA Sections recommend that PIPEDA be amended to clearly authorize the OPC to issue non-binding advance opinions to organizations proposing new programs, technologies, methodologies or specific transactions.**

---

8 *See* for example, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, and Office of the Information and Privacy Commissioner for British Columbia, *Getting Accountability Right with a Privacy Management Program* (April 2012), available online (http://ow.ly/a3SV30a9mvn).

VI. PUBLICLY AVAILABLE AND PUBLIC INFORMATION

PIPEDA was carefully drafted to be technology neutral, and stands the test of time, allowing organizations to evolve their privacy practices to reflect changing business models, technologies and customer expectations. While PIPEDA is consent-based, it also offers practical exemptions to consent where it is not practical or necessary, including exemptions for publically available information – with the understanding that all other PIPEDA privacy obligations and safeguards would continue to apply.

However, unlike PIPEDA, the Regulations published subsequently missed the mark in certain respects, and have created uncertainty.[9] Exemptions in the Regulations have been unable to keep up with changes in technology, with how organizations communicate with individuals, or how they use information that individuals have chosen to make public. The result is uncertainty about what level of consent is required to use personal information that individuals make public online.

Directories Exemption

When PIPEDA came into force, the government wanted to preserve the ability of organizations to collect, use and disclose personal information in telephone directories without consent – once again, with the understanding that all other PIPEDA privacy obligations and safeguards would continue to apply. A narrow exemption for contact information in telephone directories was included in subsection 1(a) of the Regulations, which is not technology neutral. It does not reflect the current online environment, where individuals can choose whether to make their personal information (including other contact information) public through a wide variety of social media platforms where they control what personal information is made public or not.

Publications Exemption

As technology has evolved, organizations are turning instead to a much broader exemption in the Regulations to accommodate the online and social media context by relying on subsection 1(e) in the Regulations on printed or electronic publications. The term "publication" generally refers to the act of announcing or bringing information before the public, and some dictionaries explicitly contemplate that it includes posting content online.

---

9 *See Regulations Specifying Publicly Available Information,* SOR/2001-7, available online (http://ow.ly/yHeq30a9lPv).

Amendments are required to ensure that PIPEDA and its Regulations are technology neutral, and able to accommodate existing and evolving business models and customer expectations. The aim of these amendments should be to maintain PIPEDA's balance while removing unnecessary uncertainty. If a more principles-based and technology-neutral approach is not possible, another possibility may be to review and update the list of exemptions. In either case, the exemptions should not be too broad.

Parliament could consider amending subsections 7(1), (2) and (3) of PIPEDA to expand what is meant by "publicly available," or add another exemption in each of the three subsections that addresses the collection, use and disclosure of publicly available personal information without consent in a technology-neutral fashion. Similar to the existing regime, any subsequent use by business should remain subject to all other privacy obligations and safeguards in PIPEDA. The government could also consider amending the exemptions in the Regulations directly, and the OPC could issue additional guidance on the level of consent required to use personal information that individuals make public.

Any of these options would help to clarify the balance between protecting the privacy of individuals and the legitimate needs of business to use personal information – promoting innovation through increased trust and certainty, and reflecting the choice individuals may have made to make some of their personal information public.

RECOMMENDATION

4. **The CBA Sections recommend that amendments are required to ensure that PIPEDA and its Regulations are technology neutral, and able to accommodate both existing and evolving business models and customer expectations.**

VII. ADEQUACY

Given the global nature of data flows and their importance to commerce, it is important for Canada to collaborate with other jurisdictions to align laws for cross-border data transfer. Canada has enjoyed partial adequacy status under the EU's 1995 Data Protection Directive through PIPEDA since December 2001.[10] This status has enabled the transfer of personal

[10] Council of the European Union, *COMMISSION STAFF WORKING DOCUMENT: The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act* (November 22, 2006), available online (http://ow.ly/83lI30a9m3A).

information from the EU to organizations in Canada that are subject to PIPEDA without the need to implement other mechanisms to safeguard privacy, such as binding corporate rules or model contracts.

The Council of the EU's adequacy status decision for Canada was based on an assessment of whether PIPEDA addressed the basic privacy principles necessary to provide an adequate level of protection for EU data subjects. It recognized the legitimacy of PIPEDA containing exceptions and limitations on the right to privacy to safeguard important interests, such as national security, without making specific enquiries into their nature and scope.

Recent developments in EU privacy law, stemming from legislation and case law, are now raising questions about whether Canada's adequacy status may be at risk. While losing adequacy status would not be fatal to the ability of Canadian organizations to receive transfers of personal information from the EU, a distinct convenience accompanies an adequacy decision. This takes on added importance as Canada seeks to enhance its trade in goods and services with EU countries through international trade agreements such as the Canada-EU Comprehensive Economic and Trade Agreement.[11]

When the EU's new GDPR comes into force in 2018, it will repeal and replace the 1995 Data Protection Directive, and change the EU's approach to an adequacy determination.

It is not yet clear what the EU's new approach will be, or whether there will be an expansion of the basic principles that a third country's privacy laws will need to address. Article 41 of the GDPR, which addresses the elements to be considered by the European Commission in considering adequacy, differs significantly from Article 25 of the 1995 Data Protection Directive. It specifically directs the Commission to examine the relevant legislation in force in the third country, including laws concerning public security, defence, national security and criminal law, as well as international commitments. What is clear is that the GDPR will include explicit rights to be forgotten and to data portability. It will also impose mandatory obligations for breach notification, privacy by design, and consent to process the personal information of children under 13 years of age.

In the meantime, the EU will continue to grapple in the immediate term with the new EU-US Privacy Shield and the impact of the emerging policies of the US administration on its efficacy,

---

11 Government of Canada, *Text of the Comprehensive Economic and Trade Agreement – Table of contents* (November 2016), available online (http://ow.ly/XRqM30a9mdT).
Bill C-30, *Canada-European Union Comprehensive Economic and Trade Agreement Implementation Act*, available online (http://ow.ly/KKtk30a9mgH).

and it can be expected that some further guidance on what constitutes "adequacy" in the new EU privacy regime will be forthcoming.

Once the GDPR comes into force, Canada's adequacy status will be time limited, remaining in force until it is amended, replaced or revoked. It will also be subject to monitoring by the European Commission, and a regular report on adequacy will be presented to the European Parliament and to the Council, starting four years from the date the GDPR comes into force (at the latest).

The broad framework that regulates the flow of personal information between the private and public sector in Canada would be considered as a whole in assessing our status under the new GDPR regime. Recent and upcoming legislative amendments, as well as case law developing in response to the evolving privacy interests of Canadians, may reconfirm our adequacy status. However, if the Commission chose to revoke Canada's adequacy status, it would enter into consultations with the Canadian government in an attempt to address problematic issues. Transfers of personal information to Canadian organizations would be prohibited during that period, absent implementation of "adequate safeguards," described in Article 42 of the GDPR, by Canadian organizations.

Careful consideration must be given to the desirability of amending PIPEDA for the sole purpose of maintaining Canada's EU adequacy status. While achieving this status was a motivating factor behind the creation of PIPEDA, it was drafted with a broader purpose. As Canada's federal private sector privacy law, it needs to strike the right balance between information sharing and privacy that is appropriate for the Canadian context, taking into account our *Charter* values, among other factors. PIPEDA is also only one part of Canada's privacy framework, and may not always be the appropriate or only vehicle for addressing adequacy concerns that may arise, particularly in relation to information sharing.[12]

RECOMMENDATION

5. **The CBA Sections recommend that while Canada's EU adequacy status should be subject to careful monitoring, amending PIPEDA to anticipate changes that may be required to maintain this status is premature.**

---

12 *See for example,* Canadian Bar Association, *Security of Canada Information Sharing Act (SCISA)* (January 2017) Submission available online (http://ow.ly/59Ta30a9mm3) for points raised on effective oversight of information sharing for the purpose of safeguarding national security that are relevant to adequacy.

VIII. CONCLUSION

The CBA Sections appreciate the opportunity to share our view that the existing consent and ombudsperson models found in PIPEDA should generally be maintained, while carefully monitoring Canada's EU adequacy status. Amendments should be made in the context of these models to ensure the Act and its regulations are technology neutral and to allow the OPC to issue non-binding advance opinions. We trust that our comments will be of assistance, and would be pleased to provide any clarifications.

IX. SUMMARY OF RECOMMENDATIONS:

The CBA Sections recommend:

1. **maintaining the consent model in PIPEDA in the absence of a compelling need for legislative change, and the continuing use of a multifaceted "tool kit" approach to privacy protection in Canada.**
2. **maintaining the ombudsperson model, unless there is compelling evidence that a change to the OPC's enforcement powers is actually needed.**
3. **amending PIPEDA to clearly authorize the OPC to issue non-binding advance opinions to organizations proposing new programs, technologies, methodologies, or specific transactions.**
4. **amending PIPEDA and its Regulations to ensure they are technology neutral, and able to accommodate both existing and evolving business models and customer expectations.**
5. **carefully monitoring Canada's EU adequacy status, however amending PIPEDA to anticipate changes that may be required to maintain this status would be premature.**