Special Committee review of the *Personal Information Protection Act* (PIPA):
Input from BC Tech, 7 July 2021

Context

There is a growing consensus among policy-makers that changes to Canadian privacy laws are required to reflect the exponential growth of digital products and services, and the increased importance of data in the modern economy. At the federal level, the government has published a detailed discussion paper on proposals to modernize the *Personal Information Protection and Electronics Documents Act*. In the Province of Quebec, Bill 64, An Act to Modernize Legislative Provisions Respecting the Protection of Personal Information, was introduced in the Quebec National Assembly on June 12, 2020.

The BC Information and Privacy Commissioner has indicated that "*[m]ajor reform is urgently needed*" to PIPA, which is largely unchanged from the version that came into effect in January 2004.

It is expected that the Special Committee will use the current review process to issue recommendations calling for significant amendments to PIPA.

Members of BC Tech have much at stake in the legislative review process. While trust of consumers is often critical to the success of technology businesses, privacy rules can have meaningful, often unintended, consequences, particularly if the rules are not interoperable with rules in other jurisdictions.

What's clear is that a balanced approach is needed – one that recognizes the right of privacy of individuals and the need of organizations to collect, use or disclose personal information for reasonable purposes. If this balance is not achieved, the continued growth of the tech-sector in BC would be jeopardized and, more broadly, BC would become a less attractive jurisdiction in which to carry on business.

These risks are not theoretical. Following the adoption of the General Data Protection Regulation (GDPR) in the EU, it has become more difficult for smaller companies in Europe to survive – let alone unseat incumbents. Large companies have the technology, legal and financial resources required to redesign products and operations, and to bear the risk of large fines. Smaller companies often don't.

How effective is the current legislation?

What works well?

PIPA has proven to be effective and resilient. It can be applied to countless new and unforeseen commercial activities in a rapidly changing data environment, without the need for frequent legislative amendments.
PIPA's effectiveness can be attributed to the following four key features:

1) PIPA is principles-based, allowing organizations to implement privacy protections in a flexible and context-specific manner, taking into account actual risks;

2) PIPA is technology and business sector neutral, making it largely future-proof;
3) PIPA's privacy principles are both non-prescriptive and generally consistent with common-sense business practices, making it possible for most businesses to understand what the law requires; and
4) PIPA generally balances privacy considerations with business requirements.

What does not work well?

PIPA is a consent-based statute. This means that the authority to collect, use or disclose personal information requires the consent of the individual, subject to limited exceptions. While the objective of a consent-based model (i.e., putting individuals in control of their data) is laudable, it's clear that consent has become ineffective in the modern digital world. It is unrealistic to expect the average person to invest the time required to fully understand the details of every privacy policy they may come across on a daily basis. It is equally challenging for industry to comprehensibly communicate the details of every potential use of personal information to individuals.

These challenges are exacerbated when new, unanticipated uses of information are identified. Increasingly, data analytics makes it likely that organizations will have the ability to use information for new purposes that benefit individuals, businesses and society in unanticipated ways from when consent was originally obtained. In these instances, it can be very challenging, if not often impossible, to obtain consent.

A legislative review of PIPA provides an opportunity to explore how alternatives to consent can be adopted that both enable the responsible use of information, while also making privacy protections more effective.

Future Changes

General comments

It is critical that any amendments to PIPA reinforce the four key features of PIPA described above. Making refinements to the existing regulatory framework is preferable to adopting a wholesale new approach.

Additionally, it is critical that PIPA be interoperable with privacy frameworks deployed in other leading jurisdictions, including the European Union. Interoperability does not require that the same exact obligations be adopted (for example, by copying legislative requirements). Rather, it can be achieved through a regulatory framework with compatible outcomes and without requiring that different operational processes or technological systems be adopted than those that meet the global standard.

While interoperability is an important consideration for privacy legislation anywhere in the world, it is particularly critical in the case of smaller jurisdictions – like BC. Whereas the EU (with almost half a billion people) may have the economic might to direct how products or services are delivered, the same can't be said when the applicable market is small. For small markets, it often will be the case that the costs of

compliance cannot be justified economically, making it more likely that impacted businesses will decide to stop selling into the market or even relocate their headquarters to another jurisdiction.

What would be an improvement to the current legislation?

1) Adding new grounds for processing personal information. Consent should be only one of multiple-grounds for processing personal information. Under the GDPR, there are six additional grounds: performance of a contract, compliance with a legal obligation, vital interest of the data subject, public interest and legitimate interest. These additional grounds should be added to PIPA.

2) Excluding de-identified data from the definition of personal information. Enabling the use of de-identified data would support the use of data for analytics, artificial intelligence and other productive uses and help to relieve consent-fatigue among individuals. Legal guardrails, including a prohibition on re-identifying the information, would serve to protect the legitimate interests of individuals.

What are issues to be avoided in any changes to the current legislation?

1) Prescriptive rules. The current principles-based approach enables flexibility while protecting private information through reasonable measures. Maintaining this flexibility is critical to ensure that businesses in BC are able to effectively compete in the global marketplace, while protecting the privacy of individuals.

2) New "data residency" requirements. The approach under PIPEDA (which generally allows for processing of data outside of Canada when equivalent protections are put in place through contracts with data processors). This contrasts with Bill 64 in Quebec, which requires all organizations to undertake an assessment of, among other things, the legal framework in the destination jurisdiction, including the legal framework's degree of equivalency with the privacy protection principles in Quebec. The Quebec approach is not viable as it will undermine day-to-day business activities, including the use of online tools and cloud services (including e-commerce platforms, payment systems, customer relationship management tools and human resource management systems) that have become both ubiquitous and critical to the operations of businesses in the modern economy.

3) Enactment of new rules in respect of data portability, take-down and de-indexing. Internationally recognized standards must emerge before any such rules will be viable. As a practical matter, a

BC-based technology company cannot be expected to incur the cost of developing a compliance solution for BC and then a different solution for other markets.

4) Penalties that lack proportionality to the size of the BC market. Bill 64 in Quebec adopts penalties that are generally aligned to the GDPR (i.e., 4% of worldwide revenue) notwithstanding that it has a population that is less than 2% of the population in the EU. If Bill 64 becomes law, Quebec will have created a strong disincentive for businesses to be headquartered or do business in Quebec – as they will face penalties that are grossly disproportionate to the size of the Quebec market. If BC were to follow Quebec's lead, it would similarly undermine BC's ambition to be a favourable jurisdiction in which to start and scale businesses, including technology businesses.

5) Penalties that aren't tied to harm. An assessment of actual harm to individuals is a critical component of a penalty regime that holds non-compliant organizations to account, without creating punitive fines that discourage innovation or conditions that will promote opportunistic class actions.

6) Enforcement powers that do not comply with principles of natural justice and procedural fairness. Any audit, inspection or discovery rights need to be triggered only if there is a reasonable belief that the applicable organization is not in compliance with PIPA. Self-initiated audits, inspections and investigations that do not satisfy this trigger would be viewed as "fishing expeditions" and, therefore, inconsistent with the rule of law.

7) Health sector-specific regulation that interferes with cost-effective delivery of care. Rules that interfere with digital health deliver, especially rules applicable to data residency, will often negatively impact on the health and safety of British Columbians. Theoretical risks about access to personal information by foreign governments should not take precedence over the delivery of medical care.