Improving private sector privacy for Ontarians in a digital age - An argument for "Made in Canada and brought to Ontario" reform[1]

Dan Michaluk, Eloise Gratton, Elisa Henry, Ira Parghi[2]

Ontario has invited input on a matter of legislative reform with immense potential consequences for the conduct of business in the province. We write as legal counsel to Ontario private sector businesses targeted by this initiative.

The private sector in Ontario has been subject to privacy regulation since the early 2000s with the enactment of the *Personal Information Protection and Electronic Documents Act*.[3] Since that time, Ontario businesses have developed an understanding of fair information practice principles, developed privacy programs and administered those programs. Business have done well in meeting their obligations, and have benefited from a principled and flexible form of regulation and reasonable uniformity in Canadian privacy regulation.

We appreciate the concerns that have led Ontario to consider legislative reform. The implementation of clear and well-balanced rules for the collection, use and disclosure of personal information is an important matter of consumer rights and a significant enabler of economic growth. Legislative reform federally and in other provinces is inevitable, and Ontario is a stakeholder without a voice if it does not engage with potential legislative reform.

However, the province has presented "made in Ontario" as a governing theme for reform even though any further fragmentation of Canadian privacy law would do great harm to Ontario businesses. Ontario should consider forgoing the enactment of duplicative legislation altogether. If the province must aim to replace PIPEDA within its borders, the substance of Ontario's law should be highly aligned with other Canadian privacy laws. We see no way for this to occur without strong dialogue between the province and other jurisdictions. And this is a dialogue that must occur immediately.

In this regard, Ontario should approach the adoption of rights brought in by European legislation very carefully. The rights to erasure and data portability, in particular, are too technical and potentially burdensome to business to be required by legislation that applies across all sectors. We also question whether they are essential to consumer privacy protection.

We respectfully ask Ontario to consider these ideas along with the five specific submissions below.

1. AIM FOR STRONG ALIGNMENT WITH OTHER CANADIAN LEGISLATION

Ontario has stated, "[W]e also want to ensure that any new privacy protections do not pose unnecessary burden to businesses, or inhibit the growth and prosperity of Ontario's innovation ecosystem." Given its commitment, the province should work with other jurisdictions to promote a high degree of legislative alignment across Canada.

To date, Ontario businesses have benefited from reasonable uniformity in Canadian privacy regulation. PIPEDA applies broadly, displaced only by commercial sector regulation in British Columbia, Alberta and Québec. All three provincial statutes and PIPEDA are based on the same principles - the principles of *Fair*

---

[1] Brief submitted to the Ministry of Government and Consumer Services in response to regulatory proposal 20-MGCS015.

[2] Members of BLG's national privacy and data protection team, which Ms. Gratton and Henry co-lead. The contents of this brief should not be construed as legal advice. The opinions expressed herein are solely those of the authors in their personal capacity and in no way represent the views of the law firm Borden Ladner Gervais LLP or its clients.

[3] *Personal Information Protection and Electronic Documents Act*, SC 2000 (PIPEDA).

Information Practices that have been incorporated in data protection laws adopted in various jurisdictions around the world.[4]

Alignment, however, could be stronger. Many Ontario businesses have failed to identify and understand the unique, technical provisions relating to trans-border data flows embedded in the Alberta *Personal Information Protection Act*, for example[5] Ontario businesses have also generally looked to Québec legal counsel for even a basic understanding of the Québec *Private Sector Privacy Act* given its unique form.

Even small differences across legislation can greatly increase the cost of compliance. Ontario's initiative, by raising the prospect of adding another provincial private sector privacy law to the Canadian statutory mix, raises the potential for true fragmentation that could have extremely negative consequences for business in Ontario and elsewhere.

The dialogue required to achieve uniformity must occur immediately. Québec is now pushing the pace with *Bill 64, An Act to Modernize Legislative Provisions Respecting the Protection of Personal Information*. We understand the federal government is nearly ready to introduce legislation that will substantially amend PIPEDA. Business will be harmed if the three governments proceed in competition with one other.

2. AIM FOR REASONABLE ONTARIO-BASED ENFORCEMENT

Ontario <u>can</u> be fully committed to privacy protection and nonetheless opt against severe consequences for non-compliance.[6] In our view the province <u>should</u> opt against severe consequences for non-compliance; such consequences are harmful to business when applied to a law that is not and cannot be clear.

Canadian privacy legislation has been purposely drafted on the basis of flexible principles (or "soft law") intended to be technology neutral so that the law could be more easily applied to new types of technologies. This flexible construction is essential, yet it is understandably difficult for organizations to discern what practices will be considered compliant. [7]

The Supreme Court of Canada has also made clear that privacy is not absolute – that we always aim to strike a balance – and that privacy is a "protean," ever-changing concept.[8] American privacy expert Daniel Solove calls privacy "a concept in disarray."[9] He explains:

> Nobody can articulate what it means. Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body,

[4] See section 1.1 "The Historical Background Leading to Laws Protection Personal Information" from *Understanding Personal Information: Managing Privacy Risks*, LexisNexis, 2013.
[5] *Personal Information Protection Act*, SA 2003, c P-6.5, ss 6(2) and 13(1).
[6] We have raised our concern with the scope of the monetary penalties that may be imposed on organizations pursuant to the Quebec Bill 64's enforcement mechanisms (ss. 90.12, 91), as they may be disproportionate if applied systematically. Our brief submitted to the Quebec Assembly is available online: http://www.assnat.qc.ca/en/travaux-parlementaires/commissions/CI/mandats/Mandat-43315/memoires-deposes.html
[7] See Innovation, Science and Economic Development Canada, *Strengthening Privacy for the Digital Age, Proposals to modernize the Personal Information Protection and Electronic Documents Act*, May 2019: "It should also be recognized, though, that non-compliance can sometimes be the result of a lack of clarity or certainty in terms of organizations' obligations under the Act. Organizations may want to comply but have difficulty understanding what they need to do in certain circumstances." And "Although praised for being principles based and technology neutral, PIPEDA has been criticized for being difficult to understand," referring to Dr. Teresa Scassa, who has summarized these criticisms in her blog, dated July 9, 2018 : http://www.teresascassa.ca/index.php?option=com_k2&view=item&id=279:pipeda-reform-should-include-a-comprehensive-rewrite&Itemid=80.
[8] *R v Tessling*, 2004 SCC 67 (CanLII), [2004] 3 SCR 432, par 25, <http://canlii.ca/t/1j0wb#par25>.
[9] Daniel J. Solove, *Understanding Privacy*, Harvard University Press, May 2008, p 1. These conceptual difficulties impose a burden on legislators, regulators and regulated populations, although we acknowledge that global privacy laws are all based on fair information practice principles that frame informational privacy as requiring a right to control the collection, use and disclosure of one's personal information.

> solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations. Philosophers, legal theorists, and jurists have frequently lamented the great difficulty in reaching a satisfying conception of privacy. Legal scholar Arthur Miller has declared that privacy is "difficult to define because it is exasperatingly vague and evanescent." "On closer examination," author Jonathan Franzen observes, "privacy proves to be the Cheshire cat of values: not much substance, but a very winning smile." According to philosopher Julie Inness, the legal and philosophical discourse of privacy is in a state of "chaos."[10]

As counsel to organizations, we have seen the most novel and creative privacy claims - claims motivated by a genuine belief in what ought to be one's right to privacy yet not associated with any tangible loss. Providing for a private right of action in any Ontario legislation would invite more of such claims at little benefit to the public, and would burden our already strained civil justice system. Only the lawyers would win.

Large administrative monetary penalties or fines are similarly problematic when the bases for penalties and fines are unclear. Such penalties may incentivize Ontario businesses to act, but to what end? Those who do act will strive for an objective that is not clear and face severe consequences if they fail to meet that amorphous objective. The potential for unfair, disproportionate enforcement would be very high unless carefully constrained in the legislation.[11]

As counsel to organizations, we have also seen the benefit of the PIPEDA ombudsman model for overseeing compliance. This model has allowed organizations to innovate without great risk since they have not needed to be concerned about being fined for misreading the social norms in place at the time or the "reasonable expectation" of consumers. Instead, organizations have had the opportunity to interact with the OPC and adjust their activities. This has allowed the OPC to articulate PIPEDA's requirements through a gradual, bottom-up process that involves a positive back-and-forth with business.

3. AVOID THE RIGHTS OF ERASURE AND DATA PORTABILITY

Canadian privacy legislation has given Ontarians fundamental control of their personal information – control over its collection, use and disclosure. Ontario businesses must destroy, erase or make anonymous personal information when there is no longer a purpose for retaining it, but they are not required to find and delete personal information based on individual demand. Ontario businesses must provide access to personal information in a form that is generally understandable, [12] but are not required to meet a prescriptive standard for the export or exchange of data.

Canadian legislators have struck a balance, appropriately in our view, based on a respect for business autonomy and a need to minimize the regulatory burden on business. This is the essential problem with recognizing a right of erasure or a right to data portability: such rights will push onto business obligations that are complex, poorly understood and difficult to implement. We say this while acknowledging that data mobility can enhance consumer choice and lead to gains. Policymakers are best placed to achieve these gains through sectoral initiatives led by business. We support, for example, the ongoing initiatives to advance open banking.

4. INTRODUCE NEW LEGAL BASES FOR DATA PROCESSING

We are encouraged by Ontario's commitment to "re-imagining consent and transparency requirements, and considering alternative models." Likewise, we are pleased that the province is committed to clarifying

[10] *Ibid.*
[11] A full right of appeal, for example, would be appropriate if the province gave the Information and Privacy Commissioner/Ontario the power to administer significant monetary penalties.
[12] *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Schedule 1, Principle 4.5.3.

when consent "is not necessary, practicable or appropriate, such as in instances where the collected data has been 'deidentified' or 'derived.'"

In our view, the use of consent should be limited to situations where individuals have a real choice, as opposed to a purely illusory or non-existent choice. As said recently by the Privacy Commissioner of Canada, "Simply put, it is neither realistic nor reasonable to ask individuals to consent to all possible uses of their data in today's complex information economy. The power dynamic is too uneven."[13]

The European Union General Data Protection Regulation recognizes five legal bases for processing personal data other than consent, including the legitimate interests of a business and the need to perform a contract, including service contracts.[14] This, in our view, is a good means of addressing the problem of "consent fatigue" that is recognized in Ontario's discussion paper. We encourage Ontario to require consent only for secondary purposes and in other circumstances in which processing truly is, and should be, optional.

5. LEAVE EMPLOYEES TO THEIR NOW EXISTING RIGHTS

When British Columbia and Alberta enacted their consumer privacy legislation, they extended the scope of the legislation to employees of provincially regulated employers. This required them to enact special provisions to account for the well-recognized rights of "management" that are inconsistent with a consent based privacy regime.[15]

Employees in Ontario have privacy rights despite the absence of statutory protection. Unionized employees can grieve a workplace privacy violation even in the absence of express collective agreement rights, relying most often on the "balancing of interests" approach now endorsed by the Supreme Court of Canada in the *Irving Pulp and Paper* drug testing case.[16] In 2012, the Court of Appeal for Ontario issued the landmark *Jones v Tsige* case, recognizing an "intrusion upon seclusion" tort.[17] The Superior Court of Justice has followed by recently recognizing the "public disclosure of private embarrassing facts" tort.[18]

These developments could allow the province to enact a focused consumer privacy statute that does not necessarily need a separate facet to address workplace privacy. They could also allow the province to target a limited enforcement budget at its primary and stated concern: the enhancement of consumer privacy.

Conclusion

We are grateful for having the opportunity to provide this input. We have addressed the most significant issues for the province to consider prior to the introduction of legislation. We look forward to having an opportunity to give input that is comprehensive if and when the province proceeds with introducing a bill.

October 13, 2020

---

[13] *Appearance before the Committee on Institutions of the National Assembly of Quebec regarding Bill 64, An Act to modernize legislative provisions as regards the protection of personal information*, September 24, 2020, published at <https://www.priv.gc.ca/en/opc-news/speeches/2020/sp-d_20200924/>.

[14] See Article 29 Data Protection Working Party, "Guidelines on Consent under Regulation 2016/679", November 2017, online: < https://www.cnil.fr/sites/default/files/atoms/files/ldconsentement_wp259_rev_0.1_fr.pdf> (revised and adopted on April 10, 2018).

[15] *Personal Information Protection Act*, SBC 2003, c 63, ss 13, 16 and 19 and *Personal Information Protection Act*, SA 2003, c P-6.5 ss 15, 18 and 21.

[16] *Communications, Energy and Paperworkers Union of Canada, Local 30 v Irving Pulp & Paper, Ltd*, 2013 SCC 34 (CanLII), [2013] 2 SCR 458, par. 4, <http://canlii.ca/t/fz5d5#par4>.

[17] *Jones v Tsige,* 2012 ONCA 32 (CanLII), <http://canlii.ca/t/fpnld>.

[18] See *Yenovkian v Gulian*, 2019 ONSC 7279 (CanLII), <http://canlii.ca/t/j4gqn>.